# SAMARITAN TECHNOLOGIES TECHNICAL LIBRARY

## Table of Contents

- **APPENDIX A: SAMARITAN TECHNOLOGIES SECURITY OVERVIEW** ........................................... 2
- **APPENDIX B: SAMARITAN TECHNOLOGIES SECURITY POLICIES & PROCEDURES** .................. 4
- **APPENDIX C: SERVICE LEVEL AGREEMENT – SAMARITAN HOSTED SYSTEM** ...................... 32
- **APPENDIX D: DATA CLASSIFICATION & SECURITY POLICY** .............................................. 37
- **APPENDIX E: ASSET MANAGEMENT POLICY** .................................................................. 54
- **APPENDIX F: IT SECURITY INCIDENT RESPONSE POLICY** .................................................. 57
- **APPENDIX G: IT SECURITY INCIDENT MANAGEMENT POLICY** ......................................... 63
- **APPENDIX H: DATA BREACH RESPONSE POLICY** ............................................................ 85
- **APPENDIX I: DATA ENCRYPTION** .................................................................................. 96
- **APPENDIX J: DISASTER PREVENTION & EVENT RESPONSE (DPER) PLAN SUMMARY** ........ 104
- **APPENDIX K: OUTAGE NOTIFICATION PROCEDURE** ....................................................... 113
- **APPENDIX L: SOFTWARE & CONFIGURATION MANAGEMENT & RELEASE PROCESSES** ..... 114
- **APPENDIX M: PRIVACY STATEMENT** .............................................................................. 128
- **APPENDIX N: GOVERNMENTAL DATA REQUEST PROCEDURES** ...................................... 134
- **APPENDIX O: SUSTAINABILITY POLICY** .......................................................................... 137
- **APPENDIX P: HOW TO SUBMIT A REQUEST TO SAMARITAN** ......................................... 139
- **APPENDIX Q: SAMARITAN VPAT** .................................................................................. 141
- **APPENDIX R: MEDIA SANITIZATION AND DISPOSAL POLICY** ......................................... 144
- **APPENDIX S: NON-DISCLOSURE AGREEMENT** ................................................................. 151
- **APPENDIX T: CHANGE MANAGEMENT AND RELEASE PROCESS** ....................................... 153
- **APPENDIX U: SOFTWARE AND SERVICES SUBSCRIPTION AGREEMENT** ......................... 169
Appendix A: Samaritan Technologies Security Overview

At Samaritan, there are many things that we do to make sure that our software is secure. Here’s a summary. Full details are available in Samaritan Security Documents Library.

First, we have specific individuals assigned to our Samaritan Security Policy committee with responsibility for overseeing security for our organization, our facilities and our customers’ data.

Next, we work to embrace and include best practices in our Software Development Life Cycle. We have an established set of policies, standards, guidelines, and procedures. See the previously provided Samaritan Security Documents Library. Our development teams and entire staff is trained in these issues. We include security in our design processes and design reviews. We include discussion on these topics as part of our every Thursday morning product development committee meetings which include senior management, client services, operations, product management, product development, and quality assurance representation.

We provide for and utilize security planning in our design documents. We have defined product release and changed management procedures for both mainstream development and expedited and emergency updates.

We have data retention, disposal, and sanitization policies and guidelines in place. We constantly look for ways to improve our security and update both our standards and practices as we evaluate both potential and actual security issues.

We make use of secure data centers with Rackspace, IBM SoftLayer, and Amazon Web Services that are ISO-27001/SOC 2 compliant or FedRAMP authorized.

All data is encrypted using HTTPS with TLS 1.1 or higher in transit and all PII (Personally Identifiable Information such as names, addresses, email addresses, birthdates, and etc.) and passwords are encrypted using 128-bit AES encryption while at rest using a FIPS 140-2 certified encryption engine. All passwords are first hashed at the browser before being transmitted. In fact, passwords are doubly protected as they are hashed at the browser before being transmitted, HTTPS encrypted during transmission and the hashed values are also encrypted before being stored in our database.

We keep informed on standards and security issues by subscribing to the US-CERT Cyber Security Bulletins. As an example, we drove our clients to use TLS 1.1 or higher before many of them were aware of the issues with standard SSL.

We apply OS and database patches on the first Sunday evening of each month. We have anti-virus software installed on all our staff computers and our servers.

We perform a rolling year-round audit of our systems and security.

We implement RASP in our software. Our system its own IDS and IPS built in that automatically locks out the offending IP address when it detects malicious behavior, logs the issue, and notifies
members of our security and development teams. See the previously supplied Samaritan Security Documents Library for more information.

We perform vulnerability testing using Qualys and Zap internally to check for the OWASP Top 10 and other vulnerabilities with every new release of our software, two to four times per year. All known vulnerabilities are remediated before each release. See "VMS 8.1 Build 8102 Software Vulnerability Test" in the previously provided interim security audit report for details. Several of our customers also test using tools such as Cenzic Hailstorm, IBM Rational, and AppSpider. Usually, vulnerability testing by our clients requires us to disable our RASP. Otherwise, they can't complete their testing as they quickly get locked out.

All access either manual or via our SOAP/XML web services API is authenticated and our RASP system prevents the introduction or removal of any sensitive data.

We monitor our system availability every three minutes and our ability to send outbound emails every half hour. Our engineers are alerted via emails and text messages if the system becomes unavailable or a serious error is encountered by a user.

At Samaritan we believe that we are stewards of our clients’ data and we take that stewardship seriously doing all that we can to keep their data safe in a cost effective manner.
Appendix B: Samaritan Technologies Security Policies & Procedures

Version 2.12
9 October 2018

Contents

REVISION HISTORY.................................................................................................................. 6
1. OVERVIEW.......................................................................................................................... 9
2. AUDIENCE.......................................................................................................................... 9
3. SECURITY POLICY COMMITTEE (A.K.A. INFOSEC) ......................................................... 9
4. MODIFICATIONS TO THESE PROCEDURES .................................................................... 11
5. MANAGEMENT CONTROLS ............................................................................................... 11
6. PASSWORD MANAGEMENT............................................................................................... 12
7. PRIVACY POLICY .............................................................................................................. 14
8. CLIENT INQUIRIES ............................................................................................................ 18
9. AUTHORIZED ACCESS TO CUSTOMER DATA ................................................................. 18
10. UNAUTHORIZED ACCESS OF CUSTOMER DATA .............................................................. 19
11. TERMINATION OF EMPLOYMENT OR PARTNER STATUS ... ............................................. 20
12. RESTRICTED AND CONFIDENTIAL DATA PROTECTION ............................................ 22
13. OFFICE PHYSICAL SECURITY ......................................................................................... 22
14. OFFICE COMPUTER SECURITY ....................................................................................... 23
15. OFFICE WIRELESS SECURITY ......................................................................................... 24
16. MOBILE CODE SECURITY POLICY ................................................................................. 25
17. REMOVABLE MEDIA ....................................................................................................... 25
18. SECURITY WHEN WORKING OFF PREMISES ................................................................. 25
19. PRODUCTION SERVER SECURITY ................................................................................... 25
20. SECURITY AND DEVELOPMENT ..................................................................................... 27
21. LAW ENFORCEMENT CONTACT INFORMATION .......................................................... 28
22. FINANCIAL SECURITY .................................................................................................... 29
23. RELATED STATUTES AND POLICIES .......................................................................... 29
24. APPROVED SOFTWARE .................................................................................................. 30
25. ADDITIONAL ITEMS TO ADDRESS IF NOT ALREADY COVERED .................................... 31
<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Jun 2009</td>
<td>Bruce Behymer</td>
<td>Inserted section 5.3 AMS, RMS, and eCoordinator client account access and password policy.</td>
</tr>
<tr>
<td>30 Mar 2010</td>
<td>Bruce Behymer</td>
<td>Added several items describing the security measures that are part of the eCoordinator system itself.</td>
</tr>
<tr>
<td>2 Apr 2010</td>
<td>Bruce Behymer</td>
<td>Added several items stating the requirements for our eCoordinator servers. Added requirements for annual employee training in these policies and procedures.</td>
</tr>
<tr>
<td>11 May 2010</td>
<td>Bruce Behymer</td>
<td>Listed Juan Rivero as a member of Samaritan’s Security Committee. Juan was asked to join the committee and accepted on 30 April 2010. Added maintenance of a security log as a requirement of the Security Policy Committee. Added annual re-signing of Adherence Agreements.</td>
</tr>
<tr>
<td>15 Jun 2010</td>
<td>Bruce Behymer</td>
<td>Updated privacy policy with sections 5.1 through 5.5 of Samaritan’s software and services subscription agreement as of 14 Jun 2010.</td>
</tr>
<tr>
<td>6 July 2010</td>
<td>Bruce Behymer</td>
<td>Fixed various minor grammatical errors.</td>
</tr>
<tr>
<td>1 Sep 2010</td>
<td>Bruce Behymer</td>
<td>Substantially reorganized the latter part of the document adding the following sections and moving relevant items into them as well as adding several new items: Office Physical Security Office Computer Security Production Server Security Security and Development</td>
</tr>
<tr>
<td>Date</td>
<td>Change Author</td>
<td>Description of change</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>16 Sep 2010</td>
<td>Bruce Behymer</td>
<td>Added clarification and detail to section 6.2.3.</td>
</tr>
<tr>
<td>1 Aug 2011</td>
<td>Bruce Behymer</td>
<td>Add the following policies already supported by our products: eCoordinator and eRecruiter users may change their passwords on their own at any time.</td>
</tr>
<tr>
<td>30 Jan 2013</td>
<td>Bruce Behymer</td>
<td>Removed Juan Rivero from the Security Committee.</td>
</tr>
<tr>
<td>7 Apr 2014</td>
<td>Bruce Behymer</td>
<td>Enhanced section 6.2.3.2 to include secure user defined fields. Added section 6.2.6 covering the transmission of sensitive data to and from Samaritan's production database and application servers.</td>
</tr>
<tr>
<td>8 Apr 2014</td>
<td>Bruce Behymer</td>
<td>Marked some of the communications methods in section 6.2.6 as Samaritan internal only. Added references to firewalls to 6.2.6.</td>
</tr>
<tr>
<td>26 Jul 2014</td>
<td>Bruce Behymer</td>
<td>Added Law Enforcement Contact Information</td>
</tr>
<tr>
<td>29 Aug 2016</td>
<td>Bruce Behymer</td>
<td>Added appropriate references to the <em>Samaritan Technologies Data Breach Response Policy</em>. Added several on-line accounts to the employee termination access removal list. Removed the requirement for the employee entrance to Samaritan’s office suite to be locked at all times. This allows the door to be unlocked during normal business hours while the staff is present. Removed the following requirements as Samaritan does not have a server room or conference room at the present time:</td>
</tr>
</tbody>
</table>
The server room entrance is to be locked at all times.

The conference room is to be locked whenever the conference room is unoccupied.

Removed the following requirement as Samaritan no longer has any in house servers:

Microsoft Internet Security and Acceleration Server or an equivalent is to be used to protect Samaritan’s office network.

Added references to SoftLayer wherever there were references to Rackspace.

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 October 2016</td>
<td>Bruce Behymer</td>
<td>Removed hyperlink reference to the online account access policy since it is completely redundant with the information already contained in this document.</td>
</tr>
<tr>
<td>9 February 2017</td>
<td>Bruce Behymer</td>
<td>Added requirement for the security policy committee chairman to subscribe to security alerts and tips from US-CERT and NCSA.</td>
</tr>
<tr>
<td>13 June 2018</td>
<td>Bruce Behymer</td>
<td>Added guest register / visitor log sheet retention and review periods.</td>
</tr>
<tr>
<td>15 June 2018</td>
<td>Bruce Behymer</td>
<td>Added section 6.10 addressing system IDs, passwords, and logins.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added section 6.11 limiting access to authorized business needs.</td>
</tr>
<tr>
<td>27 June 2018</td>
<td>Bruce Behymer</td>
<td>Added System Activity Review rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added Authorized Access to Customer Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added requirement to maintain a log of all repairs and modifications that affect the physical security of Samaritan’s office suite.</td>
</tr>
</tbody>
</table>
Added a provision for callbacks to the Client Inquiries section.

Replaced all references to SSL with “TLS 1.1 or higher” which we have required for over a year now.

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 Aug 2018</td>
<td>Bruce Behymer</td>
<td>Added default data retention policy.</td>
</tr>
<tr>
<td>9 Oct 2018</td>
<td>Bruce Behymer</td>
<td>Replaced all references to TLS 1.1 with “TLS 1.2 or higher”.</td>
</tr>
</tbody>
</table>

1. Overview

At Samaritan Technologies we offer several web-based volunteer management services and tools that interact with a database of volunteer, opportunity, organization, and logbook records. The information stored in this database belongs to our clients. Thus, as providers of these services we are stewards and caretakers of their data and have a responsibility to protect its security. This document provides our company policies and procedures for keeping our customer’s data safe and secure.

2. Audience

The intended audience for this document consists of all of Samaritan's employees, consultants, and partners. As a team we all share the responsibility of looking out for our customer’s interests.

3. Security Policy Committee (a.k.a. Infosec)

3.1. Membership - The security policy committee consists of the following individuals:

3.1.1. Manager and CEO – Bruce Behymer, Committee Chairman

3.1.2. Non-employee Partner – Joey Smith

3.2. Semi-annual meetings – The security policy committee shall meet at least semi-annually to review the status of the company’s conformance to these policies and procedures. The status review shall include the following items:

3.2.1. An audit of all of the policies and processes stated in this document.

3.2.2. An audit of the status of all access entitlements of all employees, consultants, partners, and resellers shall be reviewed including any and all systems in the section of this document entitled “Termination of Employee or Partner Status”.

3.2.3. A security review of the source code of Samaritan’s products.
3.2.4. An production system activity review that includes the following types of system activity information either as a full review or as a spot check or a sampling:

3.2.4.1. Review of Security Incidents Response reports
3.2.4.2. System user privileges grants and changes logs
3.2.4.3. User-level system access logs, if available
3.2.4.4. User level system activity logs, if available
3.2.4.5. User level transaction log reports, if available
3.2.4.6. Exception reports

3.2.5. A review of the settings of Samaritan’s installation of Microsoft Internet Security and Acceleration Server or whatever equivalent system is installed in Samaritan’s offices.

3.2.6. A compromise check for all production servers under Samaritan’s control. The compromise check should include the following items:

3.2.6.1. Run a full virus scan.
3.2.6.2. Use software like Blacklight or Arcade Detector to find out if there are any hidden processes that should not be running.
3.2.6.3. Use an application like CurrPorts check all open ports and listen for port intrusions.
3.2.6.4. Check NTFS file system permissions.
3.2.6.5. Check user permissions and/or users in the admin group.
3.2.6.6. Check the log files. Check for any SQL type commands in the logs.

3.2.7. For all production and test servers perform the following audits:

3.2.7.1. Identify all open ports and what they are used for.
3.2.7.2. Review the current port monitoring settings.
3.2.7.3. Review the firewall configuration rules:
   3.2.7.3.1. FTP rules
   3.2.7.3.2. Windows Remote Desktop Protocol (RDP) rules
   3.2.7.3.3. Other rules: HTTP, HTTPS, SMTP
3.2.7.4. Confirm that all server login credentials are appropriate.
3.3. The Security Policy Committee is to maintain a log of all significant security related actions taken within the company.

3.4. Security Alerts: The Security Policy Committee Chairman is to subscribe to security alerts and tips from US-CERT and NCSA.

4. Modifications to these procedures

4.1. All modifications to this document are subject to review and approval of the Security Policy Committee.

5. Management Controls

5.1. Employee Non-Disclosure Agreements

5.1.1. All employees, contractors, and Partners with access entitlements are required to complete a non-disclosure agreement stating that they will keep information obtained as part of their employment confidential. A copy of the agreement signed by each employee is to be kept in each employee’s personnel file.

5.2. Employee Background Checks

5.2.1. All employees and partners with data access entitlements are required to have a criminal background check.

5.2.2. All new company hires are to be subject to employment verification, education verification, reference checks, drug screening, and social security verification.

5.2.3. Any exceptions to the screenings and checks listed above in this section subject to review and approval by Infosec, the chief executive officer, the vice-president of operations, and Solution Services Inc.

5.3. Training

5.3.1. Newly hired employees or contractors are to be trained in the policies and procedures discussed in this document.

5.3.2. The policies and procedures in this document are to be reviewed with all Samaritan employees and contractors that have data access rights at least once per year.

5.3.3. The trainings mentioned above should also include the data classification and security policies covered in the Samaritan Technologies Security Documents Library document.

5.4. Security Adherence Agreements

5.4.1. All employees of Samaritan and its contractors with access to client data are to sign an agreement (an Adherence Agreement) stating that have read, understand, and will comply with the policies and procedures in this document. A copy of the agreement signed by each employee is to be kept in each employee’s personnel file.
5.4.2. To accommodate changes that may have been made to this document, employees should re-sign the Adherence Agreement at least once per year. An appropriate time for such re-signing is after the annual security policies and procedures review training.

5.4.3. Persons who have not signed the Security Adherence Agreement are not to have access to client data.

5.5. Performance Evaluations

5.5.1. Employee compliance with Samaritan’s security policies and procedures are to be included in each employee’s written performance evaluations.

5.6. Disciplinary Action

5.6.1. Any employee and contractor or contractor found performing actions or omissions in violation to the policies stated in this document are subject to administrative discipline that may range from having their data access privileges suspended or revoked up to and including employment termination. Partners found performing actions or omissions in violation to the policies stated in this document are subject to discipline per the Samaritan Partnership Agreement.

6. Password Management

6.1. All employees, consultants, and partners are to be informed that they are personally responsible for the security of all passwords, access codes, and security devices such as keys and access cards assigned to them.

6.2. eCoordinator and eRecruiter users are to be allowed to change their passwords at any time on their own.

6.3. Password Strength: All passwords must be different from their associated user IDs. All passwords must be a minimum of 8 characters long and must contain at a minimum a mixture of upper case and lower case alphabetic and numeric characters. This requirement applies to all passwords used in our business setting including, but not limited to Windows passwords, eCoordinator passwords, AMS/RMS passwords and passwords for server access.

6.4. Client Accounts and Passwords:

6.4.1. When doing any testing or maintenance within AMS/RMS or eCoordinator, if possible create a new eCoordinator or AMS/RMS user login or use an existing login that has been specifically created for that purpose. If it is necessary to use a customer’s eCoordinator or AMS/RMS login, inform them beforehand that you will be using their login, and that they will receive a message saying the user id is in use if they try to login to their account while you are performing maintenance. Have them change their password after the maintenance has been completed.

6.4.2. If a client suspects an unauthorized breach of their eCoordinator or AMS login, the two principal options are:
- Disable their login and create a new one
- Have them reset their password via a gotomeeting

In accordance with the *Samaritan Technologies Data Breach Response Policy*, any suspected data breach should be reported immediately to the following people:

1) The client service team leaders for any clients possibly affected by the breach;
2) The vice president of client services; and
3) A member of the Samaritan Security Policy Committee.

6.4.3. AMS, RMS, eCoordinator, volunteer, client, approver, reference and other customer passwords (user passwords):

6.4.3.1. All User Passwords are encrypted with an MD5 or SHA-2 (preferable) hash before being transmitted from the client browser to the eCoordinator system.

6.4.3.2. All User Passwords are stored in encrypted format only.

6.4.3.3. User Passwords are never displayed in clear text format.

6.4.3.4. All AMS and RMS logins should be set to expire after a maximum of one year.

6.4.3.5. All AMS and RMS password of Samaritan staff and consultants should be changed every six months.

6.4.3.6. Password Strength: Strong passwords are a customer selectable option on the AMS Info Tab. If enabled, all passwords must be different from their associated user IDs. All passwords must be a minimum of 8 characters long and must contain at least a mixture of alphabetic and numeric characters. The maximum password size is 40 characters.

6.5. All logins to systems that contain customer data should require at least user ID and password.

6.6. Any incident in which the security of a password, access code, and/or security device such as a key or access card is compromised or such a device is lost must be immediately reported to a member of the Security Policy Committee.

6.7. Default Passwords: All default passwords and user IDs that are supplied with hardware, software, and systems will be renamed and changed from the original defaults.

6.8. A record of all key passwords and on-line accounts for the accounts and systems listed in the section of this document titled “Appendix A Samaritan Accounts and Systems” shall be maintained in an offsite safety deposit box in a bank that maintains a log of all access to the box.

6.8.1. Assignment and possession of keys to the safety deposit box shall be controlled by the Security Policy Committee.
6.9. Customer Password Reset Requests: See the section of this document titled “Client Inquiries”.

6.10. System IDs, Passwords, and Logins

6.10.1. Definition: System IDs (i.e. software system user IDs) and passwords are logins that software systems use to import, export, or provide access to data in Samaritan’s volunteer management systems via some sort of integration between the systems such as the Exchange API, the Samaritan Data Service, flat file transfer, and/or authentication systems such as LDAP, or SAML.

6.10.2. All systems that access a Samaritan volunteer management system are required to authenticate themselves via a system ID and password.

6.10.3. All System IDs must be unique for each system or integration.

6.10.4. System IDs must not be available for human use.

6.10.5. All system passwords are subject to the requirements of sections 6.4.3.1, 6.4.3.2, 6.4.3.3 of this document.

6.10.6. All system passwords are to be strong passwords as defined in this document.

6.10.7. System IDs and passwords shall not be scripted into any application or source code. They are to be stored in the same manner as human user IDs and passwords.

6.11. All access via a user ID or system ID and password is to be limited to the functionality and data for which the person or system has an authorized business need.

7. Privacy Policy

7.1. Samaritan’s Privacy Policy can be found in section 5 of the Samaritan Technologies Subscription and Services Agreement. It is as follows:

Section 5 - Customer Data and Confidentiality

5.1 Customer Data. “Customer Data” means the data of Customer that are transmitted by Customer or an Authorized User to Samaritan’s Computers as part of the licensed use of Licensed Software. Transmitting of Customer Data must be in accordance with Samaritan's then-current reasonable specifications and guidelines. Such Customer Data will be kept confidential by Samaritan (and its contractors, if any), subject to Section 5.2 below. Customer warrants that Customer Data and the transmitting and storage of such data will not infringe, misappropriate or violate the rights or intellectual property of any third party. Customer is responsible for the accuracy, integrity, completeness and content of Customer Data.

5.2 Privacy.
(a) **Use of Customer Data for Statistical Purposes:** Samaritan may extract data (including Customer Data) stored on Samaritan Servers and compile or create general bulk statistical information about volunteerism and other subjects, and may publish, copy, use, distribute, license and/or sell such general bulk statistical information and authorize others to do so. Such general bulk statistical information must not include PII, PHI, or PCI.

(b) **Individual and Organization Information:** Except as described below (Shared or Published Information) or as required by law, regulation or order of a court or government entity, Samaritan will not disclose, reveal, share, or sell any PII, PHI, or PCI in Customer Data about any individual including name, address, telephone number, or email address, nor will Samaritan disclose any statistical information in Customer Data that identifies any specific individual volunteer or organization without that volunteer's or organization's prior written approval.

(c) **Shared or Published Information:** Samaritan's eCoordinator™ and eRecruiter™ software and services are specifically designed for the purpose of easily sharing volunteerism information. Once Customer chooses to share, disclose, or publish such information, including, but not restricted to, information about individual volunteers, clients (recipients of volunteer service), service opportunities, or organizations by using Samaritan's software, Samaritan is not responsible for the use, disclosure or publication of the information by or to its recipients. Customer also acknowledges that once such information has been shared, disclosed or published it cannot be retrieved even if Customer should later desire to do so.

5.3 **Confidential Information of Customer.** Samaritan (and its contractors, if any) will keep confidential, and will not use except in the performance of Services, any other information (i.e., information other than Customer Data) disclosed by Customer to Samaritan in connection with the Services, provided that such other information when given to Samaritan is marked or identified in writing as “Confidential” or “Proprietary.” If Customer discloses such other information orally to Samaritan, and if Customer desires to have such other information protected under this Section 5.2, then Customer must reduce such other information to writing, mark it as “Confidential” or “Proprietary” and deliver such writing to Samaritan within two weeks of the first oral disclosure of such other information to Samaritan. This requirement does not apply to Customer Data.

5.4 **Confidentiality of Samaritan Information.** Customer will keep confidential, and will not use for any purpose other than this Agreement, any information disclosed by Samaritan to Customer about, or that is learned or observed by Customer from, the technologies, methodologies, equipment, software and processes used by Samaritan as well as the Licensed Software, Client Software, Documentation, and Services. Customer will ensure that its employees, agents, representatives and contractors comply with these obligations. Any exceptions to this paragraph may
only be granted in writing by Samaritan. This paragraph will not prohibit the Customer from making
general comments regarding its user experiences with Services and Licensed Software.

5.5 **Exceptions.** Neither Party will have any obligation under Sections 5.3 and 5.4 above
with respect to information that is publicly known at the time of first disclosure to the receiving Party
or that is in the receiving Party’s possession prior to first disclosure by the disclosing Party to the
receiving Party. If through no fault of the receiving Party, any confidential information of the disclosing
Party subsequently becomes publicly known, then the receiving Party will thereafter have no obligation
under Section 5.3 or 5.4 with respect to such publicly known information. If any information is lawfully
disclosed or licensed by a third party to a receiving Party, then Sections 5.3 and 5.4 will not restrict the
receiving Party from making any use or disclosure thereof that is lawfully authorized by the third party.
If any disclosure of confidential information is required by law, government regulation, or court order,
the receiving Party may make such disclosure, but the receiving Party must first give notice thereof to
the disclosing Party and cooperate with the reasonable request of the disclosing Party, at the disclosing
Party’s expense, in seeking and obtaining any protective orders or other protections that might be
available. This Section does not apply to or excuse any infringement of copyrights or patent rights.
Notwithstanding anything to the contrary, Samaritan has no obligation or restriction with respect to
any Feedback - see Section 5.8 below.

7.2. **Data Classification, Data Encryption and Data Security**

7.2.1. All transmissions of customer data between the eCoordinator databases and client
browsers are to use 128 bit or higher (preferable) TLS 1.2 or higher encryption.

7.2.2. All transmissions of customer data using the Exchange API are encrypted using 128
bit or, preferably, higher TLS 1.2 or higher encryption.

7.2.3. **Sensitive Data:**

7.2.3.1. If a customer desires to store information such social security numbers or
driver license numbers and dates the Client Services team assigned to that
customer shall obtain written instructions from the customer as to which
individuals or roles are to be allowed access to such information.

7.2.3.2. Sensitive Personally Identifiable Information (PII): Volunteer identification
information such as social security numbers or driver license numbers and
expiration dates are to be stored using one of the two following methods:

7.2.3.2.1. A) The Identification Tab of the Volunteer Profile. The Identification tab is
primarily for PII related identification numbers such as Social Security
Numbers, driver license numbers, or passport numbers, and the
associated dates. Data stored on the Identification Tab are encrypted
in the database using 128-bit AES encryption. This method is
preferable as data stored on the Identification Tab are also excluded
from bulk volunteer information displays and reports as a precaution
against bulk data theft.

7.2.3.2.2. B) Secure User Defined Fields (UDFs). Secure UDFs make use of the
column-wise data encryptions capabilities built into Microsoft SQL
Server. Note that this method provides greater convenience and flexibility, but should be used with caution. As of this writing, this method permits the data to be displayed in bulk form in data grids and exported in bulk form via data grid reports.

7.2.3.3. Protected Health Information (PHI): PHI for volunteers should be stored using secure UDFs. PHI for clients (the recipients of volunteer service) should be stored on the Special Needs tab of the client profile which is also encrypted in the database using 128-bit AES encryption.

7.2.3.4. Payment Card Information (PCI):

7.2.3.4.1. In general Samaritan’s system is not intended for and should not be used for the storage of PCI. In rare cases, a customer may request that our systems be integrated with a system which volunteers or clients may use to pay fees. In such cases PCI should be passed immediately to the payment system as part of the browser level JavaScript integration without ever being transmitted to or stored on Samaritans servers.

7.2.3.5. The Account Management System (AMS) Functional Features controls are to be used to limit access to the Volunteer Profile Identification Tab and Secure UDFs to those individuals or roles that the customer has indicated should have access to such data.

7.2.4. All unencrypted transmissions of data between the Samaritan eCoordinator database servers are performed over private network connections that are not exposed to the Public Internet.

7.2.5. Authentication between the eCoordinator database and application servers is required for inter-server data transmission.

7.2.6. All transmissions of sensitive data, including all Customer Data (not just PII, PHI, and PCI) to and from Samaritan’s production application servers are to be accomplished via one of the following secure means:

7.2.6.1. eCoordinator, eRecruiter, Sign-In, or the Exchange API using 128 or higher bit TLS 1.2 or higher encryption (HTTPS). Each of these methods also requires user id and password authentication

7.2.6.2. FTPS from specific IP addresses only via a firewall configured for this purpose.

7.2.6.3. For Samaritan internal use only, Microsoft Remote Desktop Protocol with transport layer encryption enabled for Microsoft Windows servers from specific IP addresses only via a firewall configured for this purpose.

7.2.6.4. For Samaritan internal use only, SSH for Linux servers.
7.2.6.5. Bulk data files for import or export are to be encrypted before transmission with an encryption protocol (minimum 256 bit) agreed upon by Samaritan's development team leader and the internal or external party exchanging data.

8. Client Inquiries

8.1. When a client requests confidential information or a password reset do the following:

8.1.1. Verify the identity of the requestor by asking for the following information:

8.1.1.1. The requestor’s eCoordinator userID as stored on the Clients tab in their account in AMS.

8.1.1.2. Verify their telephone number and zip code as stored in Samaritan’s customer service database.

8.1.1.3. If you are uncertain of the identity of the caller, call them back at the phone number listed in Samaritan’s customer support database.

8.1.2. Confirm that the requestor has a legitimate need to know the information that they are asking for or action you are to perform.

8.1.3. A record of the request is to be entered into Samaritan’s customer service database and should record the following information:

8.1.3.1. The Requestor’s Name

8.1.3.2. The things you did to verify the requestor’s identity

8.1.3.3. The stated need

8.1.3.4. The information requested

8.1.3.5. The information provided or action performed.

8.1.3.6. Your name and the date you assisted the customer with the request.

8.2. Administrator resets of eCoordinator or AMS passwords should be configured to require change on first subsequent login by the user.

9. Authorized Access to Customer Data

9.1. The following job titles are granted access to Customer Data as described in the following table. Individual access is granted by the Vice President of Operations or his/her supervisor. (See the Samaritan Technologies Data Classification and Security Policy document.) In each case access to Customer Data is to be limited to the specific customers or accounts assigned to the individual by Vice President of Operations.

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Range of Access</th>
<th>Duration of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Accounts Access</td>
<td>Duration</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Vice President of Operations</td>
<td>All accounts</td>
<td>Until change of position or employment</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>All accounts</td>
<td>Until change of position or employment</td>
</tr>
<tr>
<td>Client Services Representative</td>
<td>Assigned accounts only</td>
<td>Until change of position or employment or account assignment</td>
</tr>
<tr>
<td>Account Manager</td>
<td>Assigned accounts only</td>
<td>Until change of position or employment or account assignment</td>
</tr>
<tr>
<td>Corporate Relations Manager</td>
<td>Assigned accounts only</td>
<td>Until change of position or employment</td>
</tr>
<tr>
<td>Implementation Manager</td>
<td>Assigned accounts only</td>
<td>Until implementation or update is complete</td>
</tr>
<tr>
<td>Front End Developer</td>
<td>Assigned accounts only</td>
<td>Until implementation or update is complete</td>
</tr>
<tr>
<td>Development Team Leader</td>
<td>All Accounts</td>
<td>Until change of position or employment</td>
</tr>
<tr>
<td>Assistant Development Team Leader</td>
<td>All Accounts</td>
<td>Until change of position or employment</td>
</tr>
</tbody>
</table>

### 10. Unauthorized Access of Customer Data

10.1. All known incidents of unauthorized access of Customer Data are to be reported to immediately to the following people:

- The client service team leaders for any clients possibly affected by the breach;
- The vice president of client services; and
- A member of the Samaritan Security Policy Committee.

The Security Policy Committee Chairman will then convene a Data Breach Response team to address the issue as described in the *Samaritan Data Breach Response document*. 
10.2. A record of the report including the following information is to be recorded in the client’s account history in Samaritan’s customer service database and filed with the Security Policy Committee which shall maintain a log of all such incidents and reports:

10.2.1. The nature of the unauthorized access,
10.2.2. The type and quantity of data accessed if known,
10.2.3. Who the data was disclosed to if known,
10.2.4. Any damage to the client data that occurred if known,
10.2.5. The client contact person that was informed of the unauthorized access,
10.2.6. The time, date and method by which the client was informed,
10.2.7. Any special instructions or requests that were made by the client in response to the notice of unauthorized access.

10.3. Retention of Records

10.3.1. Rackspace is to be contacted immediately and asked to retain all backups of the server data for the period immediately preceding and following the unauthorized client data access.

10.3.2. All retained backups, records and data are to be kept until the Security Policy Committee authorizes their re-use or destruction.

10.3.3. Other than for forensic requests Customer data is to be retained only for the minimum amount of time required by law.

11. Termination of Employment or Partner Status

11.1. Upon departure from the company all access to the following systems is to be removed for the departing person. Note this is a generic list. Specific accounts and systems are listed in Appendix A to this document.

11.1.1. Email
11.1.2. On-line file storage
11.1.3. On-line calendars
11.1.4. On-line customer relationship management systems
11.1.5. On-line accounting systems
11.1.6. On-line customer service systems
11.1.7. The internal only sections of the Samaritan knowledge-base.
11.1.8. Web hosting

11.1.9. Root access to any and all servers

11.1.10. FTP access to any and all servers

11.1.11. AMS (Account Management System)

11.1.12. RMS (Recruiter Management System)

11.1.13. Account Information Tool

11.1.14. eCoordinator accounts

11.1.15. Authorization as a Rackspace contact

11.1.16. On-line advertising accounts

11.1.17. On-line bank accounts

11.1.18. On-line time tracking accounts

11.1.19. On-line project management accounts

11.1.20. Domain registration accounts

11.1.21. Company credit cards

11.1.22. Phone system and voice mail

11.1.23. All physical locks to our offices are to be changed

11.1.24. Desktop and Notebook passwords

11.1.25. Safety deposit box access and keys

11.2. Responsibility for removing the access to the system belongs to the prior (to termination) supervisor of the terminated employee.

11.3. If possible access to the above systems and any specific systems listed in Appendix A should be removed within 24 hours after, if not prior to, termination. All access changes should be completed within a maximum one week of termination or the change in the employee’s responsibilities.

11.4. Uninformed absence: If an employee or contractor has an uninformed absence lasting five days or more the above procedures should be implemented as if the employee had been terminated and customers with which the employee was activity engaged will be informed of the uninformed absence, the removal of the absent employee’s systems access, and contact information for the person who has been assigned as a replacement.
12. **Restricted and Confidential Data Protection**

12.1. This section addresses the following items:

12.1.1. Procedures and controls for the generation, distribution, tracking, storage, and destruction of Restricted and Confidential documents;

12.1.1.1. A log of all restricted and confidential documents is to be maintained by a staff member assigned by the Security Policy Committee.

12.1.1.1.1. The log should record

12.1.1.1.1.1. Who has the document
12.1.1.1.1.2. The title of the document
12.1.1.1.1.3. The person delivering the document
12.1.1.1.1.4. The owner/originator of the document
12.1.1.1.1.5. The expiration date of the document

12.1.1.1.2. The log should be reviewed at least twice per year by a member of the Security Policy Committee for a review of expiration dates and the need to destroy expired documents.

12.1.2. Restricted and confidential documents should be kept in a locked drawer or cabinet.

12.1.3. Policies for the destruction of Restricted and Confidential information at the end of its life cycle.

12.1.3.1. All paper documents are to be shredded or burned.
12.1.3.2. All floppy disks or optical media are to be crushed.
12.1.3.3. Backup media is to be destroyed at the end of its useful life.
12.1.3.4. Production storage systems containing customer data is to be certifiably erased when no longer used.
12.1.3.5. Customer data received for data conversions is to be deleted from local PCs once the data conversion project is completed and the production data has been verified by the customer.
12.1.3.6. Local PC disks should be degaussed or destroyed (e.g. solid state storage devices) when retired from service.

13. **Office Physical Security**
13.1. Samaritan has a “clean desk” policy:

13.1.1. Desktops are to be cleared of all documents when not occupied.

13.1.2. The clean desk policy is enforced via spot audits by the company security officer.

13.2. The main entrance to Samaritan’s office suite should be locked after business hours or whenever the office suite is unoccupied such as during “all hands” meetings in the conference room.

13.3. The operations manager’s office is to be locked whenever the operations manager is off premises.

13.4. All visitors are to sign-in and sign-out on the log in the reception area.

13.5. The visitor log / guest register sheets are to be retained for at least six months.

13.6. The visitor log / guest register sheets are to be reviewed weekly by a member of the security committee, the vice president of operations, or their designees.

13.7. All visitors are to be escorted while on premises at our offices.

13.8. The entrances to Samaritan’s building, its office suite, and the operations manager’s office are to all be separately keyed.

13.9. The rear entrance to the building hosting Samaritan’s offices is to be locked outside of business hours.

13.10. The front entrance to the building hosting Samaritans office is to be locked outside of business hours.

13.11. The entrance to Samaritan’s office suite is to be protected by video surveillance. The video surveillance recordings are to be retained for at least two weeks.

13.12. The Vice President of Operations is to maintain a log of all repairs and modifications to the physical security of Samaritan’s office suite. At a minimum this log should record a description of the modification, the date of the modification, and who the modification was performed by.

14. Office Computer Security

14.1. Management assignment or approval is required for employees or consultants to use any company networking and computing resources.

14.2. All access to office computers must require authentication in compliance with the password policies in this document.

14.3. Anti-virus software is to be installed on all individual use computers and office servers where the operating system permits it.
14.3.1. Personal computer anti-virus software should be configured for either continuous scanning or nightly scanning.

14.3.2. Server anti-virus software should be configured to scan all file updates.

14.3.3. Anti-virus software should be configured to check for updates daily or more frequently.

14.4. All computers are to be configured to lock their desktops after a maximum of thirty minutes of inactivity.

14.5. By default all logins to Samaritan’s software accounts are to automatically log off a session after 20 minutes of inactivity. This timeout shall be adjustable via the AMS Info tab or the RMS Options tab. Customer administrative users are to be informed that this is a configurable parameter.

14.6. Firewalls are to be installed for all office servers.

14.7. When decommissioned, all hard disks under Samaritan control are to be erased using a commercially available multi-pass overwrite data erasure program specifically designed for the removal of confidential information.

14.8. All office computers should be configured to obtain standard time synchronization from time.windows.com.

14.9. All company email correspondence should make use of the company’s https encrypted email system.

15. **Office Wireless Security**

15.1. The settings of all office wireless network routers are to be included in each semi-annual audit.

15.2. Encryption should be enabled for all wireless network traffic.

15.3. Stateful Packet Inspection (SPI) filtering should be enabled.

15.4. The default password for the router should be changed.

15.5. Remote administrative login should be disabled.

15.6. The router’s firewall should be enabled.

15.7. All unnecessary ports should be disabled via the router’s firewall.

15.8. Network Address Translation (NAT) should be enabled.

15.9. The wireless router should be configured to obtain standard time synchronization from ntp.org.
16. **Mobile Code Security Policy**

16.1. Disable Java in Java enabled browsers except where absolutely necessary for applications that require it.

16.2. Anti-virus software should be configured to scan all web pages and unregistered executables before execution.

17. **Removable Media**

17.1. Only company supplied removable media us to be used for work purposes.

17.2. Only company supplied numbered individually assigned encrypted and logged USB Flash drives are to be used. For further information See the *Samaritan Technologies Data Classification and Security* document for more information.

17.3. All removable media that is used for work purposes is to be approved by and registered with Infosec.

17.4. Personal and work information are not to be stored on the same removable media devices.

17.5. All removable media should be included in your PC anti-virus scans.

17.6. Assigned removable media devices will be returned to Infosec upon termination.

18. **Security When Working Off Premises**

18.1. All notebook computers and devices (such as phones or tablets) used for company work must be password protected.

18.2. Company data and documents should not be stored on individual notebooks. Instead they should be stored on company provided, numbered, individually assigned, encrypted and logged USB flash drives.

18.3. Recovery passwords for company issued USB flash drives are not to be stored on the devices that the flash drives are used on.

18.4. Caution should be used to avoid the use of unsecured networks if at all possible while traveling.

19. **Production Server Security**

19.1. All production servers under Samaritan’s control are to be housed in professional grade data centers separate from Samaritan’s local office network.

19.2. Production servers are to only host applications that are part of Samaritan’s commercial offerings or applications for ensuring the availability and security of those offerings or applications otherwise necessary for the operation of those offerings. No
other applications should be installed or resident on production servers. Production servers are not to be used for Samaritan’s websites or business applications.

19.3. All remote administrative server access is to be performed via secure protocols such as SSH or RDP. “Split tunneling” of VPN or other remote connections is not permitted.

19.4. All production server administrative passwords are to be limited to those who have a specific need for server administrative access including the development team leader, the assistant development team leader, the quality assurance manager, the company security officer, and the on-site data center technicians responsible for the server maintenance except for the servers of dedicated server or self-hosted server customers in which case the customer shall dictate which individuals have administrative server access.

19.5. Access to all production servers must require authentication (i.e. at least a username and password).

19.6. All anonymous FTP access to the server is to be disabled.

19.7. All anonymous database SQL query capability is to be disabled.

19.8. All database query capability must be authenticated and is limited to Samaritan’s production applications, the development team leader, the assistant development team leader, the quality assurance manager, and the company security officer except for the servers of dedicated server or self-hosted server customers in which case the customer shall dictate which individuals have database query capability.

19.9. Firewalls are to be used to protect all servers containing or involved in the processing of customer data for which Samaritan has responsibility.

19.9.1. Firewall rules should specifically exclude remote server administrative access except for the IP addresses of those individuals that are permitted administrative server access.

19.9.2. Firewall rules should specifically exclude all FTP access except for the IP addresses of those individuals who have been authorized to have such access.

19.10. All FTP access must be authenticated.

19.11. All FTP access should be restricted to a specific to the servers and set of folders that are appropriate for the work being done by the person who has been granted access.

19.12. Anti-virus software is to be installed on all servers where the operating system permits it.

19.12.1. The anti-virus software should be configured to scan all file updates.

19.12.2. The anti-virus software should be configured to check for updates daily or more frequently.
19.13. All ports which are not essential to a server’s operation are to be disabled.

19.14. All process and applications which are not essential to the server operation are to be disabled.

19.15. For policies and procedures regarding production server availability and recoverability see the document *Summary of Samaritan’s Disaster Prevention and Event Response Plan*.

19.16. Port availability monitoring is to be enabled on all production servers which house client data and are under Samaritan control.

19.17. eCoordinator application availability monitoring is to be run on an on-going basis for all eCoordinator servers.

19.18. All server hard disks at Rackspace or SoftLayer are to be disposed of in a manner consistent with Rackspace’s or SoftLayer’s policies for the safeguarding of such expired restricted and confidential information.

19.19. The use of utility programs capable of potentially overriding system, object network, virtual machine and application controls is strictly prohibited unless specifically authorized by Infosec.

19.20. The semi-annual production server audit should include checks for the following:

   19.20.1. Unsuccessful login attempts
   19.20.2. Repeated password changes for a specific user ID
   19.20.3. account lock-out and resets
   19.20.4. Actions that disable security features (e.g., OS patches, antivirus)
   19.20.5. Actions that modify logging features or result in deletion of logs
   19.20.6. Software installations

19.21. Activity to hypervisor functions and administrative consoles should be logged and reviewed daily the development team leader.

20. **Security and Development**

20.1. All system requirement specification documents are to include a section specifically addressing security issues associated with the systems they describe.

20.2. All new feature requests entered into the Jira database are to include a section specifically addressing security issues and requirements associated with the feature they describe.
20.3. With the exception of a data migration test database located on the same physical server as the production system to be migrated or on a replacement server for the production system, production data is not to be copied into a test environment.

21. Law Enforcement Contact Information

21.1. Salt Lake City FBI Office:

5425 West Amelia Earhart Drive
Salt Lake City, UT 84116
Phone: (801) 579-1400
Fax: (801) 579-6000
E-mail: SaltLakeCity@ic.fbi.gov

21.2. Utah Statewide Information & Analysis Center (SIAC)

410 West 9800 South, Suite 370
Sandy, Utah 84070
(801) 256-2360
SIAC@utah.gov

21.3. Report Suspicious Activities (SARS) to SARS@Utah.gov


21.5. Internet Crime Complaint Center (IC3)

TO file a complaint to IC3, go to the following URL and fill out the form at http://www.ic3.gov/default.aspx.
22. **Financial Security**

22.1. Weekly reviews of all credit card and checking account activity are to be held by the Chief Executive Office, the Vice President of Operations, and the head of the accounting department.

23. **Related Statutes and Policies**

23.1. Governmental regulations: At a minimum, Samaritan’s operations should be consistent with the following laws and governmental policies as are appropriate for the services that Samaritan offers:


23.1.2. HIPAA: [http://www.hhs.gov/hipaa/for-professionals/index.html](http://www.hhs.gov/hipaa/for-professionals/index.html)


23.1.4. California’s Electronic Communications Privacy Act: (requires warrants before disclosure of personal information) [https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178](https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178)


23.1.6. Canada - Personal Information Protection & Electronic Documents Act (PIPEDA): [https://www.priv.gc.ca/leg_c/leg_c_p_e.asp](https://www.priv.gc.ca/leg_c/leg_c_p_e.asp)


23.1.8. An excellent summary of most of these laws can be found here: [https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675](https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675)

23.2. **Related Samaritan Policy and Technology Documents:**

23.2.1. Samaritan Technologies Data Breach Response Policy

23.2.2. Samaritan Technologies Disaster Prevention and Event Response Policy

23.2.3. Samaritan Technologies Data Encryption

23.2.4. Samaritan Asset Management Policy

23.2.5. Samaritan Software Change Management and Release Process
24. Approved Software

24.1. The following software applications are approved by default (i.e. whitelisted). Items not on this list should be approved by Infosec before installation:

24.1.1. Microsoft Word
24.1.2. Microsoft Excel
24.1.3. Microsoft PowerPoint
24.1.4. Microsoft Visio
24.1.5. Google Gmail
24.1.6. Google Calendar
24.1.7. Google Chrome
24.1.8. Google Drive (only Samaritan’s own account for company data)
24.1.9. Google Sheets
24.1.10. Google Docs
24.1.11. Mozilla FireFox
24.1.12. Windows 7
24.1.13. Windows 10
24.1.15. Microsoft Edge
24.1.16. Atlassian Jira
24.1.17. Zen Desk
24.1.18. Samaritan eCoordinator
24.1.19. Samaritan eRecruiter
24.1.20. Samaritan Coordinator CS
24.1.21. Basalmic
24.1.22. TechSmith Snagit
24.1.23. Microsoft Paint
24.1.24. Apple Safari
24.1.25. Apple OS X

25. Additional Items to address if not already covered

25.1. Employee access log for recording all system access granted to each employee.
25.2. Employee access audit log with remediation actions taken.
25.3. List of employees with access to modify server and network configurations.
25.4. Default whitelist of approved software.
   25.4.1. Process for periodic review of software installed on Samaritan computers including comparison to entitlements and removal of any non-approved software.
25.5. Mobile Code Security Policy
   25.5.1. Disable Java in Java enabled browsers
   25.5.2. Anti-virus to scan all web pages and unregistered executables before execution.
25.6. Policy for disabling staff access to a project when no longer assigned to that project.
25.7. Client notification of unapproved absence for staff assigned to a client project.
25.8. Items to audit and log:
   25.8.1. AMS access to each instance
25.9. Server remote access policy
   25.9.1. Allowed methods
   25.9.2. Requirements
   25.9.3. Disallowed methods
      25.9.3.1. Split access
Appendix C: Service Level Agreement – Samaritan Hosted System

1.0 General

This Service Level Agreement ("SLA") sets forth the service level credits available to Customer for Critical Outage Events and Response Time failures.

For purposes of this SLA, the first “contract year” is the Initial Term. Each one year Renewal Period is also a “contract year.”

2.0 Critical Outage Events

The SLA target is a level of Zero Critical Outage Events during any contract year.

A Critical Outage Event is an unscheduled outage event or series of intermittent unscheduled outage events that result from an Error in the Licensed Software that causes the Licensed Software, or a major functional component thereof, or Customer Data on Samaritan Servers to become unavailable to Customer for a total of eight (8) or more hours within a single twenty-four (24) hour period beginning at the start of the first outage event during the twenty-four hour (24) period. For purposes of the calculation of credits under Section 5: (a) there will be no more than one Critical Outage Event during any twenty-four (24) hour period, (b) there will be no overlapping of such periods or Critical Outage Events; and (c) a maximum of one Critical Outage Event may occur during any twenty-four (24) hour period.

3.0 Corrective Action - Critical Outage Events

Appropriate corrective action includes isolating and identifying the problem causing the Critical Outage Event, developing and implementing a corrective action plan, and communicating such plan to Customer. Alternatively, if necessary at Samaritan’s discretion, appropriate corrective action includes developing and implementing a temporary workaround solution. The action plan should specify the activities required to correct the Critical Outage Event, the order and schedule of corrective actions required, and the Party responsible for performing each corrective action. Each Party will execute the activities assigned to it in the plan. No unreasonable assignment will be made to Customer. Samaritan will monitor the progress made in executing the plan and will provide regular status reports to Customer until the Critical Outage Event is corrected. In order to expedite the corrective actions for a Critical Outage Event, Samaritan may present or make available its corrective action plan and record of actions taken in the form of an “after action” report after access to the Licensed Software and Customer Data has been restored.

Customer will expeditiously work and cooperate with Samaritan to provide any information and
assistance reasonably necessary to demonstrate the effects and causes of the Critical Outage Event in a repeatable manner and to develop and implement a corrective action plan.

4.0 Response Time

Samaritan shall exercise commercially reasonable efforts to correct any Error reported by Customer in accordance with the priority level reasonably assigned to such Error by Samaritan. The following definitions will apply to such prioritization:

“Priority 1 Error” means an Error that renders the Licensed Software inoperative or causes the Licensed Software to be unavailable or unusable.

“Priority 2 Error” means an Error, other than a Priority 1 Error, that results in the loss of any major or significant feature or functionality of the Licensed Software or in a significant degradation of the performance of Licensed Software or that significantly restricts Customer’s use of the Licensed Software.

“Priority 3 Error” means an Error, other than a Priority 1, 2, or 4 Error, that results in the loss of any other feature or functionality of the Licensed Software.

“Priority 4 Error” means an Error that has a negligible or insignificant impact on Customer’s use of the Licensed Software.

PRIORITIZED RESPONSE TIMES

<table>
<thead>
<tr>
<th>PRIORITY 1 ERRORS:</th>
<th>TIME TO RESPONSE</th>
<th>TIME TO REPAIR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 business day</td>
<td>2-5 business days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PRIORITY 2 ERRORS:</th>
<th>TIME TO RESPONSE</th>
<th>TIME TO REPAIR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 business day</td>
<td>5-10 business days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PRIORITY 3 ERRORS:</th>
<th>TIME TO RESPONSE</th>
<th>TIME TO REPAIR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 business days</td>
<td>As scheduled for correction and implementation by Samaritan</td>
</tr>
</tbody>
</table>
Repair means to correct the Error or provide a reasonable work-around solution consistent with sections 3.2 and 7.8 of the Software and Services Subscription Agreement.

**ESCALATION PATH FOR EMERGENCIES**

<table>
<thead>
<tr>
<th>Order</th>
<th>Person</th>
<th>Contact Type</th>
<th>Phone/Pager (Duty Pager)</th>
<th>Elapsed Time to Escalate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Customer service contact assigned at contract execution</td>
<td>Client Services</td>
<td>801-328-3972 ext. 4</td>
<td>Next Business Day</td>
</tr>
<tr>
<td>2</td>
<td>Customer service contact assigned at contract execution</td>
<td>Client Services</td>
<td>801-328-3972 ext. 203</td>
<td>1 Business Day</td>
</tr>
<tr>
<td>3</td>
<td>Keith Leonard</td>
<td>VP Operations</td>
<td>801-328-3972 ext. 201</td>
<td>1 Business Day</td>
</tr>
<tr>
<td>4</td>
<td>Bruce Behymer</td>
<td>Product Development</td>
<td>760-809-6589</td>
<td>1 Business Day</td>
</tr>
</tbody>
</table>

The above listed individuals are to be contacted only during the support hours specified by Customer’s selection of support CLINs from Appendix B. Note that the specific individuals
named above may be replaced by other individuals at Samaritan’s selection and convenience upon notice to Customer.

5.0 Credits

Samaritan will provide a “one (1) day credit” for each unscheduled Critical Outage Event during a contract year (“Critical Outage Event Credit”). Customer will not be eligible to receive multiple Critical Outage Event Credits for the same or overlapping twenty four (24) hour period(s) of time. The cap on Critical Outage Event Credits equals a total of ten “one (1) day” credits per contract year. In no event will the total credits for Critical Outage Events for any contract year exceed this cap.

Samaritan will provide a “one (1) day credit” for each Error reported by Customer for which Samaritan does not respond to Customer within the time specified by the Prioritized Response Times table above (“Response Time Credit”). The cap on Response Time Credits equals a total of ten “one (1) day” credits per contract year. In no event will the total credits for Response Time for any contract year exceed this cap.

A “one (1) day credit” means X divided by Y, where X equals the sum of the Annual Subscription Fee and Annual Support Fee for the applicable contract year and Y equals the number of days in the applicable contract year.

Any Critical Outage Event Credits due may be paid directly to Customer or may be applied toward any outstanding balance owed by Customer.

Credits will not be given if the Critical Outage Event or Error is caused by or attributable to (i) any conduct or action of the Customer or its users including, without limitation, their negligence or misconduct, (ii) the initiation of any outages requested by Customer, or the implementation or installation of any scripts, applications, equipment, or services requested by Customer, where such request is characterized to Samaritan as “urgent” in writing (which may be by email) by at least one of Customer’s contacts listed in Appendix C, (iii) maintenance outages scheduled in advance by Samaritan, or (iv) Force Majeure as defined in the Software and Services Subscription Agreement. Customer will reimburse Samaritan for outage fees, service level credits and other payments, if any, owed to Samaritan’s other customers for outages or errors that occur as a result of item (i) or (ii).
Customer’s right to terminate the Software and Services Agreement under Section 3.0 above and any credits due Customer under this SLA will be the sole and exclusive remedy of Customer for any claim relating to outages or response times.

6.0 Security Shut-Downs

Credit will not be given for any events resulting from an interruption or shut down of the Licensed Software due to circumstances reasonably believed by Samaritan to be a significant threat to any of the following: the normal operation of the Licensed Software or services to other customers, or the Samaritan Servers, or access to or integrity of Customer Data or the data of other customers (e.g., hacker or virus attack). In the event of such an interruption or shutdown, Samaritan will return the Licensed Software to normal operation as soon as reasonably practicable in accordance with its reasonable business judgment.
Appendix D: Data Classification & Security Policy

Version 1.0

2 September 2016

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 September 2016</td>
<td>Bruce Behymer</td>
<td>Initial draft.</td>
</tr>
</tbody>
</table>

Overview

At Samaritan Technologies we offer several web-based volunteer management services and tools that interact with a database of volunteer, opportunity, organization, and logbook records. The information stored in these databases belongs to our clients. Thus, as providers of these services we are stewards and caretakers of their data and have a responsibility to protect its security. This document augments the data classifications of Personally Identifying Information (PII), Protected Health Information (PHI), and Payment Card Information found in the Samaritan Security Policies and Procedures for keeping our data and our customer’s data safe and secure.

1. Audience

The intended audience for this document consists of all of Samaritan’s employees, consultants, and partners. As a team we all share the responsibility of looking out for our customer’s and Samaritan’s interests.

2. Policy

All Samaritan and Customer Data must be classified according to the Samaritan Technologies Data Classification Schema and protected according to Samaritan
Technologies Data Security Standards. This policy applies to data in all formats or media.

3. Data Classification Schema

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Three levels of data classification will be used to classify Samaritan and Customer Data based on how the data are used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

Data are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. For example, a volunteer database may contain a volunteer’s contact information as well as their social security number. Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

Samaritan Technologies Data Classifications

A. Public - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the Samaritan or our customers, affiliates, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:
   
   Samaritan’s public web site.
   
   Publically available opportunity listings on our customers’ eRecruiter websites.
   
   Publically available organization listings on our customers’ eRecruiter websites.

B. Internal - Data intended for internal Samaritan business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the Samaritan Technologies community. Unauthorized disclosure could adversely
Internal data generally have a low to moderate sensitivity. Examples include:

- Financial accounting data that does not contain confidential information.
- Customer support records.
- Information technology transaction logs.
- Employee and Human Resource records.
- Customer agreements.

C. **Confidential** - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the VPO is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the Samaritan or our customers, the personal privacy of individuals, or on compliance with federal or state laws and regulations or Samaritan contracts. Confidential data have a very high level of sensitivity. Examples include:

- Customer data supplied for data conversions.
- Social Security Numbers.
- Credit card numbers.
- Personally Identifying information (PII).

Although definitions vary from state to state many states include but don’t necessarily limit their definitions of PII, to the following: an individual's name; date of birth; address; telephone number; driver's license number or card or non-driver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information. For Samaritan’s purposes, PII also includes ones name in combination with a passport number.

- Passport number.
Personnel / Human Resource records.

Medical records (also referred to as Protected Health Information or PHI).

Authentication tokens (e.g., personal digital certificates, passwords, biometric data).

D. **Proprietary Data** - Classification of data provided to or created and maintained by Samaritan Technologies on behalf of a third party, such as a customer, government agency, or corporation, will vary depending on contractual agreements and/or relevant laws or regulations. **Customer Data is both confidential and proprietary.** In general, the classification and security standards for proprietary data owned by the third party will be defined by the third party. Proprietary data owned by Samaritan Technologies must be classified and protected according to Samaritan’s data classification policy and security standards. Individuals managing or accessing proprietary data are responsible for complying with any additional requirements and security policies and procedures specified by the third party owner on in agreements such as the *Samaritan Technologies Software and Services Subscription Agreement* or a non-disclosure/confidentiality agreement. Proprietary data also include data classified by the federal government as Classified National Security Information (confidential, secret, top secret).

E. **Customer Data** – The following is from Samaritan’s standard software and services agreement:

“Customer Data” means the data of Customer that are transmitted by Customer or an Authorized User to Samaritan’s Computers as part of the licensed use of Licensed Software [from Samaritan].

Customer Data is both confidential and proprietary.

When Customer Data is received for a data conversion it should only be stored on numbered and individually assigned company issued encrypted flash drives. The drive should be encrypted using Microsoft BitLocker set to only encrypt the used portion of the drive. BitLocker recovery passwords are to be created and stored by the Vice President of Operations in a separate encrypted device or locked box. They are not to be stored in a file on the workstation where the flash drive was encrypted and will be used. New files will be automatically encrypted as they are added to the drive. If the Customer Data is to be transmitted it is to be stored in a password encrypted Microsoft Excel file during transmission with the password supplied to the recipient.
via a separate channel such as over the phone. At the end of the data conversion project or at the end of the flash drive’s life, the flash drive should be sanitized or disposed of per Samaritan’s Media Sanitization and Disposal Policy.

4. Data Security Standards

The following table defines required safeguards for protecting data and data collections based on their classification. Data security requirements for Proprietary Data are determined by the contracting organization and are therefore not included in the table below.

In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

<table>
<thead>
<tr>
<th>Security Control Category</th>
<th>Data Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public</td>
</tr>
<tr>
<td>Access Controls</td>
<td>Confidential, Proprietary (unless otherwise stated in an agreement), and Customer Data</td>
</tr>
<tr>
<td>No restriction for viewing.</td>
<td>Viewing and modification restricted to authorized individuals as needed for business-related roles.</td>
</tr>
<tr>
<td>Authorization by VPO or designee required for modification; supervisor approval also required if not a self-service function.</td>
<td>VPO or designee grants permission for access, plus VPO or designee grants permission for access, plus approval from supervisor.</td>
</tr>
<tr>
<td>Copying/Printing (applies to both paper and electronic forms)</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>System Security</td>
<td>Protection only with router ACLs acceptable.</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Virtual Environments</td>
<td>May be hosted in a virtual server environment.</td>
</tr>
<tr>
<td></td>
<td>All other security controls apply to both the host and the guest virtual machines.</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Should not share the same virtual host environment with guest virtual servers of other security classifications.</td>
</tr>
<tr>
<td>Physical Security</td>
<td>System must be locked or logged out when unattended. Host-based software firewall recommended.</td>
</tr>
<tr>
<td></td>
<td>Customer Data for data conversion may be stored in a locked office on a company issued encrypted flash drive until the data conversion is complete.</td>
</tr>
<tr>
<td></td>
<td>Physical access must be monitored, logged, and limited to authorized individuals 24x7.</td>
</tr>
<tr>
<td>Remote Access to systems hosting the data</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Storage on a secure server recommended. Storage in a secure Data Center recommended.</td>
</tr>
<tr>
<td><strong>Transmission</strong></td>
<td><strong>No restrictions.</strong></td>
</tr>
</tbody>
</table>
password using MS Word or Excel (File/Info/Permissions) and sent as an attachment with the password sent to the recipient via a different channel such as over the phone.

<table>
<thead>
<tr>
<th>Backup/Disaster Recovery</th>
<th>Backups required; daily backups recommended.</th>
<th>Daily backups required. Off-site storage recommended.</th>
<th>Daily backups required of server hosted data required. Off-site storage of server hosted recommended. Customer Data received for data conversions should not be copied or stored on any local media other than company issued encrypted flash drives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)</td>
<td>See Samaritan’s &quot;Media Sanitization and Disposal Policy&quot; Paper: no restrictions.</td>
<td>See Samaritan’s &quot;Media Sanitization and Disposal Policy&quot;.</td>
<td>See Samaritan’s &quot;Media Sanitization and Disposal Policy&quot;. Paper: See Samaritan’s &quot;Media</td>
</tr>
</tbody>
</table>
5. **Contracts with Third Parties**

Contracts between Samaritan and third parties involving Samaritan and Customer Data must include language requiring compliance with all applicable laws, regulations, and Samaritan policies related to data and information security; immediate notification of the SPCC and VPO if Samaritan and Customer Data is used or disclosed in any manner other than allowed by the contract; and, to the extent practicable, mitigate any harmful effect of such use or disclosure.
6. Definitions

ACL

Access Control List; a set of rules in a network device, such as a router, that controls access to segments of the network. A router with ACLs can filter inbound and/or outbound network traffic similar to a firewall but with less functionality.

Authentication

Process of verifying one's digital identity. For example, when someone logs into web-based email, the password verifies that the person logging in is the owner of the userID. The verification process is called authentication.

Authorization

Granting access to resources only to those authorized to use them.

Availability

Ensures timely and reliable access to and use of information.

Classified National Security Information

Information that has been determined by the federal government to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. There are three classifications - confidential, secret, and top secret (see White House Press Release: Classified National Security Information).

Confidentiality

Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Firewall

A specialized hardware and/or software system with stateful packet inspection that filters network traffic to control access to a resource, such as a database server, and thereby provide protection and enforce security policies. A router with ACLs is not considered a firewall for the purposes of this document.
IDS

Intrusion Detection System; a system that monitors network traffic to detect potential security intrusions. Normally, the suspected intrusions are logged and an alert generated to notify security or system administration personnel.

Integrity

Guards against improper modification or destruction of information, and ensures non-repudiation and authenticity.

IPS

Intrusion Prevention System; an IDS with the added ability to block malicious network traffic to prevent or stop a security event.

Local Network

Any segment of Samaritan’s data network physically located in Samaritan’s Salt Lake City office.

Remote Access

Accessing any Samaritan’s local network from any physical location outside the data center or Samaritan’s offices. This includes access from off premises using Samaritan’s VPN service.

Secure Data Center

A facility managed by full-time IT professionals for hosting computer, data storage, and/or network equipment with 24x7 auditable restricted access, environmental controls, power protection, and network firewall protection.

Secure Server

A computer that provides services to other computers, applications, or users; is running a server operating system; and is hardened according to relevant security standards, industry best practices, and Samaritan Technologies security policies.

Sensitivity
Indicates the required level of protection from unauthorized disclosure, modification, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. Adverse impact could be financial, legal, or on one's reputation or competitive position. The more sensitive the data, the greater the need to protect it.

**Samaritan Data**

Any data related to Samaritan Technologies functions that are:

A. Stored on company information technology systems.

B. Maintained by Samaritan Technologies staff, or sub-contractors.

C. Related to company processes on or off premises. This applies to any format or media (in other words, it is not limited to electronic data).

**VPN**

Virtual Private Network; a VPN provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

**7. Roles and Responsibilities**

Everyone with any level of access to Samaritan and Customer Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function. The following roles have specific responsibilities for protecting and managing Samaritan and Customer Data and Data Collections.

A. **Vice President of Operations (VPO)** – Responsible for overseeing all information assets. Has responsibility for overseeing a collection (set) of Samaritan and Customer Data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. The VPO is responsible for ensuring the proper classification of data and data collections under his/her control, granting data access permissions, appointing Data Managers for each Samaritan and Customer Data collection, making sure people in data-related roles are properly trained, and
ensuring compliance with all relevant polices and security requirements for all data for which they have responsibility.

B. **Security Policy Committee** – Members of this committee maintain the data classification schema and resolve data classification or ownership disputes.

C. **Data Manager** - Individuals authorized by the VPO to provide operational management of a Samaritan and Customer Data collection. The Data Manager will maintain documentation pertaining to the data collection (including the list of those authorized to access the data and access audit trails where required), manage data access controls, and ensure security requirements are implemented and followed.

D. **Data Processor** - Individuals authorized by the VPO or designee and enabled by the Data Manager to enter, modify, or delete Samaritan and Customer Data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.

E. **Data Viewer** - Anyone in the Samaritan community with the capacity to access Samaritan and Customer Data but is not authorized to enter, modify, or delete it.

F. **Security Policy Committee Chair (SPCC)** - Provides advice and guidance on information and information technology security policies and standards.

G. **Internal Audit Office** – Usually members of the Samaritan Security Policy Committee. They performs audits for compliance with data classification and security policy and standards.

### 8. Related Laws, Regulations, or Policies

Samaritan Technologies Policies

A. Samaritan Technologies Security Policies and Procedures
B. Samaritan Technologies Disaster Prevention and Event Response Plan Summary
C. Samaritan Technologies Software and Services Subscription Agreement
D. Samaritan Technologies Data Encryption
E. Samaritan Technologies Service Level Agreement
F. Samaritan Technologies IT Security Incident Management
G. Samaritan Technologies IT Security Incident Response Policy

Federal Legislation and Guidelines

A. Family Educational Rights and Privacy Act of 1974 (FERPA)
B. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
C. Gramm-Leach-Bliley Act (GLBA)
D. Electronic Communications Privacy Act of 1986 (ECPA)
E. NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization
F. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
G. NIST Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories
H. Executive Order 12958: Classified National Security Information, As Amended, March 2003

Other

- Payment Card Industry Data Security Standard (PCI DSS)

9. Questions/Waivers

The Security Policy Committee Chair (SPCC) is responsible for this policy. The SPCC or Vice President of Operations (VPO) or designee must approve any exception to this policy or related procedures. Questions should be directed to the SPCC.
Appendix E: Asset Management Policy

Version 1.0
29 August 2016

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 Aug 2016</td>
<td>Bruce Behymer</td>
<td>Initial draft.</td>
</tr>
</tbody>
</table>

Overview

Samaritan’s asset management policy guides how we purchase, maintain, and secure equipment and other assets. This ensures that purchases are made wisely, making the best use of our available resources, and that we protect these investments by insuring them, tracking their usage and maintaining them in good working order.

In managing our assets well, we also provide accountability to our members for the use of the assets for which they have been assigned usage rights.

10. Audience

The intended audience for this document consists of all of Samaritan’s employees, consultants, and partners. As a team we all share the responsibility of looking out for our assets and their usage.

11. Scope

This policy will apply to all equipment, software, licenses, buildings and other assets purchased by Samaritan for use by its employees, contractors, or partners.

12. Procedures

12.1. Purchasing of assets
12.1.1. The purchase of new equipment or other assets above a value of $50 will be approved by the vice president of operations, chief executive officer, or a department head with delegated budget authority from either of these officers.

12.1.2. The process for purchasing equipment and other assets will involve:

   12.1.2.1. Submitting an acquisition request to the vice president of operations, chief executive officer, or a department head with delegated budget authority from either of these officers.

12.2. **Maintaining a register of assets and assignments**

12.2.1. Assets will be entered in an asset register at the time of purchase and details of assets updated as required or as changes occur. It is the responsibility of the vice president of operations to oversee the maintenance of the asset register.

12.2.2. The asset register will include the following information for each asset:

   12.2.2.1. Asset Name
   12.2.2.2. Asset Description
   12.2.2.3. Serial Number
   12.2.2.4. Support Reference Number
   12.2.2.5. Date of approval
   12.2.2.6. Who approved the acquisition
   12.2.2.7. Who acquired the asset
   12.2.2.8. Date of acquisition
   12.2.2.9. The cost of the asset
   12.2.2.10. A reference to the insurance policy and number for the asset if relevant.
   12.2.2.11. The date the asset is decommissioned.
   12.2.2.12. Who decommissioned the asset.
   12.2.2.13. When the asset was disposed of.
   12.2.2.14. Who disposed of the asset.
   12.2.2.15. The method of disposing of the asset if applicable.
12.2.3. The asset register will include a history of the assignment of each asset including the following information:

12.2.3.1. The condition of the asset when assigned, noting any damage at the time of assignment.

12.2.3.2. The person the asset is assigned to.

12.2.3.3. The date of assignment.

12.2.3.4. Who made the assignment.

12.2.3.5. Any restrictions on the assignee’s usage of the asset.

12.2.3.6. The date that the asset was returned or access was revoked.

12.2.3.7. The condition of the asset upon return noting any new damage at the time of return.

12.2.3.8. Who received the asset when it was returned or who revoked the access to the asset.

12.2.3.9. Any additional notes relevant to the asset.

12.3. Insurance

12.3.1. All assets will be insured to the value of their replacement against fire, theft, burglary and accidental damage. It is the responsibility of the vice president of operations to see that each asset is properly insured and that the insurance is maintained.

12.4. Maintenance of assets

12.4.1. All major assets will be checked for repairs or replacements that may be needed on an annual basis. It is the responsibility of the vice president of operations to see that assignments are made for the performing the asset condition audit and that necessary repairs are made.

12.5. Security

12.5.1. All assets will be used in adherence to the Samaritan Security Policies and Procedures document.

12.5.2. It is the responsibility of the vice president of operations in conjunction with the Samaritan Security Policy Committee (Infosec) to see that each asset is hardened in a manner consistent with the requirements of the Samaritan Security Policies and Procedures document prior to the asset’s assignment and usage.
Appendix F: IT Security Incident Response Policy

Version 1.0
2 September 2016

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 September 2016</td>
<td>Bruce Behymer</td>
<td>Initial draft.</td>
</tr>
</tbody>
</table>

Overview

This policy governs the actions required for reporting or responding to security incidents involving Samaritan information, Client Data, and/or Samaritan information technology resources to ensure effective and consistent reporting and handling of such events.

13. Audience

The intended audience for this document consists of all of Samaritan’s employees, consultants, and partners. As a team we all share the responsibility of looking out for Samaritan’s and our customer’s interests.

14. Policy

All members of the Samaritan community are responsible for reporting known or suspected information or information technology security incidents. All security incidents at Samaritan must be promptly reported to the Samaritan Technologies Security Policy Committee Chairman and other appropriate company authority(ies) as outlined below in the section titled “Implementing Procedures”.

Incident response will be handled appropriately based on the type and severity of the incident in accordance with the Incident Response Summary Table below and Samaritan’s IT Security Incident Management Policy. Handling of security incidents involving confidential data will be overseen by an Executive Incident Management Team.

All individuals involved in investigating a security incident should maintain confidentiality, unless the Security Policy Committee Chairman (SPCC) authorizes information disclosure in advance.

15. Definitions

Security incident
Any real or suspected event that may adversely affect the security of Samaritan information or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person’s name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
- Violation of a Samaritan security policy
- Security weakness such as an un-patched vulnerability

**Personal identity information (PII)**

Samaritan defines PII as including, but not limited to: an individual's name; date of birth; address; telephone number; driver's license number or card or nondriver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information. For Samaritan's purposes, PII also includes ones name in combination with a passport number.

16. Roles and Responsibilities

A. The incident manager is responsible for managing the response to a security incident as defined in the incident response summary table below.

B. The Executive Incident Management Team oversees the handling of security incidents involving confidential data (e.g., personal identity information). This team has authority to make decisions related to the incident and to notify appropriate parties. The team consists of:

- Senior administrator for the affected unit
- Chief Information Officer
- Chief Information Security Officer
- Representative from the Office of General Counsel
- Assistant Vice President for Media Relations
- Others as needed (for example, Samaritan Police for criminal incidents)

17. Implementing Procedures
A. **Reporting Security incidents**
Any member of the Samaritan community who suspects the occurrence of a security incident must report incidents through the following channels:

All suspected high severity events as defined below, including those involving possible breaches of personal identity information, must be reported directly to the Security Policy Committee Chairman (SPCC) as quickly as possible by phone (preferred), e-mail, or in person. If the SPCC cannot be reached, contact the Vice President of Operations (VPO).

All other suspected incidents must also be reported to the SPCC. These incidents may be first reported to departmental IT support personnel, or the VPO who can then contact the SPCC. Reports should be made by sending email to security@samaritan.com (preferred) or by notifying the SPCC by phone, email, or in person.

For detailed information about reporting IT security incidents, see the Samaritan IT Security Incident Management Procedures.

B. **Responding to Security Incidents**

**Incident Severity**
Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of the company, its information, and its customers. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (Not Applicable).

a. **High**
The severity of a security incident will be considered "high" if any of the following conditions exist:

i. Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire company is affected)

ii. Poses a potential large financial risk or legal liability to the company or its customers

iii. Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)

iv. Adversely impacts an enterprise system or service critical to the operation of a major portion of the company or its customers (for example, e-mail, production information systems, financial information system, human resources information system, Internet service, or a major portion of the company network)

v. Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.

vi. Has a high probability of propagating to many other systems on site and/or off site and causing significant damage or disruption

b. **Medium**
The severity of a security incident will be considered "medium" if any of the following conditions exist:
i. Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
   ii. Adversely impacts a non-critical enterprise system or service
   iii. Adversely impacts a departmental system or service, such as a departmental file server
   iv. Disrupts a building or departmental network
   v. Has a moderate probability of propagating to other systems on site and/or off site and causing moderate damage or disruption

c. **Low**
   Low severity incidents have the following characteristics:
   i. Adversely impacts a very small number of systems or individuals
   ii. Disrupts a very small number of network devices or segments
   iii. Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

d. **NA (Not Applicable)**
   This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found.

**Incident Response Summary Table**
The following table summarizes the handling of IT security incidents based on incident severity, including response time, the responsible incident managers, and notification and reporting requirements. Detailed procedures for incident response and management are further defined in the Samaritan IT Security Incident Management Procedures.

<table>
<thead>
<tr>
<th>Incident Severity</th>
<th>Characteristics (one or more condition present determines the severity)</th>
<th>Response Time</th>
<th>Incident Manager</th>
<th>Who to Notify</th>
<th>Post-Incident Report Required*</th>
</tr>
</thead>
</table>
| High              | A. Significant adverse impact on a large number of systems and/or people
                    B. Potential large financial risk or legal liability to the Company or its customers | Immediate     | Security Policy Committee Chairman or an Executive Incident Management Team | A. Security Policy Committee Chairman
                    B. Vice President of Operations
                    C. Vice President of Client Services
                    D. Departmental security contact | Yes |

*Note: The table is truncated for clarity. Detailed procedures are included in the full document.*
<table>
<thead>
<tr>
<th>Level</th>
<th>A.</th>
<th>B.</th>
<th>C.</th>
<th>D.</th>
<th>E.</th>
<th>F.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Adversely impacts a very small number of non-critical individual systems, services, or people</td>
<td>Adversely impacts a non-critical enterprise system or service</td>
<td>Threatens confidential data</td>
<td>Adversely impacts a critical enterprise system or service</td>
<td>If breach of PII, see Samaritan Data Breach Response Policy and the Samaritan IT Security Incident Management Procedures for additional notification requirements</td>
<td>Technical support for affected device</td>
</tr>
<tr>
<td></td>
<td>Appointed by unit head</td>
<td>Disrupts a building or departmental network</td>
<td>Technical support for affected device</td>
<td>Significant and immediate threat to human safety</td>
<td>High probability of propagating to a large number of other systems on or off site and causing significant disruption</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Next business day</td>
<td>Technical support for affected device</td>
<td>Security Policy Committee Chairman</td>
<td>Medium</td>
<td>Adversely impacts a moderate number of systems and/or people</td>
<td>No, unless requested by the Security Policy Committee Chairman or other appropriate administrator</td>
</tr>
<tr>
<td></td>
<td>4 hours</td>
<td>Appointed by unit head</td>
<td>Vice President of Operations</td>
<td>Adversely impacts a non-critical enterprise system or service</td>
<td>Disrupts a building or departmental network</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vice President of Client Services</td>
<td>Adversely impacts a departmental scale system or service</td>
<td>Moderate risk of propagating and causing further disruption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Departmental security contact</td>
<td>Threatens confidential data</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Technical support for affected device</td>
<td>Adversely impacts a very small number of non-critical individual systems, services, or people</td>
<td>Adversely impacts a non-critical enterprise system or service</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security Policy Committee Chairman</td>
<td>Threatens confidential data</td>
<td>If breach of PII, see Samaritan Data Breach Response Policy and the Samaritan IT Security Incident Management Procedures for additional notification requirements</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vice President of Operations</td>
<td>Adversely impacts a departmental scale system or service</td>
<td>High probability of propagating to a large number of other systems on or off site and causing significant disruption</td>
<td>No, unless requested by the Security Policy Committee Chairman or other appropriate administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Departmental security contact</td>
<td>Threatens confidential data</td>
<td>Adversely impacts a critical enterprise system or service</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Technical support for affected device</td>
<td>Adversely impacts a very small number of non-critical individual systems, services, or people</td>
<td>Adversely impacts a non-critical enterprise system or service</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security Policy Committee Chairman</td>
<td>Threatens confidential data</td>
<td>If breach of PII, see Samaritan Data Breach Response Policy and the Samaritan IT Security Incident Management Procedures for additional notification requirements</td>
<td>No, unless requested by the Security Policy Committee Chairman or other appropriate administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vice President of Operations</td>
<td>Adversely impacts a departmental scale system or service</td>
<td>Moderate risk of propagating and causing further disruption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Departmental security contact</td>
<td>Threatens confidential data</td>
<td>Adversely impacts a critical enterprise system or service</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Technical support for affected device</td>
<td>Adversely impacts a very small number of non-critical individual systems, services, or people</td>
<td>Adversely impacts a non-critical enterprise system or service</td>
<td>No, unless requested by the Security Policy Committee Chairman or other appropriate administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security Policy Committee Chairman</td>
<td>Threatens confidential data</td>
<td>If breach of PII, see Samaritan Data Breach Response Policy and the Samaritan IT Security Incident Management Procedures for additional notification requirements</td>
<td></td>
</tr>
</tbody>
</table>
B. Disrupts a very small number of network devices or segments
C. Little risk of propagation and further disruption
C. Vice President of Client Services
D. Departmental security contact

N/A
“Not Applicable” - used for suspicious activities which upon investigation are determined not to be an IT security incident.


18. Related Laws, Regulations, or Policies
A. Samaritan Technologies IT Security Incident Management Procedures
B. Samaritan Technologies Data Breach Response Policy
C. Samaritan Technologies Security Policies and Procedures

19. Questions/Waivers
The Security Policy Committee Chairman (SPCC) is responsible for this policy. The SPCC or designee must approve any exception to this policy or related procedures. Questions should be directed to the SPCC.
Appendix G: IT Security Incident Management Policy

Version 1.0

2 September 2016

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 September 2016</td>
<td>Bruce Behymer</td>
<td>Initial draft.</td>
</tr>
</tbody>
</table>

Overview
The purpose of these procedures is to insure effective and consistent management of security incidents involving Company information and/or information technology resources. These procedures implement the Samaritan Technologies IT Security Incident Reporting and Response Policy.

I. **Audience**
These procedures apply to all Samaritan employees, partners and contractors with responsibility to respond to security incidents involving Samaritan IT resources or data.

II. **Definitions**
These procedures apply to all Samaritan employees, partners and contractors with responsibility to respond to security incidents involving Samaritan IT resources or data.

A. **Confidential Data** — Highly sensitive data, including Customer Data, intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. See the Samaritan Technologies Security Policies and Procedures document for an expanded definitions and examples.

B. **Security incident** — Any real or suspected event that may adversely affect the security of company information, Customer Data, or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person’s name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
• Violation of a Company security policy
• Security weakness such as an un-patched vulnerability

C. Personal identity information (PII) — an individual's name (first name and last name, or first initial and last name) in combination with one or more of the following: a) Social security number, b) driver’s license number or state identification card number, c) passport number, or c) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer’s financial account.

III. Security Incident Classification System
Security incidents will be classified according to incident categories and severity of incident in order to determine the appropriate response. A security incident classification scheme will be maintained by the Security Policy Committee Chairman (SPCC) to describe security events and support incident tracking over time.

A. Incident Categories
The following categories will be used to describe IT security incidents. Several categories may apply to a single incident. The examples listed in each category are not meant to be exhaustive.

1. Confidential personal identity data exposure
   Social Security Numbers with or without names
   Credit Card information
   Identity theft
   Other

2. Criminal activity/investigation
   Subpoena, search warrant, or other court order
   Litigation hold request (aka e-Discovery)
   Online theft, fraud
   Threatening communication
   Child pornography
   Physical theft, break-in

3. Denial of Service
   Single or distributed (DoS or DDoS)
   Inbound or outbound

4. Digital Millennium Copyright Act (DMCA) violation
   Official DMCA notification from copyright owner or legal representative
Illegal distribution of copyrighted or licensed material (movies, music, software, games)

Illegal possession of copyrighted or licensed material

5. Malicious code activity

Worm, virus, Trojan
Botnet
Keylogger
Rootkit

6. Policy violation

Company policy violation
Personnel action/investigation

7. Reconnaissance activity

Port scanning
Other vulnerability scanning
Unauthorized monitoring

8. Rogue server or service

Rogue file/FTP server for music, movies, pirated software, etc.
Phishing scam web server
Botnet controller

9. Spam source

Spam relay
Spam host
Company computer on a block list
Company email on a spam black list (i.e. Spamhaus)

10. Spear Phishing

Scam e-mail specifically targeting a company e-mail addresses that tries to trick people into divulging private information

11. Unauthorized access
Abuse of access privileges
Unauthorized access to data
Unauthorized login attempts
Brute force password cracking attempts
Stolen password(s)

12. Un-patched vulnerability
   Vulnerable operating system
   Vulnerable application
   Vulnerable web site/service
   Weak or no password on an account

13. Website or social media site defacement
   Defacement of web site
   Inappropriate post to company or customer social media, wiki, blog, etc.
   Redirected web site

14. No Incident
   When investigation of suspicious activity finds no evidence of a security incident

Incident Severity
The severity of incident is a subjective measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

- Scope of impact – how many people, departments, or systems does it affect?
- Criticality of the system or service – how important is it to the continuing operation of the company or its customers? What would be the impact on the company or customers, either functional or financial, if this system or service were unavailable or corrupted?
- Sensitivity of the information stored on or accessed through the system or service – does it contain confidential data, such as personal identity information or credit card information?
- Probability of propagation – how likely is it that the malware or negative impact will spread or propagate to other systems, especially to other systems off premises?

Four levels of incident severity will be used to guide incident response: high, medium, low, and NA ("Not Applicable").
1. **High**
   The severity of a security incident will be considered “high” if any of the following conditions exist:
   
   - Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)
   - Poses a potential large financial risk or legal liability to the Samaritan or its customers
   - Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)
   - Adversely impacts an enterprise system or service critical to the operation of a major portion of the university (for example, e-mail, production information system, financial information system, human resources information system, Internet service, or a major portion of the company network)
   - Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
   - Has a high probability of propagating to many other systems on premises and/or off premises and causing significant damage or disruption

   High severity incidents require an immediate response and focused, dedicated attention by the SPCC and other appropriate Samaritan officials and IT security staff until remediated. These incidents also have extensive notification and reporting requirements, as outlined in the Incident Response Summary Table below. A Post-Incident Report is required.

2. **Medium**
   The severity of a security incident will be considered “medium” if any of the following conditions exist:
   
   - Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
   - Adversely impacts a non-critical enterprise system or service
   - Adversely impacts a departmental system or service, such as a departmental file server
   - Disrupts a building or departmental network
   - Has a moderate probability of propagating to other systems on premises and/or off premises and causing moderate damage or disruption

   Medium severity incidents require a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident. Notification requirements are outlined in the Incident Response Summary Table below. A Post-Incident Report is not required unless requested by the SPCC, Vice President of Operations (VPO) or other appropriate administrator.

3. **Low**
   Low severity incidents have the following characteristics:
Adversely impacts a very small number of systems or individuals
Disrupts a very small number of network devices or segments
Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

Since a single compromised system can “wake up” and negatively affect other systems at any time, appropriate personal (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day. Notification requirements are outlined in the Incident Response Summary Table below. A Post-Incident Report is not required unless requested by the SSPC or VPO.

4. **NA ("Not Applicable")**
This is used for events reported as a suspected IT security incident but upon investigation, no evidence of a security incident is found. This usually corresponds to the incident category, "No Incident."

**Incident Response Summary Table**
The following table summarizes the handling of IT security incidents based on incident severity, including response time, the responsible incident managers, and notification and reporting requirements.

<table>
<thead>
<tr>
<th>Incident Severity</th>
<th>Characteristics (one or more condition present determines the severity)</th>
<th>Response Time</th>
<th>Incident Manager</th>
<th>Who to Notify</th>
<th>Post-Incident Report Required</th>
</tr>
</thead>
</table>
| High              | 1. Significant adverse impact on a large number of systems and/or people                                                       | Immediate     | SPCC or an Executive Incident Management Team | 1. Security Policy Committee Chairman  
2. Vice President of Operations  
3. Unit head  
4. Departmental security contact  
5. Technical support for affected device  
6. If breach of PII, see the Samaritan Data Breach Response Policy and Samaritan IT Security Incident Management Procedures for additional notification requirements | Yes |
|                   | 2. Potential large financial risk or legal liability to the Samaritan or its customers                                 |               |                 |                                                                                                                  |                              |
|                   | 3. Threatens confidential data                                                                                              |               |                 |                                                                                                                  |                              |
|                   | 4. Adversely impacts a critical enterprise system or service                                                                  |               |                 |                                                                                                                  |                              |
|                   | 5. Significant and immediate threat to human safety                                                                          |               |                 |                                                                                                                  |                              |
|                   | 6. High probability of propagating to a large number of other systems on                                                        |               |                 |                                                                                                                  |                              |
or off premises and causing significant disruption

<table>
<thead>
<tr>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Adversely impacts a moderate number of systems and/or people</td>
</tr>
<tr>
<td>2. Adversely impacts a non-critical enterprise system or service</td>
</tr>
<tr>
<td>3. Adversely impacts a departmental scale system or service</td>
</tr>
<tr>
<td>4. Disrupts a building or departmental network</td>
</tr>
<tr>
<td>5. Moderate risk of propagating and causing further disruption</td>
</tr>
</tbody>
</table>

| 4 hours | Appointed by unit head |

<table>
<thead>
<tr>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Adversely impacts a very small number of non-critical individual systems, services, or people</td>
</tr>
<tr>
<td>2. Disrupts a very small number of network devices or segments</td>
</tr>
<tr>
<td>3. Little risk of propagation and further disruption</td>
</tr>
</tbody>
</table>

| Next business day | Technical support for affected device |

| Security Policy Committee Chairman |
| Vice President of Operations |
| Unit head |
| Departmental security contact |
| Technical support for affected device |

No, unless requested by SPCC, VPO or other appropriate administrator

<table>
<thead>
<tr>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Not Applicable” – used for suspicious activities which upon investigation are determined not to be an IT security incident.</td>
</tr>
</tbody>
</table>

V. Security Incident Reporting and Detection

A. Security Incident Reporting

1. All members of the Samaritan community are responsible for promptly reporting suspected or known security incidents, including an observed or suspected security weakness in Company systems or services, in accordance with the Samaritan Security Policies and Procedures document.
2. All suspected high severity incidents, including those involving possible breaches of personal identity information, must be reported directly to the Security Policy Committee Chairman (SPCC) as quickly as possible by phone (preferred), email, or in person:

Bruce Behymer  
Samaritan Security Policy Committee  
265 East 100 South  
Salt Lake City, UT 84111  
Phone: 801-328-3972 x250  
E-mail: security@samaritan.com

3. If the SPCC is not available, contact the company’s Vice President of Operations (VPO):

Keith Leonard  
Samaritan Technologies Operations  
265 East 100 South  
Salt Lake City, UT 84111  
Phone: 801-328-3972 x201  
E-mail: kleonard@samaritan.com

4. All other suspected incidents must also be reported to any of the following:
   a. Send email to security@samaritan.com (preferred)
   b. Contact the SPCC listed above
   c. Contact any member of the Samaritan Security Policy Committee. Any incident that is not high severity may be reported first to departmental IT support personnel, or the unit head before reporting it to the people listed above.

5. **Warning:** If reporting a suspected security weakness or system vulnerability, do not attempt to confirm it by testing the weakness since that could be interpreted as a potential misuse of the system or cause damage to it.

6. When receiving a report of a suspected or confirmed security incident, the SPCC or designee will gather as much of the following information as possible:
   a. Name, affiliation, e-mail address, and phone number of person reporting the incident
   b. Description of the suspected security incident
   c. Information to help identify the source of the suspicious activity, like an IP address or an e-mail message with full headers.
   d. Date(s) and time(s) of the suspicious activity, noting the time zone.
e. Evidence of suspicious activity (for example, full headers of an e-mail message suspected to be spam originating at Samaritan, appropriate log records, etc.)

7. In addition to documenting the initial report, the SPCC or designee will:
   a. Create an entry in the Samaritan security incident tracking system (see “Incident Tracking and Reporting” below)
   b. Initiate appropriate incident handling procedures
   c. As appropriate, communicate with and provide feedback about the results to those reporting the incident once the incident has been handled and closed

B. Incident Detection

1. In addition to reports from the Samaritan community of suspected or confirmed security incidents, anomalous events may be detected that indicate potential security incidents. Having mechanisms to detect anomalous events early and reliably helps minimize their impact. Detection can be very challenging since there are potentially so many different types of incidents and vectors for attack on a huge number and variety of systems and networks. Thus no one person, unit, or technology can possible monitor it all. Detection is therefore a collaborative effort among Samaritan and departmental IT and security personnel.

2. Channels for detecting possible security incidents include:
   a. E-mail sent to security@samaritan.com
   b. E-mail sent directly to the SPCC
   c. Phone call to the SPCC
   d. Automated botnet detection system
   e. Network performance monitoring (e.g., noticing a congested network segment)
   f. Court orders (for example, a subpoena or search warrant). All IT-related court orders should be directed to Samaritan’s General Counsel.
   g. A customer contacts via support or a staff member, or the support ticket database.
   h. Monitoring security mailing lists and web sites for threat alerts [for example, the SANS Internet Storm Center (isc.sans.org) and dashboard (https://isc.sans.edu/dashboard.html)].
   i. Monitoring external sources of information about new vulnerabilities and exploits and about incidents occurring at other organizations.
   j. Employing passive detection techniques such as network flow analysis (top talkers, traffic volume thresholds, communication with known malicious sites, etc.); log file analysis (operating system, system services, databases, applications, network devices, etc.); intrusion detection/prevention systems, and monitoring alerts from security systems (firewalls, anti-virus protection, intrusion detection/prevention systems, wireless network management systems that detect rogue wireless access points, etc.)
k. Employing active detection techniques such as port scans looking for unusual services, vulnerability scans (Zap or Cenzic Hailstorm), manual monitoring of radio frequencies to detect unauthorized wireless access points, file integrity verification that detects changes to important files, and OWASP attack detection in our products.

VI. Incident Handling and Response

Security incident response will be typically handled through several stages: analysis, containment, eradication and recovery, and follow-up.

A. Analysis

Once a potential security incident is reported or anomalous activity detected, analysis must be performed to determine if it is indeed symptomatic of a security incident and to understand the nature of the incident for proper remediation.

1. Goals

a. Understand the nature and scope of the incident

b. Collect enough information about the incident so the response team can prioritize the next steps in handling the incident, which is normally containment

c. Determine if confidential data is involved in the incident

2. Components of security incident analysis

a. Collaboration with other professionals as needed (for example, a security analyst, network analyst, system administrator, and application manager working as a team to analyze the system exhibiting the anomalous behavior; consulting external sources like REN-ISAC, US-CERT, SANS, etc.)

b. Understanding normal system and network behavior so anomalous activity can be identified

c. Analysis and correlation of as many indicators as possible, such as monitoring network traffic to/from the host suspected of being compromised, network packet captures for more in-depth analysis, log file analysis, interviews with users and/or system administrators, etc.

d. Initial determination of the incident’s scope (How many systems affected? Is it actively propagating? If so, how?)

e. Research of the specific malware or type of attack

f. Collection of additional data which may require permission from the SSCP or VPO

3. Procedures for Analysis

a. Detect security event (see section V.B. above)

b. Analyze event data to determine if it is indicative of a security incident and get an initial impression of the nature and scope of the incident

c. Notify the SPCC who may assist with the initial analysis of the event data. Other appropriate personnel may be notified at this point as well, like relevant IT support staff, or a supervisor or department head.
d. The SPCC will record it in the Incident Tracking System (see section VI.E below)

e. If there’s a need to access personal data, like an individual’s e-mail or files, in order to gather more information about the incident, first get approval from the VPO.

f. Determine if any confidential data was or might have been affected.

g. If the incident is of high or medium severity:

i. Copy the database instance or, if possible, image the hard drive, memory, and any other relevant media before performing analysis that might alter evidence. For hard drives, bit-by-bit copies are required in case deleted files need to be recovered. This is especially important for cases that involve confidential data, possible criminal investigation, or sensitive personnel actions.

ii. Preserve the original media in a secure location and perform analysis on a copy of the data.

iii. Take notes on all actions taken.

h. Perform additional forensics sufficient to characterize the incident (for example, analyze network traffic or server security log data).

B. **Containment**

Once a security incident is confirmed, the next step is typically containment.

1. **Goals**

   a. Stop potential loss of confidential data

   b. Protect other computers and information on the company network and Internet (for example, keep the malware from spreading to other computers on or off premises)

   c. Prevent further damage to the compromised system and/or information

   d. Identify the location and owner of the computer(s) so they can be engaged in containment, eradication, and recovery

2. **Delaying containment**

   In some cases, containment may need to be delayed in order to monitor the attacker’s activity, usually to collect more evidence. However, the risk of the compromised system being used to attack other systems or breach confidential data could lead to legal liabilities. Consult with SPCC and Samaritan’s General Counsel before deciding to delay containment.

3. **Procedures for Containment**

   a. Identify the location and/or owner of the system(s) involved in the incident by checking any of the following:

   i. Network ARP tables to map the IP address to a MAC address

   ii. DHCP logs for MAC address and hostname

   iii. ”nbtscan” command to query host NetBIOS information
b. Determine if the computer needs to have its network access blocked. If so, this can be accomplished in several ways by the IT team:

i. At the switch port, router interface, premises border.

ii. Block the MAC address on all company wireless networks (be sure to block it on all wireless networks, not just individual office suites, for example. Also block the wired network interface for the same computer if known).

iii. Disable dial-up modem access.

iv. Disable VPN access.

v. If the offending device is an unauthorized wireless access point, its connection to the company’s data network must be blocked or removed. This can be done either via the network switch port to which it is connected, or by physically locating the device and unplugging it.

c. If the computer is blocked record the action in the Samaritan Blocked Computer Log in the Security Folder of Samaritan’s Google Drive account.

d. An alternative to blocking all network access, if available, is to put the computer in a network quarantine that redirects its network traffic to a web server with instructions for the owner on how to proceed. This can be done in Impulse SafeConnect, for example.

e. There may be cases when a specific protocol or UDP/TCP port needs to be blocked at the premises border or some other network interface in order to prevent propagation of the malware or to protect the company from further attacks. Consult the IT network team if considering this since they will have to implement it in company firewalls or router Access Control Lists.

f. Notify the system administrator and/or user responsible for the system.

g. Isolate the affected computer(s) either by unplugging the network cable (preferred) or shutting down the computer. Unplugging the network cable and leaving it running is best since shutdown can alter or destroy evidence, like with memory-resident malware. For wireless computers, the wireless interface can be disabled while leaving the computer running.

h. Perform containment on the affected system(s) to keep it(them) from doing further damage to the computer or the data on it. This step depends on the nature of the compromise/malware, the need for preserving evidence (i.e., if you have to preserve evidence, don’t do anything to the computer until images of RAM and the hard drive are captured), the urgency of restoring the service hosted on the affected systems, and the time and resources available.

C. **Eradication and Recovery**

1. **Goals**

   a. Preserve evidence if it has not already done

   b. Perform additional analysis as needed to complete the investigation
c. Remove the components of the incident impacting the affected systems, such as deleting the malicious code or disabling a compromised user account.

d. Mitigate the attack vector so a similar incident does not occur (for example, patch the vulnerability used to compromise the system, apply standard system hardening procedures, adjust firewall rulesets, etc.)

e. Restore systems to normal operation

2. Procedures for Eradication and Recovery

a. Determine the full scope of the incident – how many systems did it affect and therefore need to be repaired?

b. Determine if any additional analysis is needed:

   i. Determine if any of the affected systems still need to have memory, hard drive(s), or other media imaged to preserve evidence; make an image copy of the media, preserve the original and perform analysis on the copy.

   ii. Perform additional analysis, which may include:

      - Searching for malware by running an anti-virus scan and/or rootkit detection software, or looking for specific files known to be associated with current threats
      - Recover deleted files and file fragments
      - Perform a vulnerability scan
      - Check for unusual running processes and suspicious registry entries, especially ones that run on start-up
      - Determine open network ports and processes listening to those ports
      - Take a network packet capture and analyze the network traffic
      - Analyze network flow data
      - Analyze log files for unusual activity
      - Search for confidential data that may have been missed in the initial analysis

c. If eradication and recovery keeps the system or service out of operation beyond the length of time that can be tolerated by the company and/or our customers, invoke business recovery and continuity procedures to restore the service until normal operations can be resumed.

d. Determine if a reformat/reinstall is required. **Compromises that allow remote control of the system, gain root/Administrator privileges, and/or install a backdoor require a complete, clean re-install of the system for eradication.**
D. **Follow-up**

1. **Goals**
   
a. Determine lessons learned and make recommendations to prevent subsequent similar incidents
   
b. Issue final reports
   
c. Archive evidence and documentation
   
d. Close out the incident

ii. Reformatting the hard drive and re-installing from a backup tape prior to the compromise is acceptable, as is restoring from a clean image for those systems that use disk imaging technology like Symantec Ghost.

iii. Note that reinstalling must occur without exposing the vulnerable system to the company network and the Internet

e. If infected with malware and a reformat/reinstall is not required, remove the malware from the system. Running an anti-virus scan after updating virus definition/pattern file may suffice. Specific instructions for removing certain types of malware may also be found by searching the Internet.

f. If the incident involves an unauthorized wireless access point, locate the device and contact the person responsible for it to ensure that it ceases operation.

g. Mitigate the attack vector to prevent further instances. This may include:

   i. Patching vulnerabilities in the operating system and all applications software
   
   ii. Changing passwords
   
   iii. Placing the system behind a firewall
   
   iv. Adjusting firewall rules
   
   v. Updating or installing new security software (for example, anti-virus software or a host-based personal firewall)
   
   vi. Applying standard system security hardening techniques
   
   vii. Passing a security assessment
   
   viii. User training

h. Restore network access if the system was blocked during the containment phase. The request to remove the network block must be approved by the SSCP.

i. Return the system to normal operations
2. Procedures

a. The Incident Manager should confirm that all action items, investigations, analyses, and communications are completed

b. Hold a Post-Incident Review session, if required, to determine ways to improve the company’s management of security incidents and help prevent future incidents, not to assign blame.

   i. It should be scheduled to occur within 2-3 weeks of the incident’s remediation

   ii. Include the incident response team and relevant stakeholders

   iii. Appoint one person to record notes – successes, failures, recommendations, and action items

   iv. Cover the following areas in the review session:

      - Are there any open issues? In other words, is remediation of the incident complete?

      - What could have prevented the incident?

      - How effectively was the incident handled (response time, communication, following procedures, containing spread/damage, etc.)?

      - Recommend changes to policy, procedure, and security controls to prevent and more effectively handle future incidents.

      - Identify any needed follow-up tasks and assign those tasks to individuals

c. Evidence management — does any evidence need to be preserved longer? If so, for how long and by whom? Release or properly destroy any evidence that is no longer needed.

d. Complete a Post-Incident Report if required (see “Post-Incident Report” in section IX.C below) and submit it to the Chief Information Officer. Security incidents with a severity category of “high” must complete a post-incident report. The VPO may request a post-incident report for any security incident.

e. The VPO will review any recommendations and consider assigning resources to implement them.

f. Archive reports and other relevant documents and communications ("work product") according to the company’s retention of records policy and procedures. This includes log files, timelines, recovered files, notes, network flow data, e-mails, etc.

g. Close out incident tickets in the incident tracking system

VII. Collection and Preservation of Evidence

When a security incident involves legal action against a person or organization, or a personnel action against a Company employee, evidence must be collected, preserved, and presented to conform to the rules for evidence specified in the relevant jurisdiction(s). The following procedures help ensure
the strong evidence trail needed for admissibility (making sure it can be used in court) and weight of evidence (high quality and completeness).

A. When collecting evidence, follow all appropriate company policies and procedures, such as getting permission from the VPO to access data.

B. Document all actions taken in the collection and preservation of the evidence.

C. For data stored on electronic media, such as a hard disk drive, USB flash drive, CD, DVD, or RAM, make a mirror image or copy (depending on applicable requirements) of the media. For example, if forensics will require recovering deleted files or file fragments from a hard drive, a bit-by-bit mirror image of the drive is required since a file-by-file copy will not capture that data.

   1. Have another person witness the imaging/copying process. If the incident involves a high profile or sensitive criminal case, have a law enforcement officer assist with the collection of the evidence, witness the imaging/copying process, and store the originals.

   2. Log all actions taken during the imaging/copying process, including date, time, and location the image/copy was made, who performed the actions and who witnessed it, and the tools and programs used.

   3. Label the original media and store it along with the log of the imaging/copying process in a secure location.

D. Perform all forensics work on the image or copy, not the original. Additional images or copies of the original can be made if needed (for example, if forensics analysis on the copy destroyed some evidence and you need to continue analysis on a fresh copy).

E. For paper-based documents, keep the original in a secure location and log the following:

   a. who found the document

   b. where it was found

   c. date and time it was found

   d. who witnessed the discovery

VIII. Incidents Involving Confidential Personal Identity Information

Incidents suspected of or known to involve confidential personal identity information, such as names with social security numbers or credit card numbers, have special legal, policy, and notification requirements in addition to the normal incident handling procedures outlined in this document.

A. Examples of State Law

   1. **California: SB 1386**, passed in 2002 as the first of many laws enacted by states to frame the response requirements for incidents involving personally identifying information (PII), did much to set the standard in this area: Among other things it states the following:
“personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number.
2. Driver’s license number or California Identification Card number.
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

...“personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."

..."breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure...

...[the company] shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

2. **Kansas**: Kansas Statute 50-7a, the *Unfair Trade and Consumer Protection — Protection of Consumer Information* ([kansasstatutes.lesterama.org/Chapter_50/Article_7a](kansasstatutes.lesterama.org/Chapter_50/Article_7a))

Kansas law requires a “reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonable likely to occur, the ... agency shall give notice as soon as possible to the affected Kansas resident.” Thus prompt action in cases known or suspected to involve personal information is critically important.

**B. Executive Incident Management Team**

1. Incident response in these cases will be overseen by an Executive Incident Management Team (EIMT) as mandated by the company’s Security Incident Reporting and Response
Policy. An EIMT may also oversee the response to other high-severity incidents, but the primary purpose is to deal with incidents involving personal identity information, protected health information, or payment card information.

2. The purpose of the EIMT is to provide executive guidance to the response process to insure: a) an appropriate, timely, and legal response, b) to make decisions related to the incident, and c) to notify appropriate parties.

3. The team consists of:

- Senior administrator for the affected unit
- Chief Information Officer (VPO)
- Security Policy Committee Chairman (SPCC)
- The company’s General Counsel
- Others as needed (for example, marketing and communications, police for criminal incidents, or the data steward of the affected data)

The VPO will convene the EIMT at the appropriate time per the procedure that follows.

**Procedure for handling a breach of confidential personal identity data**

If the SPCC determines that confidential data has been or may have been breached, the SPCC will immediately notify the VPO.

The SPCC will oversee additional forensics analysis to gather as much information as possible about what happened, being sure to properly protect evidence.

If after analysis the VPO and SPCC have definitive evidence that the confidential data was not breached, then no further special action is required and normal incident response procedures may continue. However, the security of this system and the need to store confidential data on it should be carefully assessed.

If there is a possibility that confidential data involving personal identity information was breached, the VPO will convene the EIMT as quickly as possible to review the evidence and determine if a breach of confidential personal identity data occurred or is “reasonably likely” to have occurred (wording of the state notification law).

If the EIMT determines that personal identities are not at risk, no further special action is required and normal incident management procedures may continue.

If Customer Data is at risk implement the procedures found in the *Samaritan Data Breach Response Policy* document to ensure proper coordination with the customer.

The SPCC will convene a Post-Incident Review Session with key stakeholders from the EIMT and others as needed (see above).

The SPCC will draft a confidential Post-Incident Report (see "Post Incident Report" below) to be reviewed by appropriate members of EIMT for accuracy and submitted to the VPO and senior administrator(s) in the affected unit(s).
Discuss how the incident could have been prevented and steps to take to prevent similar incidents in the future, maintain a record of the steps taken.

**Incident Tracking and Reports**

**Incident Tracking System**

1. The SPCC will maintain an incident tracking system and record the following information about all reported security incidents:

   a. Incident ID number assigned by the SPCC in the form YYYY-XXX where "YYYY" is the year in which the incident occurred and "XXX" is a unique number that roughly corresponds to the sequential order of occurrence of the incident that year. For example, 2007-103 would be the 103rd incident that occurred in 2007.

   b. Incident category(ies), severity, and description

   c. Identity of the affected system(s) – IP address, domain name, MAC address

   d. Whether the system contains confidential data

   e. Location of the affected system(s) – building and department

   f. Contact information – usually the departmental security contact, or appropriate system administrator

   g. Dates and times – first notice, when contact notified, blocking/unblocking

   h. Recovery action taken

2. All IT security incidents or suspected incidents (i.e., reports of suspicious activity that upon investigation are determined not to be a security incident) will be recorded in the incident tracking system.

3. The incident tracking system should be used to identify trends or outbreaks that may require changes to security controls and/or policies to reduce the risk of future occurrences.

4. The incident tracking data is considered confidential and should therefore be encrypted when stored or transmitted and disclosed only to authorized individuals. The confidentiality of reports derived from the incident tracking data will be determined on a case-by-case basis by the SPCC and/or the VPO.

**A. Post-Incident Report**

1. Individual security incidents may require completion of a Post-Incident Report. Incidents with a severity category of "high" must submit one, and the VPO or SPCC may request one for any security incident. Normally, the incident manager will complete the post-incident report.

2. The VPO will review any recommendations in the report and determine additional follow up actions.

3. Post-incident reports must be submitted to the VPO and SPCC, be marked as confidential, and use the form specified in Appendix 1.
X. Related Company Policies and Procedures

A. Samaritan Technologies IT Security Incident Reporting and Response Policy

B. Samaritan Technologies Security Policies and Procedures

XI. References

A. Computer Security Incident Response Team (CSIRT) resources, CERT Coordination Center, Carnegie Mellon University Software Engineering Institute — www.cert.org/csirts/


C. EDUCAUSE/Internet2 Cybersecurity Initiative Incident Notification Toolkit — wiki.internet2.edu/confluence/display/itsg2/Data+Incident+Notification+Toolkit

D. Thresholds for notification: deciding whether or not to notify — net.educause.edu/ir/library/pdf/CSD4236.pdf

E. EDUCAUSE/Internet2 Cybersecurity Initiative Confidential Data Handling Blueprint — wiki.internet2.edu/confluence/display/itsg2/Confidential+Data+Handling+Blueprint


Exhibit A: Sample IT Security Post-Incident Report

IT Security Post-Incident Report

Incident ID Number: YYYY-NNN

Incident Category(ies):

Classification(s) of Data Involved in the Incident (per the Samaritan Technologies Security Policies and Procedures Data Classification Schema):

Incident Title:

Incident Manager (name, title, e-mail, phone):
Incident Administrative Contact (name, title, e-mail, phone):

Incident Departmental Contact (name, title, e-mail, phone):

Date of Initial Suspicious/Malicious Activity:

Date Incident Reported:

Date Incident Fully Contained:

Post-Incident Review Session:

  Date:

  Participants:

Date Incident Response Completed:

Post-Incident Report Submitted by (name, title, e-mail, phone):

Date Post-Incident Report Submitted:

Incident Overview:

Provide a general overview of what happened, indicating how the security breach occurred and the scope of the incident (for example, who was affected, what systems were compromised, the dates of major milestones, etc.). Detailed information, like a timeline, may be added to the end of the report as appendices.

Incident Detection:

Briefly describe how the incident was first discovered (when, how, and by whom).

Incident Response:

Describe how the incident was contained (prevented from spreading and/or doing further damage) and eradicated (removed from infected hosts). Also describe recovery activities.
Incident Notification

If the incident involved the breach of, or suspected breach of personal identity information that requires notification, then describe how and when the affected people were notified. Include any public communications, like a press release.

Incident Follow-Up

Identify steps taken to prevent future incidents, lessons learned, and any other recommendations resulting from the incident and the post-incident review session.

A. Steps Taken to Prevent Future Incidents
   i.

B. Lessons Learned
   i.

C. Other Recommendations
   i.

Appendices

Attach any other relevant information about the incident that should be archived.
Appendix H: Data Breach Response Policy

Version 1.4
27 June 2018

Cancellation: Not applicable.

Inquiries: Samaritan Security Policy Committee (Infosec).

Retention: Indefinite.

Review: Subject to review for currency 24 months from date of issue.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Apr 2014</td>
<td>Bruce Behymer</td>
<td>Quality Assurance Manager responsibilities transferred to the Product Development Manager. The description of these responsibilities was clarified to extend only to those systems processing, transferring, or storing customer data. References to Samaritan’s own enterprise (internal business) network security has been removed. Security of Samaritan’s internal business network is an IT responsibility that falls under the Vice President of Operations. Director of Client Services responsibilities transferred to the Vice President of Client Services. Director of Operations responsibilities transferred to the Vice President of Operations.</td>
</tr>
<tr>
<td>25 September 2015</td>
<td>Bruce Behymer</td>
<td>Fixed a few grammar errors and inconsistent fonts sizes.</td>
</tr>
</tbody>
</table>
Introduction:

Safeguarding personally identifiable information (PII) at Samaritan and preventing its unauthorized acquisition, access, use, or disclosure are essential to ensure Samaritan retains the trust of our customers, our customers’ volunteers and clients, and the public.

To that end, Samaritan has established the Samaritan Security Policy Committee (Infosec), the purpose of which is to establish and maintain the security of Samaritan’s information systems including those systems which are used to store and provide access to Customer Data.

Additionally, upon discovery of a Data Breach, a Data Breach Response Team is formed to coordinate Samaritan’s response to any breach of PII at Samaritan. The Data Breach Response Team will be comprised of the following Samaritan Staff Members:

- All members of the Samaritan Security Policy Committee
- Samaritan’s Vice President of Client Services
- Samaritan’s Vice President of Operations
- Samaritan’s General Legal Counsel
- Samaritan’s Client Services Team Leader(s) for the affected customer(s)
- Samaritan’s Director of Product Development
- Samaritan’s Product Development Manager
Other members of the Data Breach Response Team may include:

- Members of the Samaritan Product Development Staff for determining the full nature of the data that was breached and the individuals affected, and diagnosing and repairing any defects that may have been involved in the Data Breach.

- Members of the Samaritan Quality Assurance Staff for verifying the any product defects that may have been involved in causing a Data Breach and verifying the fixes to any such defects.

Definitions:

Data Breach means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, theft, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access to Customer Data, in usable form whether physical (such as paper documents) or electronic information. A Data Breach includes the compromise of a Samaritan information system that could allow unauthorized access to PII.

Affected individuals are those individuals whose PII was, or is reasonably believed to have been, acquired by an unauthorized person.

Personally Identifiable Information (PII) is any information that permits an individual’s identity to be directly or indirectly inferred from that information. Dates and places of birth, drivers’ license numbers, mothers’ maiden names, Social Security numbers, credit card numbers, resumes, fingerprints, and medical records are just a few examples of PII.

Roles and Responsibilities:

Every member of the Samaritan community, including all employees and contractors is responsible for immediately reporting to Infosec upon learning of or discovering a data breach. If in doubt, individuals should err in favor of reporting. Contractor supervisors should ensure the contractors they supervise are aware of this directive and that breaches involving their contractors are reported in a manner consistent with it.

Client Services Team Leaders will immediately notify the Vice President of Client Services and a member of Samaritan Security Policy Committee when they detect or become aware of a breach to Samaritan’s information systems.

The Samaritan Security Policy Committee (Infosec) Chair (SPCC) will convene the Data Breach Response Team when he or she learns of a material breach. After consulting with the Data
Breach Response Team, the Chair is responsible for deciding when, who, and how to notify of a breach. The Chair is also responsible for maintaining appropriate records of breaches, reporting, and notifications, and, when warranted, for informing Samaritan’s Partners of the Data Breach. The Samaritan Security Policy Committee Chair reports monthly to Infosec any breaches deemed nonmaterial.

**Samaritan’s Product Development Manager** is responsible for monitoring the Samaritan production servers, computer systems, and networks which transmit, process, and store production customer data. When Samaritan detects a breach or a breach is reported to Samaritan, the Product Development Manager is responsible for notifying the Security Policy Committee Chair. The Product Development Manager in coordination with the Director of Product Development is also responsible for the appropriate technical response to a breach, such as resolving any identified security deficiencies that allowed the breach to occur. The Product Development Manager will report a breach to the U.S. Computer Emergency Readiness Team (US-CERT) when the Security Policy Committee Chair determines, in the exercise of his or her discretion, such a report is appropriate. Samaritan’s Vice President of Operations shall serve as the Chair of the Data Breach Response Team in the absence of the Security Policy Committee Chair.

**Samaritan’s General Counsel** is responsible for providing legal advice, including counsel on any Samaritan legal or regulatory obligations, in the event of a breach.

**Samaritan’s Vice President of Operations** is responsible for providing the Data Breach Response Team with information about any available insurance coverage relevant to a breach and for providing any required notice of a breach to insurance carriers. The Vice President of Operations will advise the Security Policy Committee Chair of a potential breach promptly.

**Samaritan’s Commitment to the Customer:**

Upon Samaritan’s discovery of any actual or suspected Data Breach of Customer Data, Samaritan shall immediately, and in no event later than one hour of discovery, report the breach to Customer’s Data Breach Notification Contacts listed below or in Samaritan’s customer contact database. Samaritan is responsible for positively verifying that notification is received and acknowledged by at least one of the Customer Data Breach Notification Contacts.

**Customer Data Breach Notification Contacts:** (Insert the appropriate contact information.)

Contact1 Name
Determining Whether or Not to Notify Victims: If confidential data resides on a compromised computer, it is not always obvious whether the data were accessed and therefore whether potential victims need to be notified, especially in light of some state laws that require notification if “misuse of the information has occurred or is reasonably likely to have occurred.” The following questions provide guidance to consider along with the Customer when deciding whether confidential data was breached:

A. Is the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information?

B. Is there evidence that information has been downloaded, copied, or otherwise accessed, for example: an ftp log that contains the name of a file containing notice triggering information?

C. Was a privileged (e.g. root or administrator) or non-privileged account, one with access to privileged information, compromised?

D. Was one system or multiple systems compromised?

E. Was the disclosure accidental or a result of human error?

F. Was the discloser a result of a software defect (bug) that needs to be fixed?
G. Is the receiving party likely to distribute the information further? Is the recipient willing to sign a statement that they will return and delete the disclosed information in their possession or have already done so and will not distribute the information any further?

H. Is an attacker involved? Is the identity of the attacker known or unknown? If known was the attacker a disgruntled insider or an unaffiliated third party? Were multiple attackers involved?

I. Are there indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported?

J. Did the unauthorized person have access to the information for an extended period of time?

K. What was the time between compromise start and compromise discovery?

L. Did the compromise indicate a directed attack, such as a pattern showing the machine itself was targeted versus an automated attack?

M. Did the attack appear to seek and collect the information?

N. Did the attack appear to include tampering with records (e.g., changing grades)

O. Did the attacker attempt to cover up their activity?

P. Did the attacker release information about the nature or scope of the attack?

Q. Was the information encrypted and would the encryption method effectively prevent the information from being accessed.

R. What is the potential damage to individuals if notification is not given?

S. What is the potential damage to company and customer credibility in the case of notification?

T. What is the potential damage to company and customer credibility in the case of failure to notify?

**Affected Party Notification:** Samaritan has in place procedures and the capability to promptly notify any individual whose Customer Data was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by Samaritan shall be coordinated with, and subject to the prior approval of Customer, based upon a risk-based analysis conducted by the Customer in accordance with Customer’s Data Breach Notification Policy. If the Licensed Software is hosted on Customer’s own servers then Customer will provide Samaritan with access to the Licensed Software and Customer Data as needed in order to allow Samaritan to comply with this requirement and remediate any technical issues necessary to prevent data breach.

The following is a list of things to consider and address with respect to notifying affected parties:
A. Determine if the affected individuals need to be notified and the appropriate method for notification (Individual states may have specific stipulations)

B. Determine if the affected individuals need to be notified and the appropriate method for notification (Individual states may have specific stipulations)

C. Determine who will draft and sign the notification (see Appendix 2 for sample notification letter)

D. Assign someone to collect victim mailing addresses and to distribute notifications

E. Determine the point of contact for inquiries from the victims, media, and other interested parties and the type of assistance to offer. In determining the type of assistance appropriate to the situation, consider assistance such as:
   - Providing personal assistance in getting free credit protection,
   - Establishing a toll-free phone number for victims to call for assistance, and/or
   - Establishing a specific email address for victims to get more information,
   - Establishing an informational website.

F. Determine the need for a news release and timing in relation to the communication with victims. The drafting of a news release should be coordinated by a representative from the Vice President for Communications and Marketing or designee and the Customer. The content of the release should be reviewed by the Executive Incident Management Team (EIMT) leader for accuracy.

G. Determine if all national consumer credit agencies need to be notified (required by Kansas law if notifying more than 1,000 consumers) and if so, who will notify them and what information will be provided

**Notification Content:** Subject to the Customer’s analysis of the Data Breach and the terms of its instructions to Samaritan regarding any resulting Data Breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by Customer. At minimum, a notification should include:

A. A brief description of how the Data Breach occurred;
B. A description of the types of personal information involved in the Data Breach;
C. A statement as to whether the information was encrypted or protected by other means;
D. Steps an individual may take to protect themselves;
E. What the Customer is doing, if anything, to investigate the Data Breach, to mitigate losses, and to protect against any further Data Breaches; and
F. A point of contact information identifying who affected individuals may contact for further information.

In the event that a breach occurs as a result of the violation of a term of a Contract or written Agreement with Customer by Samaritan or its employees, Samaritan shall, as directed by Customer and at no cost to the Customer, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the Data Breach. Should the Customer elect to provide and/or procure notification or identity protection services in response to a Data Breach that results from the action of Samaritan employee or staff member or a defect in the Licensed Software or Client Software, Samaritan will be responsible for arranging for the notification and/or identity protection services in consultation with Customer and paying for said services.

Credit Card Information

If the PII threatened in the incident includes payment (credit or debit) card information (PCI), all normal procedures for handling a suspected breach of confidential data must be followed, in addition to:

A. Include a representative from Samaritan’s Financial Services on the Executive Incident Management Team (EIMT)
B. Promptly notify the affected payment brands (VISA, MasterCard, Discover, etc.), as required by the Payment Card Industry Data Security Standards, security control 12.9.1
C. The EIMT should consider notifying the acquiring bank that processes financial transactions for the company.

Internal Notification of Action: If potential victims do need to be notified, Samaritan’s Vice President of Operations (VPO) and the SPCC, or designee(s) should notify the following Samaritan staff as quickly as possible:

A. The Managing Partner
B. The Chief Executive Officer
C. The company’s general council

Breaches of Protected Health Information (PHI) of a HIPAA Covered Entity Customer
If the Customer is a HIPAA Covered Entity such as a hospital or health provider and the customer data involved included unencrypted PII or PHI, all normal procedures for handling a suspected breach of confidential data must be followed, in addition to the following:

**Breaches Affecting 500 or More Individuals**

If the Breach involves 500 or more people then the Security Policy Committee Chair or his/her designee shall assist the covered entity in reporting the breach to the United States Secretary of Health and Human Services without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.

Submit a Notice for a Breach Affecting 500 or More Individuals

**Breaches Affecting Fewer than 500 Individuals**

If a breach of unsecured protected health information affects fewer than 500 individuals, the Security Policy Committee Chair or his/her designee shall assist the covered entity to notify the United States Secretary of Health and Human Services of the breach within 60 days of the end of the calendar year in which the breach was discovered. (A covered entity is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity may report such breaches at the time they are discovered.) The covered entity may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident. The covered entity must submit the notice electronically by clicking on the link below and completing all of the fields of the breach notification form.

Submit a Notice for a Breach Affecting Fewer than 500 Individuals

If you have any questions, you call HHS OCR toll-free at: 1-800-368-1019, TDD: 1-800-537-7697 or send an email to OCRPrivacy@hhs.gov.

**Appendix A. Sample Notification Letter to Victims of Possible Identity Theft**

[Date]

[Address Block]

Dear [first name]


We recently learned that the names, birthdates, street addresses, phone numbers, and email addresses, of [number] [organization] volunteers had been inadvertently emailed to [number] volunteers in a bulk email sent by one of our volunteer coordinators on [date]. We have updated our procedures and added safeguards to prevent this from ever happening again in the future.

You are being notified of this security breach because you are one of the volunteers whose personal information was accidentally exposed. Since much of this information is public anyway we think it highly unlikely that the exposure of this information will be misused. Although there is no evidence that any volunteer’s personal information has been misused, we are bringing this to your attention so you can be alert to any signs of possible misuse of your personal identity. There are some steps you can take to protect yourself.

First, you should place a “fraud alert” on your credit file to let creditors know to contact you before opening a new account in your name. Simply visit one of the online fraud alert web sites listed below or call any one of the three credit bureaus at the numbers provided and follow the instructions for victims of fraud. You will automatically place a fraud alert on your credit file with all three of the bureaus when you call any one of them.

**Equifax** (www.equifax.com)
Online fraud alert: www.fraudalerts.equifax.com
(800) 525-6285

**Experian** (www.experian.com)
Online fraud alert: www.experian.com/consumer/fraud_faqs.html#request
(888) 397-3742

**TransUnion** (www.transunion.com)
(800) 680-7289
Second, you are entitled to a free copy of your credit report so visit https://www.annualcreditreport.com to request your report and review the report carefully for accounts you did not open or for inquires from creditors you did not initiate. If you see anything you do not understand, call the credit agency at the telephone number on the report. Please note that [organization] is not going to contact you again, so if an unknown person should contact you, do not give out any additional personal information. Additional information about identity theft can be obtained from the Federal Trade Commission’s Identity Theft webpage and the Federal Government’s Identity Theft webpage.

[Organization] is committed to maintaining the privacy of our volunteer information. We deeply regret this situation and any inconvenience this incident may have caused you. Should you have further questions regarding this matter, please contact [firstname lastname] in the [dept name] by e-mail at [email address] or by phone at xxx-xxx-xxxx.

Sincerely,

[appropriate high level contact]
## Appendix I: Data Encryption

**Version 1.4**  
27 June 2018

### Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bruce Behymer</td>
<td>Initial Draft of document.</td>
</tr>
<tr>
<td>25 September 2015</td>
<td>Bruce Behymer</td>
<td>Added cover page, this revision history, headers and footers. Cleaned up some formatting. Removed customer specific references in the text. Added a description of the encryption of data in transit.</td>
</tr>
</tbody>
</table>
| 2 October 2015  | Bruce Behymer      | Make the following clarifications in the appropriate sections of the document:  
1. PHP encryption uses 128bit all other MSSQL, HTTPS uses 256 bit.  
2. Only Identification info encrypted by PHP, in all other cases encrypted by MSSQL.                                      |
| 27 June 2018    | Bruce Behymer      | Updated data in transit description to use 256-bit AES TLS 1.1 or higher. Passwords are now encrypted using the FIPS 140-2 certified 256-bit AES encryption available with MS SQL Server.         |
|                 |                    | All PII and secure UDFs are encrypted using the FIPS 140-2 certified 256-bit AES encryption available with MS SQL Server.                                                                                           |
Introduction

In order to minimize the effect on system performance, database encryption is only applied to fields where the sensitivity of the data being stored requires it. Some fields are encrypted with the Advanced Encryption Standard (AES) using the standard PHP libraries that are available for AES. Other fields are encrypted in the database using the column-wise FIPS 140-2 certified 256-bit AES encryption available with Microsoft SQL Server. The reason for this difference is purely historical in that Samaritan used the PHP AES libraries when encryption was needed before the native Microsoft SQL Server column-wise encryption became available. The following describes the on-disk and in-transit data encryption we use.
**Personally Identifiable Information PII:** All Personally Identifiable Information (PII) (names, addresses, birthdates, email addresses, and etc.) such as shown below is encrypted in the database using the column-wise FIPS 140-2 certified 256-bit AES encryption available with Microsoft SQL Server.

---

**Volunteer Profile: Behymer, Bruce**

<table>
<thead>
<tr>
<th>Personal</th>
<th>Group Type</th>
<th>Population Served</th>
<th>Geographic Area</th>
<th>Activity Type</th>
<th>Interests</th>
<th>Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additional**

<table>
<thead>
<tr>
<th>Availability</th>
<th>Other</th>
<th>Orientation/Training</th>
<th>References</th>
<th>Recognition</th>
<th>User Defined</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Attachments**

**History**

**Professions**

* Indicates required fields

- **Salutation:** None

- **First Name:** Bruce

- **Middle Name or Initial:**

- **Last Name:** Behymer

- **Gender:** None

- **Date of Birth:** 22 Jun 1962

**Street Address:**

1. 102 Sugarbush Dr.

2. 102 Sugarbush Dr.

**City:** Vista

**State:** California

**County:** Choose a county

**Zip:** 92084

**Country:** United States

**User ID:** 7824Zablu

**Password:** ********

**Password Verify:** ********

Volunteer needs User ID and Password (at least 6 symbols) to access profile and edit information

Would you like to receive volunteer opportunities periodically through your email address?

- [ ] Yes
- [ ] No

---

**eCoordinator Volunteer Profile With PII**
The volunteer profile identification tab: This tab was designed to store sensitive types of identification such as driver license or passport numbers that a person might use to identify himself. It is also used to verify the information that the volunteer entered when registering on-line via eRecruiter. When the volunteer shows up for his first meeting with a volunteer coordinator, the volunteer presents his identification and the coordinator enters it into this page. If the information does not match what the volunteer entered when registering then the volunteer coordinator is alerted and a note is automatically made in the volunteer’s background check history if a background check was performed using the invalid information previously entered. The Number and Expiration Date fields on this page are encrypted with 128-bit AES encryption and stored that way on disk.
The client profile special needs tab: The purpose of this tab is to record the special needs (possibly medical Personal Health Information or PHI) of a recipient of volunteer services such as a disabled person who is receiving a ride from a volunteer driver. Because the needs may be of a medical or other sensitive nature the fields of this profile tab are also encrypted with FIPS 140-2 certified 256-bit MS SQL native encryption and stored that way on disk.
Secure User Defined and Logged Data Fields: In order to provide for the encryption of data other than the specific types mentioned above, the ability to create “secure” user defined fields encrypted on disk was added as soon as column-wise encryption became available with Microsoft SQL Server. Secure user defined fields may be any of several types such as text, number, date, dropdown list, and etc. Samaritan also provides a complementary set of user definable “logged data” fields. These are fields used to record data from surveys that are stored in log books such as a record of each volunteer’s service hours, bags of trash collected, yards of trail cleared, satisfaction survey results, or other such historical data. The same level of encryption available for user defined fields is also available for logged data fields.

Creating or Editing an Encrypted Secure User Defined Field
Reference Surveys: It is Samaritan’s opinion that information collected in automated reference processing surveys from the references that a volunteer provides might be of a highly sensitive and confidential nature. So, reference survey information is also encrypted using the column-wise 256-bit encryption available in Microsoft SQL Server.
Passwords: All passwords are encrypted with an MD5 hash and then the hashed forms are encrypted using the FIPS 140-2 256-bit AES encryption available with Microsoft SQL server for storage in the database.

Security is as much about human control as it is data access controls. Samaritan’s staff is strictly governed by the terms of the Samaritan Security Policies and Procedures document. eCoordinator users are also restricted based on security roles configured according to each customer’s local policies. These security roles govern which profiles, profile details and system functions each user will be able to access. Each role can be set up and modified by the System Administrator at any time. An unlimited number of users can be attached to each role and there may be an unlimited number of roles, including roles that are unique to the requirements of a specific group.

Data in transit: All transmissions of sensitive data to and from Samaritan’s production application servers are to be accomplished via one of the following secure means:

- eCoordinator, eRecruiter, Sign-In, and the Exchange API use 128 or higher bit AES encryption (HTTPS) with Transport Layer Security (TLS) 1.1 or higher. Each of these interfaces also requires user id and password authentication.
- FTPS from specific IP addresses only via a firewall configured for this purpose.
- For Samaritan internal use only, Microsoft Remote Desktop Protocol with transport layer encryption enabled for Microsoft Windows servers from specific IP addresses only via a firewall configured for this purpose.
- For Samaritan internal use only, SSH for Linux servers.
- Bulk data files for import or export are to be encrypted before transmission with an encryption protocol (minimum 128 bit) agreed upon by Samaritan’s development team leader and the internal or external party exchanging data.
Appendix J: Disaster Prevention & Event Response (DPER) Plan
Summary

15 June 2018
Version 3.2

Contents

CONTENTS 104
REVISION HISTORY 104
INTRODUCTION 105
PLANNING 105
PREVENTION 107
PREPARATION 108
NOTIFICATION 110

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Jun 2018</td>
<td>3</td>
<td>Added Table of contents</td>
<td>Bruce Behymer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added this revision history</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reorganized document</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added operational section for company headquarters</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added financial preparation section</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added offsite backup storage at Amazon S3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added redundant service provider information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added redundant data center information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added data center failover plan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Replaced references to SSH with Windows RDP.</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Samaritan’s tested and real disaster event proven Disaster Prevention and Event Response (DPER) Plan organized into four basic areas: planning, prevention, preparedness, and notification. It encompasses multiple levels of redundancy that provide for business continuity in the event of any of several types of disaster.

Our plan also provides for continued assessment and improvement with committees that meet regularly. Many of the things documented in this summary change as we refine and improve our business continuity readiness. Additionally, for customer hosted systems, many of these items listed here will be different according to client specific policies.

This summary document is not the full plan, rather it is simply a list of the things that we already have or will shortly have in place to assure Samaritan’s business continuity on behalf of our customers. Items that yet to be implemented have the implementation timeframe in parentheses like this: (starting in 2018).

Planning

- Three member disaster recovery and event response planning team.
- Three member security committee
- Documented Policies and Procedures
  - Security Policies and Procedures
  - Disaster Prevention and Event Response (DPER) Plan
• Data Classification Policy
• Asset Management Policy
• I.T. Security Incident Response Policy
• Data Breach Response Policy
• Data Encryption
• Media Sanitization & Disposal Policy
• Privacy Policy
• Subscription and Services Agreement with Confidentiality and Service Level Agreement
• Change Management and Release Policy
• Event Client Notification Policy

• Meetings assessing issues and continuous improvement
  • Software Development Committee (weekly)
  • Multi-departmental Quality Assurance (weekly)
  • Client Services (weekly)
  • DPER committee/team readiness review and planning meetings (monthly)
  • Post-event analysis by DPER committee/team.

• Development
  • Security integrated into the software development lifecycle
  • All production software changes documented
  • All production software changes tested by QA team
  • Quality Assurance for every release includes
    ▪ Over 3,000 documented functional tests
    ▪ Almost 700 automated functional tests
    ▪ Unit tests
    ▪ Continuous Integration
      • Version Control
      • Automatic new build on each developer code commit
      • Automatic testing of each developer code commit
      • On-line build history with test status of each commit
    ▪ Section 508 and WCAG-2 accessibility testing
    ▪ OWASP ZAP tool vulnerability testing
- Performance testing
- Load testing to determine maximum number of simultaneous users

**Prevention**

- Completely separate business IT and production systems.
- Limited administrative access to servers via encrypted Windows RDP.
- Encryption
  - All passwords hashed at user’s browser before transmission.
  - All passwords and data transmitted in encrypted form.
  - All passwords and PII stored in encrypted form.
  - FIPS 140-2 certified 256-bit AES encryption engine
- Hardened servers:
  - Limited port accessibility (port numbers in parentheses)
    - Only HTTP (80) and HTTPS (443) using TLS 1.2 or above open to outside world.
    - Windows RDP (3389) accessible to limited Samaritan staff only
    - SMTP (25) for outbound email only
    - FTS/S (990) specific client IP addresses only
    - SFTP (22) specific client IP addresses only
    - All other ports disabled
  - Anti-virus with weekly or continuous signature updates
  - Server console access limited to Samaritan and data center staff
  - Firewalls separating all servers from open Internet
  - Monthly application of system file updates and security patches
  - All patches/Internetwork Operating System (IOS) upgrades are to be tested in a test environment before being released into the production.
  - Backup of the existing configurations taken prior to application of security patches/IOS upgrades and updates to network devices.
  - Settings and parameters reviewed after patch installations.
  - Only the Security Policy Committee Chair (SPCC), Vice President of Operations (VPO), the development team lead, or their designees are authorized to apply patch upgrades to network devices other than end user workstations.
  - All patches recorded in Samaritan’s asset register.
  - Retention of the evidence of all patch management reviews in the semi-annual audit logs.
- Monitoring
  - RASP-base server IDS and IPS developed by Samaritan locks out offending IP addresses, logs malicious behavior, and notifies staff.
  - Active system port activity, response, and intrusion monitoring.
  - Automatic outbound email blacklisting detection and notification

- Security Procedures
  - Semi-annual company security audits.
    - A periodic patch compliance review performed during the semi-annual security audit to ensure that all end-user computing devices and servers are installed with up to date patches and that any issues identified are tracked to closure.
    - The semi-annual security audit includes a validation review to ensure all critical/emergency patches were installed on all end-user computing devices.
  - Inquiry escalation procedures, callbacks, shredders, and a clean desk policy to prevent social engineering attacks.
  - A visitor log is maintained in our entry area.
  - Regular reviews of system access logs by support staff and corporate security officer.

- Development
  - Vulnerability testing of our volunteer management software using standard industry tools such as OWAS Zap by Samaritan’s quality assurance team followed by remediation as needed by Samaritan’s development team as part of every new software release.

- Operational (Salt Lake City company headquarters)
  - Anti-virus installed on all staff computers with weekly or continuous signature updates
  - Staff computers audited for adherence to policies
  - Office network equipment audited for adherence to policies
  - Background checks for all staff
  - Monthly staff security training
  - Office entrance always locked to outside
  - Building locked outside of business hours
  - Video surveillance of building and office entrances

Preparation
- Bare-metal disaster server recovery fire drills.
- Semi-annual readiness audits and system tests.
• World class data centers
  o Rackspace (ISO 27001 and SOC 2 compliant)
  o IBM SoftLayer (FedRAMP authorized)
  o Redundant physically separate Internet feeds
  o Redundant back up power generation
  o Redundant HVAC systems
  o Redundant network systems
  o Fire suppression systems
  o 24/7/365 staff availability with systems expertise
  o Biometric server floor access control limited to data center staff only
  o Proven economic viability through recessions and industry pull-backs

• Backup
  o Nightly backup to network storage of OS and system applications
    ▪ four week retention
    ▪ Stored off-server to network storage
    ▪ Bare metal system recovery fire drills
  o Nightly client database instance and software disk based backups that are either immediately available or can be mounted with about an hour’s notice that users can log into just like the production systems for fast easy recovery of data lost due to human error.
    ▪ Most recent backup redundantly stored on a local server hard disk
    ▪ Offsite backup storage at Amazon S3 (in 2018)
    ▪ 30 day retention

• Failover for data center failure makes use of our two data centers (Rackspace and IBM SoftLayer) each of which hosts roughly half of our clients and the offsite backup of each client’s database and software at Amazon S3.
  o In the event of a complete data center failure:
    ▪ Amazon S3 backups of client database instances and software are restored to alternate data center (starting in 2018)
    ▪ DNS A records at our redundant DNS providers are changed to point to alternate data center: Rackspace or IBM SoftLayer (starting in 2018)
  o Data center failover rehearsals (starting in 2018)
  o Round the clock availability of disaster recovery event team members.

• Service provider redundancy
- Redundant DNS providers
- Redundant outbound email servers
- Redundant server monitoring services

- Operational (Salt Lake City company headquarters)
  - Redundant local and cloud based storage of important documents, company/financial data and software.
  - Staff computers audited for adherence to policies
  - Office network equipment audited for adherence to policies
  - Monthly staff security training
  - Smoke detectors, alarms, and fire extinguishers installed in all work areas.
  - Smoke detectors, alarms, and fire extinguishers tested on an annual basis.
  - In the event that Samaritan’s staff offices are unavailable due to a power outage or other event, senior management will decide whether or not to permit the staff to work from home. Many of our staff members currently telecommute one day per week.
  - Phones can be forwarded to home offices
  - No on-site servers at company offices. All central IT services make use of cloud based service providers.
  - Paper based policies and local PC-based software provide redundancy for cloud based providers
  - Staff distributed in six widely separated geographic locations
  - Staff members redundantly trained in all responsibilities to eliminate single person dependencies.

- Financial
  - 20 year history of operation
  - No individual client represents more than five percent of revenue
  - Multiple lines of credit in place to provide contingency funding
  - Use a nation-wide multi-branch bank
  - Customer base distributed across several market segments/industries

Notification

- Automatic logging notification of development team in the event of critical software errors.
- Redundant automatic live database system monitoring with automatic notification of our event response team (and the customer for all except Samaritan’s multi-tenant SaaS hosting option.)
- Disaster event response escalation notification procedures with designated and redundant points of contact at Samaritan.

- System failures or other DPER incidents are reported to the Samaritan Security Policies Committee (Infosec), the vice-president of client services, the development team lead, and the account manager for any customers affected by the incident. The vice president of client services convenes a response team to determine the severity and extent of the incident. Once the severity and extent has been determined the vice president of client services will decide whether or not the appropriate client service teams should proceed to notify any affected clients per each client’s event/emergency/privacy/security notification lists. If such notification is provided then the vice president of client services will see that regular progress and remediation reports (at least daily if not more frequently) are provided to the affected clients until such time as the issues has been resolved. The vice president of client relations will also see that notice of final resolution and steps taken to prevent recurrence is provided to the affected clients once resolution is complete.

**Overview of Data Center Loss Recovery**

Samaritan provides several levels of backup and recovery:

Samaritan has two data centers: One hosted by IBM SoftLayer and managed by RapidScale and one hosted and managed by Rackspace with roughly half of Samaritan’s clients hosted in each data center. In each data center nightly backups are made of the server operating system and other system files. These are nightly incremental backups with weekly full backups with four week retention. Separately, each client database instance is backed up along with the specific version of Samaritan’s volunteer management software that client is running at the time to a large hard disk on the server with up to 30 days retention. These database and software backups are mountable in 15 to 20 minutes in such a way that once mounted our clients can log into them just as they would log into their normal Samaritan volunteer management system. We use these system to protect against human error on the part of our clients which we have found to be the most common source of data loss. Once the client has logged into the restored backup and identified the records that need to be restored our client service team restores them from the backup database to the live system. We are well practiced at this procedure.

As of this writing (June 2018) we are in the process of extending this system to allow us to recover from a complete data center loss as follows:

1. Each night the backups of each client’s data base and current version of our VMS software are copied to private encrypted Amazon S3 storage. As of this writing we have stored private encrypted backups in Amazon S3 storage but we are still in the process of implementing and testing steps 2, 3, 4, and 6 below. We expect this work to be completed during 2018.

2. In the event of a data center loss the backups are copied from the Amazon S3 storage to our servers at the still operational data center where they are mounted and made available for login.
3. Samaritan staff changes the DNS A records for the clients that were hosted at the non-operational data center to point to the still operational data center where their systems are newly hosted.

4. Samaritan staff sets the DNS T records for the clients that have been re-hosted to their minimal values to let DNS servers around the world quickly know that they need to update their records for the clients that have been moved.

5. As of this writing Samaritan already uses two domain name services, Rackspace and Dreamhost, so that DNS services are not a single point of failure.

6. Samaritan’s staff contacts and works with those clients that have integrations that make use of hard coded IP addresses to update their systems to make use of the new IP addresses of their volunteer management systems.
Appendix K: Outage Notification Procedure

Last updated by: Keith Leonard
Date: 1 June 2018
Primary document location: Samaritan Knowledge Base

1. Outage starts.
2. Every 3 mins the Pingdom and Samaritan Monitoring System checks instances.
3. Pingdom and Samaritan Monitoring System notifies the list of contacts (Support, IT)
4. One of the notification contacts confirms the outage.
5. Person emails "reply all" confirming the outage or identifying the false positive.
7. As clients contact Samaritan Support links tickets to "Incident".
8. Support / Account Management filters list from CRM of affected instances on the affected server.
9. Support/ Account Management filters list from CRM of affected client contacts based on the affected server/instances.
10. Support / Account Management creates email and notifies clients
11. Support / Account Management continues communication as updates are available or as designated by the Response Team. This could be every 1/2 hour, hour, etc. until the outage is resolved.
12. Once resolved, a Response Team creates a Recovery Team
13. Recovery Team performs a root cause analysis.
15. Recovery Team implements the prevention plan.
16. Support / Account Management communicates the results from the root cause analysis and prevention plan.
Appendix L: Software & Configuration Management & Release Processes

Version 1.6
29 November 2016

Contents

REVISION HISTORY ...................................................................................................................................................... 115
1. OVERVIEW .......................................................................................................................................................... 115
2. AUDIENCE .......................................................................................................................................................... 115
3. STANDARD SOFTWARE CHANGE MANAGEMENT AND RELEASE PROCESS ........................................ 116
4. EXPEDITED SOFTWARE CHANGE AND RELEASE PROCESS ........................................................................ 119
5. EMERGENCY SOFTWARE CHANGE AND RELEASE PROCESS ..................................................................... 121
6. STANDARD NETWORK / SERVER CONFIGURATION CHANGE PROCESS ..................................................... 122
7. EXPEDITED NETWORK / SERVER CONFIGURATION CHANGE PROCESS ..................................................... 124
8. EMERGENCY NETWORK / SERVER CONFIGURATION CHANGE PROCESS ..................................................... 125
Overview

At Samaritan Technologies we offer several web-based volunteer management services and tools that interact with a database of volunteer, opportunity, organization, and logbook records. The information stored in this database belongs to our clients which they use on a day-to-day basis to coordinate millions of volunteers. Thus, as providers of these services we have a responsibility constantly update our software and services to facilitate this vital work they do. We also need to make sure that the process of upgrading our software with new features is as smooth as possible to minimize any disruption the upgrade process may cause. This document provides our company process for software change management and the release process for achieving this objective.

Audience

The intended audience for this document consists of all of Samaritan's employees, consultants, and partners. As a team we all share the responsibility of making sure we offer the best product possible within our means. This document may also be shared with existing and potential clients.
Standard Software Change Management and Release Process

Our software change management and release processes are as follows:

Our development team maintains an on-line database called Jira that is used to record all known defects, suggestions for changes, and feature requests. Additionally, our client services team maintains a separate database (ZenDesk) used for tracking all customer service requests including feature requests and bug reports. We have established an integration between the two systems so that bugs and feature requests can flow directly from Client Services to Development. For each item these databases also tracks the status, priority, steps to reproduce, and history of each item as well who the item is currently assigned to.

Each time an item is entered into the Jira it is grouped into a functional area and assigned to a developer who makes and records a work level estimate and risk assessment for the item. With this information recorded, it is easy for our product development committee to see what related items a developer could address while working in a given area of the code and what the impact of each item will be to the overall product schedule.

For minor changes, features, and bug fixes a detailed description often including a mocked up screen shot is provide as part of the Jira entry.

If customer paid development work is to be included in a release then the sales proposal or contractual statement of work typically functions as the business requirements document. This will often include a gap analysis to determine which aspects of the customer’s needs can be met by configuration of existing functionality and which, as the result of a gap analysis, require new development. Once an agreement is signed, Samaritan’s product manager will interview the client to develop personas, and use cases that will be included in the feature requirements and ultimately a traceability matrix.

For major new features or enhancements a system requirements specification (SRS) document is created that includes background information describing the motivation for the new feature, a list of the related Jira database entries, the market requirements for the feature, and a detailed functional specification including screen shots, and a document change history. Sometimes a functional prototype using a tool such as Axure may also be created to better support an agile development methodology and better communicate a sense of the new functionality to all stakeholders.

If the new feature is being developed for a specific client then the SRS and/or prototype has been written based upon specific needs input obtained from the client often as part of a Business Requirements Document (BRD). Often the initial statement of work or sales proposal will function as the BRD. Once the SRS and/or prototype is complete it is then provided to the client for a walkthrough, review, iteration if needed, and sign-off.
From the SRS and/or prototype or Jira items the development team creates a work breakdown structure, assigns resources, and develops a project plan/schedule typically as an on-line interactive and collaborative GANTT chart (using Smartsheet). The project is then reviewed by the development team and managers who look for schedule optimizations as well as for high risk items that should be advanced in the schedule.

If a new feature is being developed for a specific client then the project plan and schedule is presented to the client for a walkthrough, review, iteration if needed, and sign-off at this point before any implementation work begins. Use of an online GANTT chart also permits the client to view the progress of the project at any time.

Once the project plan is approved by the Product Development Committee (PDC) the development team begins implementation on a set of test servers that we maintain in parallel to our production servers.

While the development team begins implementation of the project the quality assurance team begins designing the various functional, error, load, stress, vulnerability/security, accessibility, and usability tests. The test cases used to verify each feature are recorded in a tool called Test Link which allows us to track overall test completeness as we progress toward each release. We use a combination of manual and automated testing. With an extensive suite of automated regression tests that can be applied to each new build. As of this writing we currently have over 500 automated tests and over two thousand documented manual tests that are applied to each release. As soon as each functional element becomes operational the QA team begins testing on the test servers. All bugs are recorded in Jira.

Once a functional element becomes sufficiently stable, it is made available via our test servers to our customer service staff, project managers, and external beta test sites for usability testing. Results of the input from these usability testers is evaluated and as is appropriate incorporated into the feature design and the product, SRS and/or prototype are updated accordingly.

For the initial builds of the new release the quality assurance team applies their testing to assure conformance to the SRS or Jira write ups. However, this requirement is loosened as usability testing begins since new user feedback may take priority over the original design.

Our developers maintain our code under version control (using SVN, Star Team, or Git, or BitBucket) so that at any point we can roll back code changes as necessary.

Once all of the major functionality has been implemented a second data migration test database is created on the test servers in parallel with the other quality assurance test databases. This is database is specifically used to test our ability to maintain data integrity as we migrate the live production data to the new system. Production data migrated to this system is obfuscated to hide any Personally Identifiable Information (PII) or Protected Health Information (PHI).
The iterative process of bug fixing and usability enhancements continues with the product or project managers continually evaluating and prioritizing all Jira items related to the project until all critical items have been addressed.

During this debug period the development team also implements and update unit tests that are added to Samaritan’s Jenkins based Continuous Integration (CI) system. Each new build of the new release is created using the CI system which runs builds the software, runs it through a series of automated unit tests and standard PHP code cleanliness tools such as phpcpd, phpmrd, and phpcs, and installs the software as a specified set of instances on a specified set of servers as well as reporting on the success or failure of each step in the operation.

When the system appears to be ready for release, if new upgraded servers have been used for the test servers then these servers will typically become the new production system. Otherwise, the new database and software will be set up in parallel on the existing production servers and go through a final system test there.

If the expected configuration / implementation completion date for a new customer using a dedicated database instance of our software is expected to be after the release date of the version of our software currently under development then we will deploy the pre-release version of our software for that new customer. Then if any defects are found in the software during the deployment for that new customer we can make sure that they are fixed during the development and quality assurance process for that new version of the software. This allows us to assure that the new version will work correctly as configured for the new customer.

Again, as bug fixes are deployed they are run through our CI system of automated unit and quality tests and any resulting issues are addressed.

For existing customers with any of the non-multitenant SaaS hosting options (dedicated database instance, dedicated virtual server, dedicated physical server, self-hosted) the deployment of a new version of our software will first take place in a quality assurance instance of the software which will undergo customer specific customization and user acceptance testing by the customer before it is deployed in the customer’s production environment.

Non-multitenant SaaS customers can work with our Client Services department to schedule their upgrades at a date and time that is convenient for them. The production environment for our multi-tenant SaaS customers is upgraded as each release becomes available typically three to four times per year.

Release announcements are sent out to our client base 1 to 2 weeks prior to the release date. These announcements typically state that the release is scheduled to happen on a Thursday night between 6 pm Pacific Time and 8 am Eastern Time the following day. During this time our clients are advised that they can access their data and run reports, but any changes that they make may not be preserved. Similar warnings are posted on our login pages. In reality most
upgrades only take a couple hours, but we allow ourselves the entire night should any problems arise.

After the release begins a final data migration is performed from the live database, final manual and automated sanity tests are performed, and then if needed the DNS records are updated to point to the proper servers, the warnings are removed, and the QA and Project managers sign off on the release.

Just in case any critical problems arise the old system is left up and running and the QA and development teams are kept on alert during the two weeks after the release should there be any urgent need to revert to the prior system.

If isolated critical changes arise that need to be implemented between major releases then the changes are first implemented and tested by our QA staff and sometimes end users on our test servers before being applied to the live production system. See “Expedited Software Change and Release Process” below.

Finally, an analysis of any bugs reported post release is performed so that the communication, design, development and QA processes can be enhanced to catch and prevent any similar problems from occurring during the next release.

When a defect is encountered in a released version of our software, it is first entered into Samaritan’s customer support incident database. Depending upon the urgency and severity of the defect members of the Samaritan’s Quality Assurance, Development, and Client Services team will either meet immediately to discussing the issue and plan its resolution, or they will discuss the issue in the next weekly quality assurance meeting. (See the expedited and emergency software change and release processes below.) Once a resolution plan has been put into place the fix is first implemented in a test environment. Once correct operation has been verified in the test environment then the fix is be applied to the production environment and re-verified there after sufficient notice to or coordination with the client has taken place.

All such changes are submitted to version control and associated with the appropriate version label as well as being applied to the next version under development.

**Expedited Software Change and Release Process**

When a customer requests a small change and requests to be expedited between releases, the following process describes how that change is implemented.

19.1. Account manager, client services, or product manager composes feature request as a Jira ticket, including a required user story and business need.

19.2. Product manager schedules business need for review in Product Development Committee meeting.
19.2.1. If the PDC agrees that the business reasons and benefits provided by the potential feature are not great enough to offset the opportunity, labor, and other costs, the feature request will be archived, and may be included in the regular release process moving forward, and the expedited software process concludes.

19.2.2. If the PDC agrees that the feature request fulfills a valid business need and will hold mutual benefit for the client and the company, the expedited software process continues.

19.3. Feature request is approved by product manager.

19.4. Product manager forms design committee with relevant stakeholders, potentially including product manager, account manager, development team, client, and/or other support staff.

19.5. Design committee designs new feature based on user story and business need.

19.6. Security committee reviews and approves new feature design against security requirements and policies.

19.7. Product manager approves new feature design.

19.8. Feature request is assigned to development team lead.

19.9. Developers compose and apply new code to customer-specific QA or other test instance.

19.10. Upon code completion, QA team lead assigns to QA team members for testing.

19.11. Testers and coders engage in the standard iterative testing and bug fixing process.

19.12. Product manager, client/end-user, and/or account manager perform acceptance testing.

19.12.1. Client, coders, and testers engage in iterative acceptance process. Jira and/or Smartsheet will be used to document client feedback.

19.12.2. Client and/or product manager acceptance will be documented in appropriate Jira tickets.


19.14. Upgrade notices with expiration dates posted to login pages by account manager no later than 10 days prior to scheduled production upgrade.

19.15. Development team creates back up of production instance in case problems are encountered during or after the upgrade.

19.16. Development pushes new feature to appropriate production instance, and registers new build number.

19.18. Product manager updates appropriate Jira tickets with tags and labels (e.g., version, component, client name) for future reference.

19.19. All expedited development is discussed each week in weekly client services / product manager meeting.

**Emergency Software Change and Release Process**

19.20. Issue is received by the Development Team Lead (DTL).

19.21. Issue requiring change is received by customer support, or client services or some other department.

19.22. The person receiving the reported issue verifies the issue.

19.23. The person receiving the issue reports it to the Vice President of the Client Services or in his/her absence to the Director of Development who becomes the Issue Lead (IL).

19.24. The issue lead forms an Issue Resolution Committee (IRC) with the Development Team Leader or the most senior developer available at the time.

19.25. The IRC evaluates the issue and decide whether the issue requires immediate action, possible actions to resolve the issue, the risks associated with each action, and on which client instances the actions should be taken. The results of these decisions become the Issue Action Plan (IAP)

19.26. If the issue requires immediate action then the IRC instructs the Development Team Leader or most senior developer to be the Corrective Action Implementer (CAI) and to implement the necessary action on the client instances selected in the previous step.

19.27. The IL reports the IAP to Samaritan’s Support department.

19.28. Samaritan’s customer support team reports the IAP to the client the planned corrective action and that it is in progress.

19.29. The Development Team Leader or most senior developer available implements the change on the selected client instances.

19.30. The AI verifies the corrective action.

19.31. The IL verifies the corrective action.

19.32. The Reporter verifies the corrective action.

19.33. Samaritan’s customer support department reports that the corrective action to the client and requests that the client verify the corrective action.

19.34. The client verifies the corrective action.
19.35. The AI will create a Jira ticket describing the corrective action.

19.36. The AI assigns the Jira ticket to the Quality Assurance Team Lead for verification and regression testing.

19.37. The AI sends an email to the Samaritan development email group reporting the issue, the corrective action taken, the client instances affected, and the Jira ticket number.

19.38. The Quality Assurance Team verifies the corrective action and performs regression testing of the product areas affected by the corrective action.

19.39. The Quality Assurance team updates the Jira ticket with a subsequent related issues that they find or closes the ticket.

19.40. The Quality Assurance Team Leader having received the email sent by the AI schedules the issue for discussion in the weekly Quality Assurance Status meeting.

19.41. In their next weekly meeting the Quality Assurance Status Meeting members discuss the issue and determine if the corrective action or another long term fix should be implemented and to which customer instances release versions of the software the fix should be applied and assigns a member of the group to create and assign Jira tickets for following up on their decisions until the issues are closed.

19.42. The development team implements the follow up Jira tickets assigned to them then assigns each Jira ticket to the Quality Assurance Team for verification and closure.

19.43. The Quality Assurance Team the Quality Assurance Team verifies the tickets and iterates the issues with the development team until such time that the Jira tickets can be closed.

19.44. The Quality Assurance Team closes the Jira tickets.

19.45. The members of the Quality Assurance Team perform a post issue analysis to determine the cause of the issue and assign actions to be taken to prevent the issue or similar issues from occurring in the future.

**Standard Network / Server Configuration Change Process**

19.46. Based upon an emerging business need (security, continuity, marketing, and etc.), a contractual obligation, or an approaching capacity limitation, a member of the Product Development Committee (PDC) or Client Services Team (CST) recognizes the need for a Hardware/System Configuration Change Request (H/SCCR).

19.47. The PDC includes representatives from the Design, Development, Quality Assurance, and Client Services teams.

19.48. If the member of the PDC or CST will meet with the Vice President of Client Services (VPCS) and the Development Team Lead (DTL) to determine if the change request is minor and low risk should be handled via the Expedited Network / Server Configuration
Change Process or continue with the Standard Process. If the Expedited Process is selected then the change request proceeds through that process otherwise the change request proceeds as follows.

19.49. The PDC or CST member will submit a request to the Product Manager to add the H/SCCR to the weekly PDC meeting agenda.

19.50. The PDC reviews the H/SCCR to confirm the business need, examine alternatives, approve or disapprove the H/SCCR and if approved schedule its implementation.

19.51. If the H/SCCR is approved by the PDC then it is assigned to the Development Team Lead (DTL) who creates a Jira ticket for it.

19.52. The DTL meets with the Vice President of Client Services and Development Director (DD) to determine the best approach for implementing the H/SCCR and to develop and Action Plan (AP).

19.53. The DTL updates the Jira ticket with the action plan.

19.54. If the action plan requires scheduled down time then the DTL posts scheduled down time notices on the login pages for the instances of Samaritans systems that will be affected by the H/SCCR.

19.55. The DTL submits a ticket for the H/SCCR to the ticketing system of the hosting service either Rackspace or RapidScale. The hosting service ticket includes the details of the action plan and schedule for implementation.

19.56. If the H/SCCR is for a major system change such as a server upgrade then the new system will be built and brought up in parallel with the existing production system.

19.57. Once the H/SCCR has been implemented the hosting service representative updates the ticket in the hosting service ticketing system and assigns the ticket back to the DTL.

19.58. The DTL verifies the changes made by the hosting service.

19.59. The DTL assigns Jira Ticket installs and verifies the operation of any additional software that may be required by the H/SCCR.

19.60. The DTL assigns the internal Samaritan Jira ticket to the Quality Assurance (QA) team.

19.61. The QA team verifies the operation of the system according to the action plan and iterates with the DTL who may iterate with the hosting service as necessary.

19.62. Once the QA team verifies the operation of the system they state such in the Jira ticket and assign the ticket back to the DTL.

19.63. If the H/SCCR specifies a new server or backup and recovery system, then the DTL coordinates a backup and disaster recovery fire drill of the new system and iterates until the fire drill is successful.
19.64. The DTL coordinates with the VPCS to schedule the transfer of the production instances of Samaritan’s Volunteer Management System (VMS) to the new system and makes sure that the transfer process is detailed in the action plan and that staff members are aware of their roles in the plan and the schedule.

19.65. The VPCS confirms that the scheduled downtime notices have been in place for sufficient time.

19.66. The DTL Coordinates the transfer as detailed in the action plan.

19.67. The transfer typically will involve verification of the new production system, software, and data by the Quality assurance team in which case the DTL will assign the Jira ticket to them.

19.68. The QA team verifies the operation of the new system and software iterating with the development team as needed.

19.69. Once the QA team has verified correct operation, they update the Jira ticket and assign it back to the DTL.

19.70. The DTL removes the downtime notices and closes the ticket.

19.71. The old production system is left up and running for two weeks should there be a need to quickly revert back to the old system.

19.72. The Product Manager schedules a review of the H/SCCR for the following PDC meeting.

19.73. At the following PDC meeting the members review the upgrade and determine there are any process changes or improvements that need to be made to the action plans for future H/SCCRs.

**Expedited Network / Server Configuration Change Process**

19.74. The VPCS receives, reviews and approves or disapproves the change request. Approved change requests proceed as follows:

19.75. The VPCS approves the change request in the Jira Ticket.

19.76. The DTL creates a Change Request Ticket (CRT) in the hosting service ticketing system for either Rackspace or Rapid Scale.

19.77. The hosting service assigns a technician to implement the CRT.

19.78. The technician implements the CRT.

19.79. The technician updates the CRT with the implementation status once the change request has been implemented and assigns the CRT back to the DTL.
19.80. The DTL verifies the change and iterates via the CRT with the hosting service until the DTL is able to confirm successful verification.

19.81. The DTL updates the Jira Ticket to record the verified implementation.

19.82. The DTL will reassign the Jira Ticket to the person (requestor) who made the change request.

19.83. The requestor verifies the change and closes the ticket.

**Emergency Network / Server Configuration Change Process**

19.84. The DTL or a member of the Client Services or Development teams receives notice of an issue from an automated monitoring system or a client.

19.85. The person receiving the report issue verifies the issue.

19.86. The person receiving the report sends out an email notice of the issue to the DTL, Director of Development (DD), VPCS, and QA teams.

19.87. The person receiving the issue reports it to the Vice President of the Client Services or in his/her absence to the Director of Development who becomes the Issue Lead (IL).

19.88. The IL assigns the VPCS or a member of the CS team to notify any affected clients that Samaritan is aware of the problem and has started work on it.

19.89. The IL opens a ticket on the hosting service’s ticketing system.

19.90. The IL forms an Issue Resolution Committee (IRC) with the DTL or the most senior developer available at the time and a Hosting Service Representative (HSR).

19.91. The IRC evaluates the issue and decide whether the issue requires immediate action, possible actions to resolve the issue, the risks associated with each action, and on which client instances the actions should be taken. The results of these decisions become the Issue Action Plan (IAP) which may include things up to disaster recovery, failover, and system replacement. See the Summary of Samaritan’s Disaster Prevention and Event Response Plan document.

19.92. The IL opens a Jira ticket to record the IAP.

19.93. The HSR updates the hosting system ticket with the IAP.

19.94. If the issue requires immediate action then the IRC instructs the Development Team Leader or most senior developer to be the Corrective Action Implementer (CAI) to coordinate with the HSR and to implement the necessary action on the client instances selected in the previous step.
19.95. The IL reports the IAP along with an estimated time of restored system availability to Samaritan's Support department.

19.96. Samaritan’s customer support team reports the IAP to the affected clients and that it is in progress.

19.97. The CAI and HSR implement the IAP.

19.98. The CAI verifies results of the IAP and iterates as needed with the HSR.

19.99. Once the CAI has verified restored operation the CAI informs the IL that the system is available again.

19.100. The CAI updates the Jira Ticket.

19.101. The HSR updates the hosting service ticket.

19.102. The IL verifies the corrective action and updates the Jira ticket.

19.103. The IL assigns the Jira Ticket to the QA team who verifies correct operation of the restored system.

19.104. The QA team performs a sanity test on the system to verify the restored operation and iterates with the CAI and HSR if necessary.

19.105. The QA team updates the Jira ticket once the sanity test is successful and assigns the Jira ticket to the IL.

19.106. The IL assigns Samaritan’s customer support department to contact the affected client(s) and inform them of the restored system operation.

19.107. The IL assigns the Jira ticket to Samaritan’s QA Team Leader.

19.108. The IL sends an email to the Samaritan development email group reporting the issue, the corrective action taken, the client instances affected, and the Jira ticket number.

19.109. The Quality Assurance Team Leader having received the email sent by the IL schedules the issue for discussion in the weekly Quality Assurance Status meeting.

19.110. At the following QA Status meeting the members review the upgrade and determine there are any process changes or improvements that need to be made to prevent reoccurrences of the issue and assign action items to that end.

19.111. The development team implements the follow up Jira tickets assigned to them then assigns each Jira ticket to the Quality Assurance Team for verification and closure.

19.112. The QA Team verifies the tickets and iterates the issues with the development team until such time that the Jira tickets can be closed.

19.113. The Quality Assurance Team closes the subsequent Jira tickets.
19.114. The QA team closes the original ticket.
Appendix M: Privacy Statement

Effective as of 27 April 2016

Samaritan Technologies, ("Samaritan" or the “Company”) is committed to protecting the privacy of individuals who visit the Company’s Web sites ("Visitors"). This Privacy Statement describes Samaritan’s privacy practices in relation to the use of the Company’s Web sites and the related applications and services offered by Samaritan (the “Services”).

1. Web sites covered

This Privacy Statement covers the information practices of Web sites that link to this Privacy Statement, including: https://www.samaritan.com and https://support.samaritan.com (collectively referred to as “Samaritan’s Web sites” or “the Company’s Web sites”). Samaritan’s Web sites may contain links to other Web sites. The information practices or the content of such other Web sites is governed by the privacy statements of such other Web sites. The Company encourages you to review the privacy statements of other Web sites to understand their information practices.

2. Information collected

When expressing an interest in obtaining additional information about the Services or registering to use the Services, Samaritan requires you to provide the Company with personal contact information, such as name, company name, address, phone number, and email address (“Required Contact Information”). When licensing the Services, Samaritan may require you to provide the Company with billing information, such as billing name and address, credit card number, and the number of employees within the organization that will be using the Services (“Billing Information”). Samaritan may also ask you to provide additional information, such as support or procurement contacts (“Additional Information”). Required Contact Information, Billing Information, and Additional Information about Customers are referred to collectively as “Data About Samaritan Customers”.

As you navigate the Company’s Web sites, Samaritan may also collect information through the use of commonly-used information-gathering tools, such as cookies and Web beacons (“Web Site Navigational Information”). Web Site Navigational Information includes standard information from your Web browser (such as browser type and browser language), your Internet Protocol (“IP”) address, and the actions you take on the Company’s Web sites (such as the Web pages viewed and the links clicked).
3. Use of information collected

The Company uses Data About Samaritan Customers to perform the services requested. For example, if you fill out a “Request Demo” Web form, the Company will use the information provided to contact you about your interest in the Services.

The Company may also use Data About Samaritan Customers for marketing purposes. For example, the Company may use information you provide to contact you to further discuss your interest in the Services and to send you information regarding the Company, its affiliates, and its partners, such as information about promotions or events.

Samaritan uses Web Site Navigational Information to operate and improve the Company’s Web sites.

4. Web Site Navigational Information

Cookies, Analytics and IP Addresses

Samaritan uses commonly-used information-gathering tools, such as cookies and analytics, to collect information as you navigate the Company’s Web sites (“Web Site Navigational Information”). This section describes the types of Web Site Navigational Information used on the Company’s Web sites and how this information may be used.

Cookies

Samaritan may make use of cookies to make interactions with the Company’s Web sites easy and meaningful. When you visit one of the Company’s Web sites, Samaritan’s servers send a cookie to your computer. Standing alone, cookies do not personally identify you; they merely recognize your Web browser. Unless you choose to identify yourself to Samaritan, either by requesting a demonstration or information or filling out a Web form you remain anonymous to the Company.

Samaritan uses cookies that are session-based and persistent-based. Session cookies exist only during one session. They disappear from your computer when you close your browser software or turn off your computer. Persistent cookies remain on your computer after you close your browser or turn off your computer.

The following sets out how Samaritan uses different categories of cookies and your options for managing cookies’ settings:
Type of Cookies Description Managing Settings

**Required cookies**

Required cookies enable you to navigate the Company’s Web sites and use its features, such as accessing secure areas of the Web sites and using Samaritan Services. If you have chosen to identify yourself to Samaritan, the Company uses cookies containing encrypted information to allow the Company to uniquely identify you. Each time you log into the Services, a cookie containing an encrypted, unique identifier that is tied to your account is placed on your browser. These cookies allow the Company to uniquely identify you when you are logged into the Services and to process your online requests. Because required cookies are essential to operate the Company’s Web sites and the Services, there is no option to opt out of these cookies.

**Targeting or Advertising cookies**

From time-to-time, Samaritan engages third parties to track and analyze usage and volume statistical information from individuals who visit the Company’s Web sites. Samaritan sometimes uses cookies delivered by third parties to track the performance of Company advertisements. For example, these cookies remember which browsers have visited the Company’s Web sites. The information provided to third parties does not include personal information, but this information may be re-associated with personal information after the Company receives it.

**IP Addresses**

When you visit Samaritan’s Web sites, the Company collects your Internet Protocol ("IP") addresses to track and aggregate non-personal information. For example, Samaritan uses IP addresses to monitor the regions from which Customers and Visitors navigate the Company’s Web sites.

**Browser Statistics**

When you visit Samaritan’s Web sites, Samaritan may collect information about the Internet Browser that you use in order to best prioritize the browser support we offer.
Third Parties

Samaritan does not authorize the collection of personal information by third parties through advertising technologies deployed on the Company’s Web sites, nor do we share personal information with any third parties collected from the Company’s Web sites. Section 4 of this Privacy Statement, Web Site Navigational Information, specifically addresses the information we collect through cookies.

Compelled Disclosure

Samaritan reserves the right to use or disclose information provided if required by law or if the Company reasonably believes that use or disclosure is necessary to protect the Company’s rights and/or to comply with a judicial proceeding, court order, or legal process.

5. Electronic Newsletters and Communications Preferences
Samaritan sends electronic email newsletters to Visitors and Customers who provide contact information. You may manage your receipt of the email newsletters by emailing a request to opt_out@samaritan.com or contacting us at (801) 328-3972 x4 or (888) 904-6060 x 4.

6. Correcting and updating your information
Customers may update or change their contact information by calling (801) 328-3972 x4 or (888) 904-6060 x 4. To update Billing Information please email billing@samaritan or call (801) 328-3972 x5 or (888) 904-6060 x 5. Requests to change, or delete your information will be processed within 2 business days.

7. Customer Data

Samaritan Customers may electronically submit data or information to the Services for hosting and processing purposes (“Customer Data”). Samaritan will not review, share, distribute, or reference any such Customer Data except as provided in Samaritan’s Subscription and Services Agreement with the customer, or as may be required by law. Additional information about the Company’s privacy and security practices with respect to Customer Data is available here.

8. Security
Samaritan uses robust security measures to protect Data About Samaritan. Because the Company uses the Services to maintain Data About Samaritan Customers, this information, which is stored in the Services, is secured in the same manner as described here.

9. Mobile applications

Without limiting the generality of this Privacy Statement, in addition to information gathered through its Web sites or submitted to its Services, Samaritan may obtain information through applications (“Mobile Applications”) that Customers or their authorized individuals (“Users”) download to, and run on, their mobile devices (“Devices”). Mobile Applications provided by Samaritan may obtain information from, or access data stored on, Users’ Devices to provide services related to the relevant Mobile Application. For example, a Mobile Application may: access a camera on a User’s Device to enable the User to upload photographs to the Services; access the call history on a User’s Device to enable the User to upload that information to the Services; to allow the User to sync contact information between the information that is stored on the User’s Device and the information that is submitted to the Services. Information obtained to provide Mobile Application services may include information obtained in preparation for anticipated updates to those services. Mobile Applications may transmit information to and from Devices to provide the Mobile Application services.

Mobile Applications may provide Samaritan with information related to Users’ use of the Mobile Application services, information regarding Users’ computer systems, and information regarding Users’ interaction with Mobile Applications, which Samaritan may use to provide and improve the Mobile Application services. For example, all actions taken in a Mobile Application may be logged, along with associated information (such as the time of day when each action was taken).

Customers may configure Samaritan Mobile Application services, and the information accessed or obtained by the Mobile Application on a User’s Device may be affected by the Customer’s configuration. In addition, if a Customer purchases more than one Service from Samaritan and its affiliates, a Mobile Application may be designed to interoperate with those Services; for instance, to provide a User with access to information from any or all of those Services or to provide information from a User’s Device to any or all of those Services. Information accessed or obtained by the Mobile Application on a User’s Device may be accessible to the Customer and its organization, depending on the intended functionality of the Mobile Application.

Notices and contractual terms related to a particular Mobile Application may be found in the relevant terms of service for that application. The Company encourages you to review relevant terms of service related to any Mobile Applications you download, install, use, or otherwise interact with to understand that Mobile Application’s information practices.
The Mobile Application’s access to information through a User’s Device does not cause that information to be “Customer Data” under Samaritan’s Subscription And Services Agreement with the Customer or under this Privacy Statement, except as follows: To the extent that a User uses a Mobile Application to submit electronic data and information to a Customer account on our Services pursuant to the Customer’s Subscription and Services Agreement with Samaritan (or a similar agreement that governs the Customer’s subscription(s) to Samaritan’s Services), that information constitutes “Customer Data” as defined in such agreement, and the provisions of that agreement with respect to privacy and security of such data will apply. Additional information about the Company’s privacy and security practices with respect to Customer Data is available here.

10. Changes to this Privacy Statement

Samaritan reserves the right to change this Privacy Statement. Samaritan will provide notification of the material changes to this Privacy Statement through the Company’s Web sites.

11. Contacting us

Questions regarding this Privacy Statement or the information practices of the Company’s Web sites should be emailed to privacy@samaritan.com.
Appendix N: Governmental Data Request Procedures

Version 1.0
26 July 2014

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 July 2014</td>
<td>Bruce Behymer</td>
<td>Initial Draft</td>
</tr>
</tbody>
</table>

Overview

At Samaritan Technologies we offer several web-based volunteer management services and tools that interact with a database of volunteer, opportunity, organization, and logbook records. The information stored in this database belongs to our clients. Thus, as providers of these services we are stewards and caretakers of their data and have a responsibility to protect its security. This document provides our company policies and procedures for responding to governmental requests for customer data.

Audience

The intended audience for this document consists of all of Samaritan's employees, consultants, and partners. As a team we all share the responsibility of looking out for our customer’s interests.

20. Request Response Procedure

20.1. Create a record of the request

The person receiving the request should record the following information from the person making the request:

- The requestors contact information including:
  - name
  - phone number
  - email address
  - physical address
• The following information about the agency making the request:
  o Agency name
  o Requesting office physical address
  o Requesting office general phone number
  o Website

• The following information about the supervisor of the person making the request:
  o name
  o phone number
  o email address
  o physical address

• A description of the specific data which is being requested
• The time frame the delivery of the requested data
• The desired format of the requested data
• The desired delivery method of the requested data.

The person receiving the request should repeat all of the information back to the requesting party to confirm the accuracy of the information.

The person receiving the request informs the requesting party that the request will be forwarded to the Director or Vice President of Client Services for further processing.

The person receiving the request then passes the request and information collected to the Director or Vice President of Client Services.

20.2. Request Verification

The Director or Vice President of Client Services independently researches the contact phone number of the agency office making the request and then using the independently obtained contact information makes a call back to requestor’s supervisor at the requesting agency to confirm the legitimacy of the request.

20.3. Internal Notification

Once the legitimacy of the request has been confirmed then the Director or Vice President of Client Services notifies the following people of the request:

• All members of the Samaritan Security Policy Committee
• Samaritan’s Vice President of Client Services
• Samaritan’s Vice President of Operations
• Samaritan’s General Legal Counsel
• Samaritan’s Client Services Team Leader(s) for the affected customer(s)
• Samaritan’s Managing Partner
• Samaritan’s Chief Executive Officer

20.4. Customer Notification

The Director or Vice President of Client Services next reviews the subscription agreement for the customer whose data was requested for any specific instructions with regard to governmental data requests.

If specific instructions are found then the Director or Vice President of Client Services proceeds as specified by the agreement.

Section 5.5 of Samaritan’s standard Software and Services Subscription Agreement states:

*If any disclosure of confidential information is required by law, government regulation, or court order, the receiving Party may make such disclosure, but the receiving Party must first give notice thereof to the disclosing Party and cooperate with the reasonable request of the disclosing Party, at the disclosing Party’s expense, in seeking and obtaining any protective orders or other protections that might be available.*

With respect to Samaritan’s standard agreement and a governmental request for data, Samaritan is the Receiving Party (of the customer data originally) and the customer is the Disclosing Party of the Customer Data.

20.5. Customer Notification

The Director or Vice President of Client Services next reviews the subscription agreement for the customer whose data was requested for any specific instructions with regard to governmental data requests.
Appendix O: Sustainability Policy

As an organization that provides tools for efficient volunteer management and community service, concern for the environment and promoting sustainability are not only harmonious with what we do, but integral to Samaritan’s mission, professional activities and organizational management. We strive to follow and to promote good sustainability practices, to reduce the environmental impacts of all our activities, and to help our clients and vendors to do the same locally, nationally, and world-wide.

Principles

Our Sustainability Policy is based upon the following principles:

- Appreciation and concern for the world we live in, those we currently share it with, and those who will inherit it from us.
- Compliance with all relevant environmental legislation, regulations and requirements.
- Integrating sustainability considerations into all our business decisions.
- Ensuring that all staff are fully aware of our Sustainability Policy and are committed to implementing and improving it.
- Making our clients and suppliers aware of our Sustainability Policy, and encourage them to adopt sound sustainable management practices.

Practical steps

In order to put these principles into practice we:

Travel and meetings

- Walk, cycle and/or use public transport to attend meetings and site visits, apart from exceptional circumstances where the alternatives are impractical and/or cost prohibitive.
- Avoid unnecessary travel by making use of instant messaging, video and audio conferencing, telephone and email.
• Reduce the need for staff to travel by supporting alternative working arrangements, including home working, and promote the use of public transport by locating our office in an accessible location.

Purchase of equipment and consumption of resources

• Minimize our use of paper and other office consumables; for example, by double-siding all paper used, and emailing quotes and invoices, and arranging for electronic payment when possible.
• As far as possible, arrange for the reuse, recycling, sale, or donation of office wastes (including paper), computer supplies and redundant equipment that is no longer of use to the company.
• Purchase products made with recycled paper when available and comparably priced.

Working practices and advice to clients

• Undertake voluntary work with the local community and / or environmental organizations.
• Ensure that any associates that we employ take account of sustainability issues in their advice to clients.
• Encourage our staff and employees to make sustainability including waste reduction, recycling, use of renewable energy sources, and community service a part of their personal and family lives, in addition to their work.
• Encourage our subcontractors and vendors to make sustainability a priority in their organization.
• Include a copy of our Sustainability Policy in all our proposals to clients.
# Appendix P: How To Submit a Request to Samaritan

There are two methods for submitting a ticket:

1. Go to [http://samaritan.com](http://samaritan.com) and click the Support link at the top of the page.
2. Click the graphic that says, "Open a Support Ticket," and follow the instructions.
3. E-mail your request to [support@samaritan.com](mailto:support@samaritan.com). E-mails sent to support@samaritan.com will automatically create a request in the Support Center.

## WHAT TO INCLUDE IN YOUR REQUEST

In order to effectively address an issue we need the following information:

1. Operating System (OS) (e.g. Windows WP, 7, Mac OS X Snow Leopard) and Browser (Internet Explorer (IE) 10, Firefox 23.0.1) used
2. Name of eCoordinator account / eRecruiter # (if your system has more than one eCoordinator or eRecruiter)
3. Steps to reproduce
4. Screenshot / Screencast

## THINGS TO REMEMBER

- Please enter each task or question as a single item in the Support Center (Zendesk).
- When attaching a screenshot please use the following file types: .gif, .jpg, or .png and attach them directly into the support ticket (rather than in a Word document).
- If you think it's a bug, tells us what happened, how you tried it again, and it kept happening. Items that only happen once and cannot be reproduced are extremely hard to diagnose.
- Support will often ask for additional information in order to quickly process a ticket.
- Samaritan Support Team offers second tier support. Clients 'escalate' issues when they are unable to solve the problem. The preliminary research and confirmation of the issue will be done (and documented) by the person escalating the issue before sending it our way.
- If the issue involves a series of reports or conversations, say, over email, we recommend consolidating the chain of emails down to the salient points (who, what, where, when and why) is a good way to save time, rather than having the team try to parse through all that information without context.
• If you can repeat the issue and tell us how you did it, show us the history and provide a screen shot, our ability to diagnose and solve the issue will be better and results will come faster.
Appendix Q: Samaritan VPAT

Voluntary Product Accessibility Template

The purpose of the Voluntary Product Accessibility Template or VPAT, is to assist Federal contracting officials and other buyers in making preliminary assessments regarding the availability of commercial “Electronic and Information Technology” products and services with features that support accessibility.

In the subsequent table, the first column contains the lettered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

Date: 11 August 2017

Name of Product: Samaritan eCoordinator and eRecruiter

Contact for more Information: Bruce Behymer
801-328-3972
brucebehymer@samaritan.com
### Section 508 - 1194.22

**Web-based Internet information and applications – Detail**

**VPAT**

Voluntary Product Accessibility Template

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Supporting Features</th>
<th>Remarks and explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) A text equivalent for every non-text element shall be provided (e.g., via &quot;alt&quot;, &quot;longdesc&quot;, or in element content).</td>
<td>Yes, Alt- text is provided for all non-text elements.</td>
<td></td>
</tr>
<tr>
<td>(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.</td>
<td>Not Applicable, we do not have any multi-media presentations in our product. If any are included they are supplied by our clients.</td>
<td></td>
</tr>
<tr>
<td>(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.</td>
<td>Yes, that is correct. No important information is indicated via color only. In all cases Alt- text or a textual alternative is provided. Additionally, we test for sufficient contrast using the WebAIM tools.</td>
<td></td>
</tr>
<tr>
<td>(d) Documents shall be organized so they are readable without requiring an associated style sheet.</td>
<td>Yes, all documents are organized so that they are readable (although not pretty) without the use of an associated style sheet.</td>
<td></td>
</tr>
<tr>
<td>(e) Redundant text links shall be provided for each active region of a server-side image map.</td>
<td>Not Applicable – Server side image maps are not used.</td>
<td></td>
</tr>
<tr>
<td>(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.</td>
<td>Only client-side image maps are used, and only if the particular client wants to include them in their eRecruiter for searching for volunteer service opportunities.</td>
<td></td>
</tr>
<tr>
<td>(g) Row and column headers shall be identified for data tables.</td>
<td>Yes, the &lt;th&gt; tag is used identify row and column headers.</td>
<td></td>
</tr>
<tr>
<td>(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.</td>
<td>Yes. All multi-level tables have appropriate mark up to associate date and header cells. However, we do all that we can to avoid multi-level tables preferring to use more semantic divs instead if possible.</td>
<td></td>
</tr>
<tr>
<td>(i) Frames shall be titled with text that facilitates frame identification and navigation</td>
<td>Yes, when displaying user created surveys, the title attribute is used.</td>
<td></td>
</tr>
</tbody>
</table>
This is the only place where frames (an iframe) are part of the product. We try to avoid the use of frames if at all possible.

<table>
<thead>
<tr>
<th>(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.</th>
<th>Samaritan’s eCoordinator and eRecruiter pages do not have any flickering features.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.</td>
<td>Samaritan’s eRecruiter is compatible with all the requirements of this section. We include section 508 compatibility as part of our design and QA processes. Thus, no text-only equivalent page is required.</td>
</tr>
<tr>
<td>(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.</td>
<td>All interface items created via scripting languages (JavaScript) have Alt- text that can be read by assistive technology.</td>
</tr>
<tr>
<td>(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).</td>
<td>The only application that is required is Adobe Reader for reports in PDF format. We provide a link for downloading and installing Adobe Reader to fulfill this requirement.</td>
</tr>
<tr>
<td>(n) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.</td>
<td>Yes. All forms such as volunteer profiles and surveys (for creating log book entries) include navigational text that allows people using Assistive Technology to complete the form.</td>
</tr>
<tr>
<td>(o) A method shall be provided that permits users to skip repetitive navigation links.</td>
<td>Skip navigation or HTML 5 nav links are present on all pages to all users to skip past navigation links.</td>
</tr>
<tr>
<td>(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.</td>
<td>Yes. This happens only happens in the places that have automatic inactivity timers. In all cases the user is provided 30 to 90 seconds to indicate that more time is required.</td>
</tr>
</tbody>
</table>

Note to 1194.22: The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium: Paragraph (a) - 1.1, (b) - 1.4, (c) - 2.1, (d) - 6.1, (e) - 1.2, (f) - 9.1, (g) - 5.1, (h) - 5.2, (i) - 12.1, (j) - 7.1, (k) - 11.4.
Appendix R: Media Sanitization and Disposal Policy

Version 1.0

2 September 2016

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 September</td>
<td>Bruce Behymer</td>
<td>Initial draft.</td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Overview

The purpose of this policy is to protect Samaritan and Customer Data from unauthorized disclosure. This policy defines the requirements for ensuring that Samaritan Data and Customer Data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools - even data from files that were deleted long ago or a hard drive that was reformatted. Failure to properly purge data in these circumstances may result in unauthorized access to Samaritan and Customer Data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

21. Audience

The intended audience for this document consists of all of Samaritan’s employees, consultants, contractors and partners. As a team we all share the responsibility of looking out for our customer’s and Samaritan’s interests.

22. Policy

To prevent unauthorized disclosure of Samaritan and Customer Data, media leaving control of the responsible department and destined for reuse or disposal must have all Samaritan and Customer Data purged in a manner that renders the data unrecoverable.
Media that will be reused within the department should likewise have all Samaritan and Customer Data purged to prevent unauthorized disclosure.

Media containing Samaritan and Customer Data authorized by the appropriate administrative head (i.e. the Vice President of Operations [VOP]) for transfer to individuals or organizations outside Samaritan are exempt.

23. Definitions

Affiliated Organization

Any organization associated with Samaritan that uses Samaritan information technology resources to create, access, store or manage Samaritan and/or Customer Data to perform their business functions.

Confidential Data

Highly sensitive Samaritan and Customer Data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. See Samaritan’s Data Classification and Security Policy for an expanded definition and examples.

Customer Data

The following is from Samaritan’s standard software and services agreement:

“Customer Data” means the data of Customer that are transmitted by Customer or an Authorized User to Samaritan’s Computers as part of the licensed use of Licensed Software (from Samaritan).

Customer Data is both confidential and proprietary and is subject to the terms and conditions of the Agreement that Samaritan has in place with each customer. Section 5 of the standard Samaritan Technologies Software and Services Subscription Agreement describes Samaritan’s commitment to the privacy and security of Customer Data.

DeGaussing

Demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

Disintegration
A physically destructive method of sanitizing data; the act of separating into component parts.

HIPAA

Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.

Incineration

A physically destructive method of sanitizing media; the act of burning completely to ashes.

Internal Data

Samaritan Data intended for internal Samaritan business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. See Samaritan’s Data Classification and Security Policy for an expanded definition and examples.

Media

Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.

Media sanitization

The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

Public Data

Samaritan and/or Customer Data explicitly or implicitly approved for distribution to the public without restriction. See Samaritan’s Data Classification and Security Policy for an expanded definition and examples.

Pulverization

A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

Purging

A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in
a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

**Samaritan Data**

Any data related to Samaritan Technologies functions that are:

1. Stored on company information technology systems.
2. Maintained by Samaritan Technologies staff, or sub-contractors.
3. Related to company processes on or off premises. This applies to any format or media (in other words, it is not limited to electronic data).

**4. Roles and Responsibilities**

Each local department is responsible for ensuring that Samaritan Data and Customer Data are properly removed or destroyed from media before it leaves the control of the department for reuse or disposal.

**5. Implementation Procedures**

While the primary purpose of this policy is to protect non-public Samaritan and Customer Data (e.g., data classified either internal or confidential), it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient and cost effective to purge all Samaritan and Customer Data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside Samaritan, all Samaritan and Customer Data must be purged from the media before giving it to the third party.

Specific instructions for different types of media and regulations follow:

**A. Electronic Storage Media** (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, etc.)

If purging is done by overwriting the data, the entire media/device must be overwritten with a minimum of three passes.
Equipment that can store Samaritan or Customer Data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of Samaritan should have all data storage devices removed before disposition. If the equipment leaving Samaritan control must retain the data storage devices, all Samaritan and Customer Data must be properly purged.

The only acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, or incineration.

Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.

**Customer Data on USB Flash Drives:** Customer Data received for data conversions is to be stored on individually assigned numbered company issued USB flash drives. When the data conversion is complete or the drive has reached the end of its life it should be pulverized by repeatedly crushing it in a vice. Flash drives may be used for other data conversion projects if the customer data from the previous project is deleted first. The drive may be assigned to another Samaritan staff member for use on a data conversion project. However, unless the work is for the same project, the drive should be purged by overwriting before it is given to the new staff member. If a Customer Data is to be delivered via a flash drive to a customer then only a new previously unused encrypted USF flash drive should be used so that there is no possibility of mixing between more than one customer. All maintenance actions for USB flash drives such as assignment, purging, re-assignment, shipment to a customer, or crushing should be recorded in the company USB Flash Drive log. Maintenance of the USB Flash Drive Log will be under the direction of the VPO or designee.

**B. Paper-Based Media**

Any paper-based or other hard copy media containing confidential Samaritan and Customer Data must be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by Samaritan for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (1/32"x1/5"). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the company, an affiliated organization, or an individual. The maximum particle size for media containing internal data is 2x15 mm (1/16"x3/5").

Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

**C. Optical Media** (e.g., CDs and DVDs)

Optical media containing internal or confidential Samaritan and Customer Data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.
D. **Smartphones and other handheld devices**
   Mobile devices like Smartphones (e.g., Blackberry or Treo), MP3 players, and even cell phones, store information and often contain personal or other sensitive information. Any Samaritan or Customer Data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.

E. **Other Media Types**

F. **Export controls**
   Media containing Samaritan and Customer Data in equipment that will be reused outside the United States must comply with export laws and regulations.

G. **Electronic Protected Health Information**
   Samaritan units responsible for electronic protected health information covered by HIPAA must also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, *Physical Safeguards*, part (d), (1) & (2).

H. **Federal Tax Information**
   Samaritan units handling Federal Tax Information must also have media sanitization and disposal policies and procedures in accordance with [IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies](https://www.irs.gov/publications/p1075).

6. **Related Laws, Regulations, or Policies**

Samaritan Technologies Policies

   A. Samaritan Technologies Security Policies and Procedures
   B. Samaritan Technologies Disaster Prevention and Event Response Plan Summary
   C. Samaritan Technologies Software and Services Subscription Agreement
   D. Samaritan Technologies Data Encryption
   E. Samaritan Technologies Service Level Agreement
   F. Samaritan Technologies IT Security Incident Management
   G. Samaritan Technologies IT Security Incident Response Policy
Federal Legislation and Guidelines

A. Family Educational Rights and Privacy Act of 1974 (FERPA)
B. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
C. Gramm-Leach-Bliley Act (GLBA)
D. Electronic Communications Privacy Act of 1986 (ECPA)
E. HIPAA Final Security Rules, Section 164.310, Physical Safeguards, part (d), (1) & (2)
F. IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies
G. NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization
H. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
I. NIST Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories
J. Executive Order 12958: Classified National Security Information, As Amended, March 2003

Other

- Payment Card Industry Data Security Standard (PCI DSS)

7. Questions/Waivers

The Security Policy Committee Chair (SPCC) is responsible for this policy. The SPCC or Vice President of Operations (VPO) or designee must approve any exception to this policy or related procedures. Questions should be directed to the SPCC.
Appendix S: Non-Disclosure Agreement

This is a Non-Disclosure Agreement by and between Samaritan Technologies (hereinafter “Samaritan”) with its principal place of business at 265 East 100 South Suite 290 Salt Lake City, UT 84102 and ____________________________ with its principal place of business at ____________________________ (hereinafter “__________________”).

The parties desire to evaluate a business relationship. This Agreement sets forth the terms and conditions which will govern the disclosure of confidential information for the purpose of furthering that evaluation.

1. Definitions. For purposes of this Agreement, the following definitions shall apply:

1.1 The party receiving Proprietary Information will be referred to as the "Receiving Party," and the party disclosing its Proprietary Information will be referred to as the "Disclosing Party."

1.2 "Proprietary Information" means information disclosed to the Receiving Party by the Disclosing Party or its Agents either orally or in writing: (a) of a technical or conceptual nature consisting of or relating to the databases, software, systems, products, tests, assessments, services or component parts owned, developed or being developed by the Disclosing Party, including, without limitation, the information ascertained from plans, drawings, schematics, models or descriptions of processes or from an inspection of facilities or from computer programs, databases, software, computer hardware components, or other components; (b) relating to business plans, marketing plans or business opportunities of the Disclosing Party; or (c) relating to the Disclosing Party's finances, business, proposals, contracts, customers or potential customers or markets, or methods or proposed methods of doing business. Proprietary Information shall be labeled or identified to the Receiving Party as confidential, trade secret or proprietary information prior to or at the time of disclosure.

Proprietary Information does not include information which is or becomes generally known or available by publication or otherwise or is disclosed by the Disclosing Party to third parties without restriction on disclosure or is developed independently by the Receiving Party without reference to the Disclosing Party's materials or information. In addition, the Proprietary Information defined in subsections 1.2(b) and 1.2(c) above shall lose its confidential status two (2) years after the date of its disclosure to the Receiving Party.

1.3 "Agents" means a party's agents, employees and persons retained and engaged by it.

2. Protection of the Proprietary Information. The Receiving Party and its Agents shall use reasonable means to safeguard and keep confidential the Proprietary Information and to not, without the prior written consent of the Disclosing Party, disclose the Proprietary Information in any manner, in whole or in part, or use the Proprietary Information except for the purpose of evaluating the potential business relationship.

In the event that the Receiving Party or its Agents become legally compelled to disclose any of the Proprietary Information, the Receiving Party will use its best efforts to promptly notify the Disclosing Party and to provide reasonable cooperation to the Disclosing Party in connection with the Disclosing Party's efforts to lawfully avoid or limit disclosure and preserve the confidentiality of the Proprietary Information.
Information in such circumstances.

3. **Disclosure to Agents.** The Proprietary Information may only be disclosed to Agents of the Receiving Party who need to know such information for the purpose of evaluating a possible business relationship and in those instances only to the extent justifiable by that need. All Agents to whom any such disclosure has been made shall be informed of the confidential nature of the Proprietary Information and directed to use, hold and protect such Proprietary Information in accordance with the provisions of this Agreement.

4. **Return and Destruction.** The Receiving Party agrees to promptly return to the Disclosing Party, at any time upon the request of the Disclosing Party, all written materials containing or reflecting any Proprietary Information (including all copies or reproductions) and agrees to destroy all documents, memoranda, notes and other writing whatsoever (including all copies, extracts or other reproductions) prepared by the Receiving Party or its Agents based on the information contained in the Proprietary Information. If so requested by the Disclosing Party, the Receiving Party agrees to provide written confirmation to the Disclosing Party of its compliance with the terms of this Section. It is understood and agreed that the obligations of this Agreement will survive for two (2) years from the date of disclosure of the Proprietary Information.

5. **Negotiations.** Each party acknowledges and agrees that the other party reserves the right, in its full and absolute discretion to reject any or all proposals and to terminate discussions and negotiations with respect to a possible business relationship at any time.

6. **Remedies.** The parties acknowledge and agree that the unauthorized disclosure of the Disclosing Party's Proprietary Information could cause harm and significant injury to the Disclosing Party that may be difficult to ascertain. Accordingly, the Receiving Party agrees that the Disclosing Party shall have the right to seek and obtain immediate injunctive relief resulting from material breaches of this Agreement.

7. **Entire Agreement.** This Agreement is the entire agreement between the parties with respect to its subject matter and supersedes all earlier oral or written agreements. This Agreement shall be governed by and construed in accordance with the laws of the State of Utah and shall not be amended except by a written agreement between the parties. Failure of a party to enforce its rights on one occasion will not result in a waiver of those rights on any other occasion. This Agreement will be binding upon the parties and their respective successors and assigns.

IN WITNESS WHEREOF, the parties have executed this Non-Disclosure Agreement as of the date indicated below.

**SAMARITAN TECHNOLOGIES**

By: _____________________________ By: _____________________________
Authorized Signature

Name: ___________________________ Name: ___________________________

Title: ____________________________ Title: _____________________________

Date: ____________________________ Date: _____________________________
Appendix T: Change Management and Release Process

Version 1.6

29 November 2016

Contents

REVISION HISTORY.................................................................................................................................................. 115
1. OVERVIEW.......................................................................................................................................................... 115
2. AUDIENCE......................................................................................................................................................... 115
3. STANDARD SOFTWARE CHANGE MANAGEMENT AND RELEASE PROCESS............................................. 116
4. EXPEDITED SOFTWARE CHANGE AND RELEASE PROCESS................................................................. 119
5. EMERGENCY SOFTWARE CHANGE AND RELEASE PROCESS.............................................................. 121
6. STANDARD NETWORK / SERVER CONFIGURATION CHANGE PROCESS.............................................. 122
7. EXPEDITED NETWORK / SERVER CONFIGURATION CHANGE PROCESS.................................................. 124
8. EMERGENCY NETWORK / SERVER CONFIGURATION CHANGE PROCESS.............................................. 125
### Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 Jan 2014</td>
<td>Bruce Behymer</td>
<td>Reformatted old document and updated for the names of the tools we currently use.</td>
</tr>
<tr>
<td>21 July 2014</td>
<td>Bruce Behymer</td>
<td>Removed two redundant paragraphs about release night activities.</td>
</tr>
</tbody>
</table>
| 5 September 2015 | Bruce Behymer  | Added descriptions of pre-release deployment during new customer implementation and configuration.  
                     |                 | Added description of user acceptance testing for existing customers with quality assurance software/database instances.  
                     |                 | Enhanced the description of post release defect resolution.                         |
| 24 September 2015| Bruce Behymer  | Updated the document to also describe the upgrade process for non-multitenant SaaS hosting options and paid development. |
| 29 Nov 2016      | Mike Brady     | Added Expedited Software Change and Release Process                                   |
24. Overview

At Samaritan Technologies we offer several web-based volunteer management services and tools that interact with a database of volunteer, opportunity, organization, and logbook records. The information stored in this database belongs to our clients which they use on a day-to-day basis to coordinate millions of volunteers. Thus, as providers of these services we have a responsibility constantly update our software and services to facilitate this vital work they do. We also need to make sure that the process of upgrading our software with new features is as smooth as possible to minimize any disruption the upgrade process may cause. This document provides our company process for software change management and the release process for achieving this objective.

25. Audience

The intended audience for this document consists of all of Samaritan's employees, consultants, and partners. As a team we all share the responsibility of making sure we offer the best product possible within our means. This document may also be shared with existing and potential clients.

Our software change management and release processes are as follows:

Our development team maintains an on-line database called Jira that is used to record all known defects, suggestions for changes, and feature requests. Additionally, our client services team maintains a separate database (ZenDesk) used for tracking all customer service requests including feature requests and bug reports. We have established an integration between the two systems so that bugs and feature requests can flow directly from Client Services to Development. For each item these databases also tracks the status, priority, steps to reproduce, and history of each item as well who the item is currently assigned to.

Each time an item is entered into the Jira it is grouped into a functional area and assigned to a developer who makes and records a work level estimate and risk assessment for the item. With this information recorded, it is easy for our product development committee to see what related items a developer could address while working in a given area of the code and what the impact of each item will be to the overall product schedule.

For minor changes, features, and bug fixes a detailed description often including a mocked up screen shot is provide as part of the Jira entry.

If customer paid development work is to be included in a release then the sales proposal or contractual statement of work typically functions as the business requirements document. This will often include a gap analysis to determine which aspects of the customer’s needs can be met by configuration of existing functionality and which, as the result of a gap analysis, require new development. Once an agreement is signed, Samaritan’s product manager will interview the client to develop personas, and use cases that will be included in the feature requirements and ultimately a traceability matrix.

For major new features or enhancements a system requirements specification (SRS) document is created that includes background information describing the motivation for the new feature, a list of the related Jira database entries, the market requirements for the feature, and a detailed functional specification including screen shots, and a document change history. Sometimes a functional prototype using a tool such as Axure may also be created to better support an agile development methodology and better communicate a sense of the new functionality to all stakeholders.

If the new feature is being developed for a specific client then the SRS and/or prototype has been written based upon specific needs input obtained from the client often as part of a Business Requirements Document (BRD). Often the initial statement of work or sales proposal will function as the BRD. Once the SRS and/or prototype is complete it is then provided to the client for a walkthrough, review, iteration if needed, and sign-off.
From the SRS and/or prototype or Jira items the development team creates a work breakdown structure, assigns resources, and develops a project plan/schedule typically as an on-line interactive and collaborative GANTT chart (using Smartsheet). The project is then reviewed by the development team and managers who look for schedule optimizations as well as for high risk items that should be advanced in the schedule.

If a new feature is being developed for a specific client then the project plan and schedule is presented to the client for a walkthrough, review, iteration if needed, and sign-off at this point before any implementation work begins. Use of an online GANTT chart also permits the client to view the progress of the project at any time.

Once the project plan is approved by the Product Development Committee (PDC) the development team begins implementation on a set of test servers that we maintain in parallel to our production servers.

While the development team begins implementation of the project the quality assurance team begins designing the various functional, error, load, stress, vulnerability/security, accessibility, and usability tests. The test cases used to verify each feature are recorded in a tool called Test Link which allows us to track overall test completeness as we progress toward each release. We use a combination of manual and automated testing. With an extensive suite of automated regression tests that can be applied to each new build. As of this writing we currently have over 500 automated tests and over two thousand documented manual tests that are applied to each release. As soon as each functional element becomes operational the QA team begins testing on the test servers. All bugs are recorded in Jira.

Once a functional element becomes sufficiently stable, it is made available via our test servers to our customer service staff, project managers, and external beta test sites for usability testing. Results of the input from these usability testers is evaluated and as is appropriate incorporated into the feature design and the product, SRS and/or prototype are updated accordingly.

For the initial builds of the new release the quality assurance team applies their testing to assure conformance to the SRS or Jira write ups. However, this requirement is loosened as usability testing begins since new user feedback may take priority over the original design.

Our developers maintain our code under version control (using SVN, Star Team, or Git, or BitBucket) so that at any point we can roll back code changes as necessary.

Once all of the major functionality has been implemented a second data migration test database is created on the test servers in parallel with the other quality assurance test databases. This is database is specifically used to test our ability to maintain data integrity as we migrate the live production data to the new system. Production data migrated to this system is obfuscated to hide any Personally Identifiable Information (PII) or Protected Health Information (PHI).
The iterative process of bug fixing and usability enhancements continues with the product or project managers continually evaluating and prioritizing all Jira items related to the project until all critical items have been addressed.

During this debug period the development team also implements and update unit tests that are added to Samaritan’s Jenkins based Continuous Integration (CI) system. Each new build of the new release is created using the CI system which runs builds the software, runs it through a series of automated unit tests and standard PHP code cleanliness tools such as phpcpd, phpmd, and phpcs, and installs the software on a specified set of servers as well as reporting on the success or failure of each step in the operation.

When the system appears to be ready for release, if new upgraded servers have been used for the test servers then these servers will typically become the new production system. Otherwise, the new database and software will be set up in parallel on the existing production servers and go through a final system test there.

If the expected configuration / implementation completion date for a new customer using a dedicated database instance of our software is expected to be after the release date of the version of our software currently under development then we will deploy the pre-release version of our software for that new customer. Then if any defects are found in the software during the deployment for that new customer we can make sure that they are fixed during the development and quality assurance process for that new version of the software. This allows us to assure that the new version will work correctly as configured for the new customer.

Again, as bug fixes are deployed they are run through our CI system of automated unit and quality tests and any resulting issues are addressed.

For existing customers with any of the non-multitenant SaaS hosting options (dedicated database instance, dedicated virtual server, dedicated physical server, self-hosted) the deployment of a new version of our software will first take place in a quality assurance instance of the software which will undergo customer specific customization and user acceptance testing by the customer before it is deployed in the customer’s production environment.

Non-multitenant SaaS customers can work with our Client Services department to schedule their upgrades at a date and time that is convenient for them. The production environment for our multi-tenant SaaS customers is upgraded as each release becomes available typically three to four times per year.

Release announcements are sent out to our client base 1 to 2 weeks prior to the release date. These announcements typically state that the release is scheduled to happen on a Thursday night between 6 pm Pacific Time and 8 am Eastern Time the following day. During
this time our clients are advised that they can access their data and run reports, but any changes that they make may not be preserved. Similar warnings are posted on our login pages. In reality most upgrades only take a couple hours, but we allow ourselves the entire night should any problems arise.

After the release begins a final data migration is performed from the live database, final manual and automated sanity tests are performed, and then if needed the DNS records are updated to point to the proper servers, the warnings are removed, and the QA and Project managers sign off on the release.

Just in case any critical problems arise the old system is left up and running and the QA and development teams are kept on alert during the two weeks after the release should there be any urgent need to revert to the prior system.

If isolated critical changes arise that need to be implemented between major releases then the changes are first implemented and tested by our QA staff and sometimes end users on our test servers before being applied to the live production system. See “Expedited Software Change and Release Process” below.

Finally, an analysis of any bugs reported post release is performed so that the communication, design, development and QA processes can be enhanced to catch and prevent any similar problems from occurring during the next release.

When a defect is encountered in a released version of our software, it is first entered into Samaritan’s customer support incident database. Depending upon the urgency and severity of the defect members of the Samaritan’s Quality Assurance, Development, and Client Services team will either meet immediately to discussing the issue and plan its resolution, or they will discuss the issue in the next weekly quality assurance meeting. (See the expedited and emergency software change and release processes below.) Once a resolution plan has been put into place the fix is first implemented in a test environment. Once correct operation has been verified in the test environment then the fix is be applied to the production environment and re-verified there after sufficient notice to or coordination with the client has taken place.

All such changes are submitted to version control and associated with the appropriate version label as well as being applied to the next version under development.
27. Expedited Software Change and Release Process

When a customer requests a small change and requests to be expedited between releases, the following process describes how that change is implemented.

27.1. Account manager, client services, or product manager composes feature request as a Jira ticket, including a required user story and business need.

27.2. Product manager schedules business need for review in Product Development Committee meeting.

27.2.1. If the PDC agrees that the business reasons and benefits provided by the potential feature are not great enough to offset the opportunity, labor, and other costs, the feature request will be archived, and may be included in the regular release process moving forward, and the expedited software process concludes.

27.2.2. If the PDC agrees that the feature request fulfills a valid business need and will hold mutual benefit for the client and the company, the expedited software process continues.

27.3. Feature request is approved by product manager.

27.4. Product manager forms design committee with relevant stakeholders, potentially including product manager, account manager, development team, client, and/or other support staff.

27.5. Design committee designs new feature based on user story and business need.

27.6. Security committee reviews and approves new feature design against security requirements and policies.

27.7. Product manager approves new feature design.

27.8. Feature request is assigned to development team lead.

27.9. Developers compose and apply new code to customer-specific QA or other test instance.

27.10. Upon code completion, QA team lead assigns to QA team members for testing.

27.11. Testers and coders engage in the standard iterative testing and bug fixing process.

27.12. Product manager, client/end-user, and/or account manager perform acceptance testing.

27.12.1. Client, coders, and testers engage in iterative acceptance process. Jira and/or Smartsheet will be used to document client feedback.
27.12.2. Client and/or product manager acceptance will be documented in appropriate Jira tickets.

27.13. Account manager schedules production instance upgrade.

27.14. Upgrade notices with expiration dates posted to login pages by account manager no later than 10 days prior to scheduled production upgrade.

27.15. Development team creates back up of production instance in case problems are encountered during or after the upgrade.

27.16. Development pushes new feature to appropriate production instance, and registers new build number.

27.17. Account manager informs client regarding upgrade status.

27.18. Product manager updates appropriate Jira tickets with tags and labels (e.g., version, component, client name) for future reference.

27.19. All expedited development is discussed each week in weekly client services / product manager meeting.
28. **Emergency Software Change and Release Process**

28.1. Issue is received by the Development Team Lead (DTL).

28.2. Issue requiring change is received by customer support, or client services or some other department.

28.3. The person receiving the reported issue verifies the issue.

28.4. The person receiving the issue reports it to the Vice President of the Client Services or in his/her absence to the Director of Development who becomes the Issue Lead (IL).

28.5. The issue lead forms an Issue Resolution Committee (IRC) with the Development Team Leader or the most senior developer available at the time.

28.6. The IRC evaluates the issue and decide whether the issue requires immediate action, possible actions to resolve the issue, the risks associated with each action, and on which client instances the actions should be taken. The results of these decisions become the Issue Action Plan (IAP).

28.7. If the issue requires immediate action then the IRC instructs the Development Team Leader or most senior developer to be the Corrective Action Implementer (CAI) and to implement the necessary action on the client instances selected in the previous step.

28.8. The IL reports the IAP to Samaritan’s Support department.

28.9. Samaritan’s customer support team reports the IAP to the client the planned corrective action and that it is in progress.

28.10. The Development Team Leader or most senior developer available implements the change on the selected client instances.

28.11. The AI verifies the corrective action.

28.12. The IL verifies the corrective action.

28.13. The Reporter verifies the corrective action.

28.14. Samaritan’s customer support department reports that the corrective action to the client and requests that the client verify the corrective action.

28.15. The client verifies the corrective action.

28.16. The AI will create a Jira ticket describing the corrective action.

28.17. The AI assigns the Jira ticket to the Quality Assurance Team Lead for verification and regression testing.
28.18. The AI sends an email to the Samaritan development email group reporting the issue, the corrective action taken, the client instances affected, and the Jira ticket number.

28.19. The Quality Assurance Team verifies the corrective action and performs regression testing of the product areas affected by the corrective action.

28.20. The Quality Assurance team updates the Jira ticket with a subsequent related issues that they find or closes the ticket.

28.21. The Quality Assurance Team Leader having received the email sent by the AI schedules the issue for discussion in the weekly Quality Assurance Status meeting.

28.22. In their next weekly meeting the Quality Assurance Status Meeting members discuss the issue and determine if the corrective action or another long term fix should be implemented and to which customer instances release versions of the software the fix should be applied and assigns a member of the group to create and assign Jira tickets for following up on their decisions until the issues are closed.

28.23. The development team implements the follow up Jira tickets assigned to them then assigns each Jira ticket to the Quality Assurance Team for verification and closure.

28.24. The Quality Assurance Team verifies the tickets and iterates the issues with the development team until such time that the Jira tickets can be closed.

28.25. The Quality Assurance Team closes the Jira tickets.

28.26. The members of the Quality Assurance Team perform a post issue analysis to determine the cause of the issue and assign actions to be taken to prevent the issue or similar issues from occurring in the future.
29. **Standard Network / Server Configuration Change Process**

29.1. Based upon an emerging business need (security, continuity, marketing, and etc.), a contractual obligation, or an approaching capacity limitation, a member of the Product Development Committee (PDC) or Client Services Team (CST) recognizes the need for a Hardware/System Configuration Change Request (H/SCCR).

29.2. The PDC includes representatives from the Design, Development, Quality Assurance, and Client Services teams.

29.3. If the member of the PDC or CST will meet with the Vice President of Client Services (VPCS) and the Development Team Lead (DTL) to determine if the change request is minor and low risk should be handled via the Expedited Network / Server Configuration Change Process or continue with the Standard Process. If the Expedited Process is selected then the change request proceeds through that process otherwise the change request proceeds as follows.

29.4. The PDC or CST member will submit a request to the Product Manager to add the H/SCCR to the weekly PDC meeting agenda.

29.5. The PDC reviews the H/SCCR to confirm the business need, examine alternatives, approve or disapprove the H/SCCR and if approved schedule its implementation.

29.6. If the H/SCCR is approved by the PDC then it is assigned to the Development Team Lead (DTL) who creates a Jira ticket for it.

29.7. The DTL meets with the Vice President of Client Services and Development Director (DD) to determine the best approach for implementing the H/SCCR and to develop and Action Plan (AP).

29.8. The DTL updates the Jira ticket with the action plan.

29.9. If the action plan requires scheduled down time then the DTL posts scheduled down time notices on the login pages for the instances of Samaritans systems that will be affected by the H/SCCR.

29.10. The DTL submits a ticket for the H/SCCR to the ticketing system of the hosting service either Rackspace or RapidScale. The hosting service ticket includes the details of the action plan and schedule for implementation.

29.11. If the H/SCCR is for a major system change such as a server upgrade then the new system will be built and brought up in parallel with the existing production system.

29.12. Once the H/SCCR has been implemented the hosting service representative updates the ticket in the hosting service ticketing system and assigns the ticket back to the DTL.

29.13. The DTL verifies the changes made by the hosting service.
29.14. The DTL assigns Jira Ticket installs and verifies the operation of any additional software that may be required by the H/SCCR.

29.15. The DTL assigns the internal Samaritan Jira ticket to the Quality Assurance (QA) team.

29.16. The QA team verifies the operation of the system according to the action plan and iterates with the DTL who may iterate with the hosting service as necessary.

29.17. Once the QA team verifies the operation of the system they state such in the Jira ticket and assign the ticket back to the DTL.

29.18. If the H/SCCR specifies a new server or backup and recovery system, then the DTL coordinates a backup and disaster recovery fire drill of the new system and iterates until the fire drill is successful.

29.19. The DTL coordinates with the VPCS to schedule the transfer of the production instances of Samaritan’s Volunteer Management System (VMS) to the new system and makes sure that the transfer process is detailed in the action plan and that staff members are aware of their roles in the plan and the schedule.

29.20. The VPCS confirms that the scheduled downtime notices have been in place for sufficient time.

29.21. The DTL Coordinates the transfer as detailed in the action plan.

29.22. The transfer typically will involve verification of the new production system, software, and data by the Quality assurance team in which case the DTL will assign the Jira ticket to them.

29.23. The QA team verifies the operation of the new system and software iterating with the development team as needed.

29.24. Once the QA team has verified correct operation, they update the Jira ticket and assign it back to the DTL.

29.25. The DTL removes the downtime notices and closes the ticket.

29.26. The old production system is left up and running for two weeks should there be a need to quickly revert back to the old system.

29.27. The Product Manager schedules a review of the H/SCCR for the following PDC meeting.

29.28. At the following PDC meeting the members review the upgrade and determine there are any process changes or improvements that need to be made to the action plans for future H/SCCRs.
30. Expedited Network / Server Configuration Change Process

30.1. The VPCS receives, reviews and approves or disapproves the change request. Approved change requests proceed as follows:

30.2. The VPCS approves the change request in the Jira Ticket.

30.3. The DTL creates a Change Request Ticket (CRT) in the hosting service ticketing system for either Rackspace or Rapid Scale.

30.4. The hosting service assigns a technician to implement the CRT.

30.5. The technician implements the CRT.

30.6. The technician updates the CRT with the implementation status once the change request has been implemented and assigns the CRT back to the DTL.

30.7. The DTL verifies the change and iterates via the CRT with the hosting service until the DTL is able to confirm successful verification.

30.8. The DTL updates the Jira Ticket to record the verified implementation.

30.9. The DTL will reassign the Jira Ticket to the person (requestor) who made the change request.

30.10. The requestor verifies the change and closes the ticket.
31. Emergency Network / Server Configuration Change Process

31.1. The DTL or a member of the Client Services or Development teams receives notice of an issue from an automated monitoring system or a client.

31.2. The person receiving the report issue verifies the issue.

31.3. The person receiving the report sends out an email notice of the issue to the DTL, Director of Development (DD), VPCS, and QA teams.

31.4. The person receiving the issue reports it to the Vice President of the Client Services or in his/her absence to the Director of Development who becomes the Issue Lead (IL).

31.5. The IL assigns the VPCS or a member of the CS team to notify any affected clients that Samaritan is aware of the problem and has started work on it.

31.6. The IL opens a ticket on the hosting service’s ticketing system.

31.7. The IL forms an Issue Resolution Committee (IRC) with the DTL or the most senior developer available at the time and a Hosting Service Representative (HSR).

31.8. The IRC evaluates the issue and decide whether the issue requires immediate action, possible actions to resolve the issue, the risks associated with each action, and on which client instances the actions should be taken. The results of these decisions become the Issue Action Plan (IAP) which may include things up to disaster recovery, failover, and system replacement. See the Summary of Samaritan’s Disaster Prevention and Event Response Plan document.

31.9. The IL opens a Jira ticket to record the IAP.

31.10. The HSR updates the hosting system ticket with the IAP.

31.11. If the issue requires immediate action then the IRC instructs the Development Team Leader or most senior developer to be the Corrective Action Implementer (CAI) to coordinate with the HSR and to implement the necessary action on the client instances selected in the previous step.

31.12. The IL reports the IAP along with an estimated time of restored system availability to Samaritan’s Support department.

31.13. Samaritan’s customer support team reports the IAP to the affected clients and that it is in progress.

31.14. The CAI and HSR implement the IAP.

31.15. The CAI verifies results of the IAP and iterates as needed with the HSR.
31.16. Once the CAI has verified restored operation the CAI informs the IL that the system is available again.

31.17. The CAI updates the Jira Ticket.

31.18. The HSR updates the hosting service ticket.

31.19. The IL verifies the corrective action and updates the Jira ticket.

31.20. The IL assigns the Jira Ticket to the QA team who verifies correct operation of the restored system.

31.21. The QA team performs a sanity test on the system to verify the restored operation and iterates with the CAI and HSR if necessary.

31.22. The QA team updates the Jira ticket once the sanity test is successful and assigns the Jira ticket to the IL.

31.23. The IL assigns Samaritan’s customer support department to contact the affected client(s) and inform them of the restored system operation.

31.24. The IL assigns the Jira ticket to Samaritan’s QA Team Leader.

31.25. The IL sends an email to the Samaritan development email group reporting the issue, the corrective action taken, the client instances affected, and the Jira ticket number.

31.26. The Quality Assurance Team Leader having received the email sent by the IL schedules the issue for discussion the in the weekly Quality Assurance Status meeting.

31.27. At the following QA Status meeting the members review the upgrade and determine there are any process changes or improvements that need to be made to prevent reoccurrences of the issue and assign action items to that end.

31.28. The development team implements the follow up Jira tickets assigned to them then assigns each Jira ticket to the Quality Assurance Team for verification and closure.

31.29. The QA Team verifies the tickets and iterates the issues with the development team until such time that the Jira tickets can be closed.

31.30. The Quality Assurance Team closes the subsequent Jira tickets.

31.31. The QA team closes the original ticket.
Appendix U: Software and Services Subscription Agreement

Samaritan Technologies
265 East 100 South, #290
Salt Lake City, UT 84111

Date: 

Agreement No.: 20180808-10XX

CUSTOMER:

<table>
<thead>
<tr>
<th>Name:</th>
<th>Legal Contact:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td></td>
</tr>
<tr>
<td>Email:</td>
<td>Phone:</td>
</tr>
</tbody>
</table>

Samaritan Software, LLC doing business as Samaritan Technologies is referred to herein as “Samaritan” and is engaged in the business of providing online software and database solutions to its licensees. ________________, referred to herein as “Customer” has requested Samaritan to provide an online software and database solution (consisting of Licensed Software and Services) as described in this Agreement. Accordingly, the Parties agree to the following Terms and Conditions.

Terms and Conditions

Section 1 – Use of Licensed Software

1.1 Licensed Software. The “Licensed Software” will mean the computer program(s) listed in Appendix A under the Licensed Software heading.

1.2 License and Authorized Users. Subject to the terms and conditions of this Agreement and Customer’s compliance therewith, Samaritan grants to Customer a non-exclusive non-transferrable limited term license for Customer’s Authorized Users to access and use the Licensed Software (the “License”). The Licensed Software will be resident on Samaritan Servers (defined below). The Authorized Users will access and use the Licensed Software from Customer’s Computers (defined below) via the Internet through compatible web browsing software resident on Customer’s Computers. Except for the transmission and storage of Customer Data (as described in Section 5.1), Customer and its Authorized
Users may not transmit, upload or store any data, computer programs, or other subject matter to or on Samaritan Servers. Customer may access and use the Licensed Software only in the ordinary course of Customer’s business operations and only by and through Authorized Users. “Authorized Users” are defined in Appendix D under the Authorized Users heading. Authorized Users must be authorized by Customer and must be obligated by Customer to comply with and respect the provisions of this Agreement that relate to Authorized Users or the protection of Samaritan’s intellectual property, Licensed Software, Client Software and confidential information. The License and Customer’s rights may be further limited as described in Appendix D, including Term, Number of Users, and any other limits described in Appendix D. If any of the limits in Appendix D are exceeded, Customer must pay Samaritan at Samaritan’s then-current rates and fees for the excess. Customer and its Authorized Users may access and use the Licensed Software System only in accordance with the Documentation. Exceptions, if any, to this Section 1.2 are set forth in Appendix E.

1.3 Samaritan Servers. “Samaritan Servers” means the server(s) and any other computer(s), storage media, hardware and system(s) selected or designated by Samaritan for the storage and execution of the Licensed Software for the purpose of allowing Customer’s Authorized Users access to and use of such Licensed Software under the License of Section 1.2. The Licensed Software will be served or made available from or by the Samaritan Servers to Customer’s Computers via the Internet (see Section 1.4). Samaritan Servers are not dedicated exclusively to the Licensed Software or Customer unless specifically stated otherwise in Appendix D under the Assumptions heading. Samaritan Servers may be located at Samaritan’s or its contractor’s site(s).

1.4 Customer’s Computers. “Customer’s Computers” means computers functioning as Internet clients or workstations that are in the possession and control of Customer’s Authorized Users and used by Customer’s Authorized Users to access and use Licensed Software as described in this Agreement.

1.5 Responsibilities of Samaritan. Samaritan is responsible for the procurement and maintenance and server-side Internet access of the Samaritan Servers and the Licensed Software. Samaritan is also responsible for any operating system and other third party software needed to run the Licensed Software on the Samaritan Servers. Samaritan or its contractor, not Customer, owns and holds the licenses to such third party software. Samaritan (directly or through its contractor) will contract with the applicable third party software licensors for software maintenance and updates and new versions as Samaritan deems appropriate. Samaritan will determine which updates and new versions of the third party software are installed on the Samaritan Servers.

1.6 Responsibilities of Customer. Customer, at its expense, is responsible for procuring, installing, implementing, and maintaining Customer’s Computers (including system software), compatible web browsing software, Internet access, data feeds, telecommunications, networks, peripherals and any other items and services needed by Customer’s Computers and Authorized Users to access (via the Internet) the Licensed Software running on Samaritan Servers, and Customer Data resident on the Samaritan Servers. Customer will follow Samaritan’s then-current reasonable specifications and
guidelines with respect to the foregoing. The initial specifications include, but are not necessarily limited to, the “Specified Configuration” identified in Appendix A. Updates to the foregoing may be required from time to time as described in update notices from Samaritan. Customer is responsible for procuring, installing and implementing such updates. Customer is responsible for items listed in Appendix A as “Customer Deliverables and as listed in the Service Proposal under “Customer’s Responsibility and Deliverables”. In the event a conflict between Appendix A and the accepted Service Proposal, items listed in Appendix A take precedence.

1.7 **Licensed Software Updates and New Versions.** The License includes any maintenance fixes, patches, and updates to and new versions of Licensed Software that Samaritan elects to install on the Samaritan Servers and include in the License of Section 1.2. All such maintenance fixes, patches, updates, and new versions will become part of the Licensed Software. Customer’s rights and License will only apply to the then-most-current version of the Licensed Software installed on, and available to Customer’s Authorized Users from, the Samaritan Servers. Customer shall coordinate with Samaritan to see that the version of the Licensed Software in use by Customer’s Authorized Users is no more than one year older than the version of the Licensed Software most recently released by Samaritan for production usage. Customer acknowledges that usage of older versions of the Licensed Software may incur increased support costs as outdated versions of the Licensed Software may require extra work to address issues that have already been addressed in more recent versions. Prior or outdated versions of the Licensed Software (and any maintenance fixes, patches, workarounds, and updates to such prior or outdated versions) may be discontinued by Samaritan. Notwithstanding anything herein to the contrary, Samaritan has no obligation to include in the License or make available for access and use by Customer, any future features or functionality of the Licensed Software that represent a substantially new capability or utility of the Licensed Software in the reasonable discretion of Samaritan. Samaritan may condition the inclusion and availability of such features and functionality on the payment of additional fees and/or on other conditions and terms. If Customer agrees to pay such additional fees and agrees to such other conditions and terms, if any, then that future feature or functionality of the Licensed Software will be included in the License of Section 1.2 and will be Licensed Software under and subject to this Agreement. Exceptions, if any, to this Section 1.7 are set forth in Appendix E.

1.8 **No Rights to Code.** Customer and Authorized Users are not entitled to receive any copy of any of the Licensed Software in any form (source code, object code, executable code, or other form). The License is strictly limited to remote access via the Internet as described above. In the event that Customer or any Authorized User does receive any of the Licensed Software, Customer and Authorized Users will not decompile, disassemble or reverse engineer any of the Licensed Software, or distribute or publish any copy of any of it, or modify it or create any derivative work based on it, or in any way facilitate any of the foregoing. Nothing in this Section 1.8 prohibits Customer’s Authorized Users from receiving or displaying on Customer’s Computers any web pages “served up” by the licensed use of the Licensed Software.
1.9 **Documentation.** To the extent that any documentation or materials (in any form, online, electronic, printed or otherwise) relating to the Licensed Software or Services are made available by Samaritan to Customer or any Authorized User, they are referred to herein as “Documentation” and Customer and its Authorized Users will use such Documentation only to facilitate the licensed use of the Licensed Software (and Client Software, if any) under this Agreement and Customer and Authorized Users will not disclose any of the contents of such Documentation to any third party and will not distribute any copy of any of such Documentation to any third party unless and to the extent only that Samaritan gives specific written permission. Samaritan is the owner of the copyrights to such Documentation.

1.10 **Client Software.** If and to the extent that Samaritan provides to Customer any Client Software, then Customer is licensed to have its Authorized Users use such Client Software on Customer’s Computers only for the purpose of enabling or facilitating the licensed access to, and use of, the Licensed Software in accordance with this Agreement, and for no other purpose (the “Client Software License”). “Client Software” is any client software, applet, or program provided by Samaritan to Customer for use on Customer’s Computers for the purpose of enabling or facilitating access to and use of the Licensed Software. Client Software is not Licensed Software. Customer is not entitled to any source code for the Client Software. Customer must not decompile or otherwise reverse engineer the Client Software. Customer must not disclose or distribute any of the Client Software to any third party. The Client Software License will terminate upon any termination of the License of Section 1.2. Upon termination of the Client Software License, Customer must erase or destroy all copies of the Client Software within the possession or control of Customer. Client Software does not include any client software, applet, or program licensed or provided by Samaritan to Customer under a different agreement (e.g., a separate license agreement) or any third party software or products distributed or provided by Samaritan to Customer.

1.11 **Passwords and Access.** User IDs (e.g., logins), passwords and access to the Licensed Software and Customer Data residing on Samaritan Servers will be administered and governed by Samaritan’s then-current reasonable guidelines and procedures. Customer is responsible for any and all activities that occur under its accounts(s) and for the confidentiality of all User IDs and passwords of Authorized Users and for the confidentiality of any other security-related information disclosed to Customer. Customer must safeguard such User IDs, passwords, and security-related information. Customer must notify Samaritan of any known unauthorized use of Customer’s account(s) and any other breach of security relevant to this Agreement or Samaritan.

1.12 **Security.** Customer is responsible for maintaining adequate technical and procedural access controls and system security requirements and devices to ensure that there is no unauthorized or improper access or use of Customer Computers, Client Software, Licensed Software or Samaritan Servers or violation of data privacy or confidentiality from, by or through any equipment, computers, networks, communication links or devices, offices, facilities, employees, agents, representatives, contractors, volunteers, clients, customers, affiliates or Authorized Users of Customer. Samaritan is not responsible or liable for any unauthorized or improper access to or use of the Client Software, Licensed Software, Customer Computers, or any Customer Data where such access or use originates outside of Samaritan.
Servers or from, by or through any equipment, computers, networks, communication links or devices, offices, facilities, employees, agents, representatives, contractors, clients, customers, affiliates or Authorized Users of Customer. Customer will also be responsible for implementing and maintaining virus detection, quarantine, and eradication capabilities and other similar protections for its computers and systems. These capabilities and protections are not provided by Samaritan to Customer.

1.13 **Personal Information.** Customer and its Authorized Users must not disclose any personally identifiable information (PII), protected health information (PHI), payment card information (PCI) or any other personal information in violation of any law, regulation or government order or the rights of any person. Customer will indemnify Samaritan and its officers, managers, employees, contractors and representatives against, and hold them harmless from, any such violation and any claims of such violation, and any judgments, settlements, damages, awards, expenses, costs, losses, and attorneys’ fees.

1.14 **Intellectual Property.** The Licensed Software, Client Software, and Documentation and the copyrights and intellectual property in and to the Licensed Software, Client Software, Documentation and Services are the property of Samaritan (and its licensors, if any, to the extent that the Licensed Software, Client Software, Documentation and Services include any computer programs or intellectual property licensed by such licensors to Samaritan for inclusion in or with the Licensed Software, Client Software, Documentation or Services). Samaritan does not assign or convey ownership of any copyright or other intellectual property to Customer.

**Section 2 – Services**

2.1 **Data Storage Services.** As part of the Services, the Customer Data will be stored on Samaritan Servers and available to Customer in connection with its licensed use of the Licensed Software and in accordance with this Agreement (the “Data Storage Services”) - see Section 5.1. See also “Temporary Customer Data Storage Services” under Section 6.4.

2.2 **Services - Configuration, Training, Support, etc.** “Services” will mean the Data Storage Services and any configuration services, training, support, maintenance, and other services described in this Agreement and the Statement of Services which is attached as part of Appendix A to this Agreement. Samaritan will perform the Services for Customer. If the Statement of Services includes any time schedule or times for performance or completion of performance of Services, such time schedule and times are estimates and Samaritan will use commercially reasonable efforts to meet such time schedule and times, but they are not guaranteed by Samaritan.

2.3 **Additional Services.** If Customer desires additional services or changes to the Statement of Services, the Parties may supplement or amend the Statement of Services of Appendix A or add additional Statements of Services to Appendix A, but any such supplement, amendment or additional Statement of Services must be agreed to by both Parties in writing. The additional services and changes
to Services described in such supplements, amendments and additional Statements of Services will be governed by this Agreement as “Services.” The Fees and Payment Schedule of Appendix B will be supplemented or amended or additional Fees and Payment Schedules will be added to this Agreement to specify the fees and charges which must be paid by Customer for the additional or changed Services. If no fees or charges are specified for the additional or changed Services, and if Samaritan provides or agrees to provide such additional or changed Services, then Customer must pay to Samaritan the then-current standard fees charged by Samaritan for such additional or changed Services, unless Samaritan has waived in writing the fees or charges for the additional or changed Services. See also Section 4.6.

2.4 Cooperation. Customer will make promptly available to Samaritan such information, assistance and cooperation as Samaritan may reasonably request in providing Services to Customer under this Agreement.

2.5 Licensed Global Publishing Content. Customer and its Authorized Users may submit “Licensed Global Publishing Content” to Samaritan in accordance with Appendix F.

Section 3 - Support and Maintenance

3.1 Telephone Support. Telephone Support shall mean support delivered via telephone or other methods as defined in this Section 3.1. Customer shall be entitled to Telephone Support from Samaritan's customer support personnel. Telephone Support is subject to the reasonable availability of Samaritan's customer support personnel during the times and on the days specified in Appendix A. Telephone Support is subject to Samaritan's then-current Telephone Support policies, limitations and procedures. The Support Fee entitles Customer to not more than the Maximum Number of Support Hours of Telephone Support as set forth in Appendix A. Telephone Support beyond this limit is governed by Section 2.3 of this Agreement as Additional Services. All communications between Customer and Samaritan relating to support issues must be with Customer’s support contact person(s) listed in Appendix C and such contact person(s) must have received training from Samaritan and must be familiar with any user documentation or other instructions/information provided by Samaritan to Customer. Samaritan has no obligation to communicate with any other Customer personnel or Authorized Users on support issues or on Errors under Section 3.2. Telephone Support (including hours) may also be provided via emails, Internet chat, and faxes or other electronic means rather than telephone, and the foregoing will apply to such emails, Internet chat, and faxes or other electronic means as part of such support unless specified otherwise in Appendix A.

3.2 Maintenance and Errors. Samaritan is responsible for the maintenance of the Licensed Software and Samaritan Servers as provided in Section 1.5. Samaritan shall use commercially reasonable efforts to diagnose Errors reported by Customer and to troubleshoot such Errors and to provide maintenance fixes, work-around solutions, or other solutions to such Errors. The term “Errors” as used herein means programming errors in the Licensed Software that materially and adversely causes the Licensed Software to fail to operate or perform in accordance with its then-current Documentation. These Errors do not include any problem or error associated with Customer’s responsibilities under Section 1.6,
Section 1.12 or a Force Majeure. If a problem or error reported by Customer is not an Error as described above, then Customer will pay Samaritan on a time plus expenses basis under Section 2.3 for services, diagnosis, troubleshooting, and workarounds related to such problem or error. Customer will report Errors to Samaritan in accordance with Samaritan’s then-current reasonable Error reporting procedure and shall provide to Samaritan reasonably detailed documentation and written explanation, together with underlying data, to substantiate any Error and to assist Samaritan in its efforts to diagnose, reproduce and correct the Error. Samaritan reserves the right to prioritize Errors, including Errors reported by Samaritan’s other customers or licensees, and the timing of efforts under this Section, with the understanding that Samaritan must be reasonably diligent.

Section 4 - Payments, Assumptions, and Change Orders

4.1 Fees. Customer will pay to Samaritan the fees and other charges set forth in the Fees and Payment Schedule attached hereto as Appendix B. Payment of the Subscription fee only entitles Customer to the License of Section 1 for the specified Term. The other fees and charges in Appendix B are payment for the Services specified in the Statement of Services of Appendix A, but not any Additional Services. Additional fees and charges may be required as provided in Sections 1.7 and 2.3. All payments to Samaritan under this Agreement will be in United States of America dollars. For each Renewal Period, the fees are subject to increase by Samaritan.

4.2 Users. The License and Customer’s rights are limited to and the fees are based on the Number of Users specified in Appendix D.

4.3 Expenses. In addition to these fees, Customer will reimburse Samaritan for costs and expenses (including any travel, lodging and meals) reasonably incurred by Samaritan in connection with any Services provided at a Customer location or any other location other than a facility of Samaritan or the location of Samaritan Servers.

4.4 Taxes. The fees and other amounts payable by Customer to Samaritan under this Agreement do not include any taxes of any jurisdiction that may be assessed or imposed upon the Licensed Software, Client Software or Documentation accessible by or delivered to Customer, or any license or right granted under this Agreement, or the Services provided under this Agreement, or otherwise assessed or imposed in connection with the transactions or matters contemplated by this Agreement, including any sales, use, excise, value added, personal property, export, import and withholding taxes, and excluding only federal and state taxes based upon Samaritan’s net income. Customer shall directly pay any such taxes assessed against it, and Customer shall promptly reimburse or pay Samaritan for any such taxes payable or collectable by Samaritan. If any taxes are withheld from any payments to Samaritan under this Agreement, Customer must pay such taxes and ensure that Samaritan receives the full amount of all payments as stated in this Agreement.
4.5 **Late Payment, Suspension and Termination.** Any amount not paid by Customer to Samaritan in full in a timely manner will accrue interest at the rate of 1.5% per month or the highest rate allowed by applicable law, whichever is less, and such interest will be promptly paid by Customer to Samaritan in addition to all other amounts payable under this Agreement. If Customer fails to pay to Samaritan, within ten (10) days after Samaritan makes written demand there for, any past-due amount payable under this Agreement (including interest thereon), in addition to all other rights and remedies which Samaritan may have at law or in equity, Samaritan may, in its sole discretion and without further notice to Customer, suspend performance of any or all of Samaritan’s obligations and Customer’s rights under this Agreement (including, without limitation, the License and support) until all past due amounts are paid in full and Samaritan shall have no liability, during the suspension of such services, with respect to Customer’s inability to access or use the Licensed Software or Customer Data. If the failure to pay lasts for more than 30 days after such demand, Samaritan may terminate this Agreement in accordance with Section 6.2.

4.6 **Assumptions.** It is understood that this Agreement and the License and Services are based on the “Assumptions,” if any, stated in Appendix A. If actual loads, traffic, demands or other circumstances are not within such Assumptions, then additional fees or charges may be required by Samaritan.

4.7 **Amendments.** If the Parties desire to amend this Agreement, including any Appendix, they may do so, but only by a written amendment signed by both Parties.

4.8 **Acceptance.** During the Initial Term after Samaritan completes the initial implementation services specified in Appendix A Samaritan will give notice to Customer requesting that Customer determine whether the implementation is acceptable. Customer will have ten (10) business days (the “Initial Review Period”) to give notice to Samaritan either accepting the implementation or stating the reasons why the implementation is unacceptable. If Customer does not provide notice of acceptability or unacceptability within the Initial Review Period then the implementation will be considered accepted by Customer, and all related fees are due for payment (as defined in Appendix B). Upon Customer’s use of eRecruiter on a publicly accessible website interface or Customer’s intranet in order to recruit volunteers from members of the public not employed by or affiliated with Customer or Customer employees or the addition of more than thirty (30) volunteer records to the Customer Data stored on the Samaritan Servers beyond any initial data conversion the implementation services will be considered accepted by Customer, and all related fees are due for payment (as defined in Appendix B). If the implementation services are not acceptable, then Samaritan will promptly revise/re-perform the implementation services, at no additional charge to Customer, and then request that Customer determine whether the revised/re-performed implementation is acceptable. Notwithstanding the foregoing, changes, omissions, or additions to Customer’s written specifications will not be considered reasons for unacceptability. Customer will have five (5) business days (the “Revision Review Period”) to give written notice to Samaritan either accepting the revised/re-performed implementation or stating the reason the revised/re-performed implementation is unacceptable. If Customer does not provide notice of acceptability or unacceptability within the Revision Review Period then the implementation will be considered accepted by Customer, and all related fees are due for payment (as defined in Appendix B). If the revised/re-performed implementation is unacceptable, then Customer may, at its option, either: (a)
extend the time for Samaritan to correct the unacceptable implementation and continue acceptance testing in accordance with the procedure set forth above; or (b) give notice to terminate this agreement to Samaritan

Section 5 - Customer Data and Confidentiality

5.1 Customer Data. “Customer Data” means the data of Customer that are transmitted by Customer or an Authorized User to Samaritan’s Computers as part of the licensed use of Licensed Software. Transmitting of Customer Data must be in accordance with Samaritan’s then-current reasonable specifications and guidelines. Such Customer Data will be kept confidential by Samaritan (and its contractors, if any), subject to Section 5.2 below. Customer warrants that Customer Data and the transmitting and storage of such data will not infringe, misappropriate or violate the rights or intellectual property of any third party. Customer is responsible for the accuracy, integrity, completeness and content of Customer Data.

5.2 Privacy.

(a) Individual and Organization Information: Except as described below (Shared or Published Information) or as required by law, regulation or order of a court or government entity, Samaritan will not disclose, reveal, share, or sell any PII, PHI, or PCI in Customer Data about any individual including name, address, telephone number, or email address, nor will Samaritan disclose any statistical information in Customer Data that identifies any specific individual volunteer or organization without that volunteer’s or organization’s prior written approval.

(b) Shared or Published Information: Samaritan’s eCoordinator™ and eRecruiter™ software and services are specifically designed for the purpose of easily sharing volunteerism information. Once Customer chooses to share, disclose, or publish such information, including, but not restricted to, information about individual volunteers, clients (recipients of volunteer service), service opportunities, or organizations by using Samaritan’s software, Samaritan is not responsible for the use, disclosure or publication of the information by or to its recipients. Customer also acknowledges that once such information has been shared, disclosed or published it cannot be retrieved even if Customer should later desire to do so.

(c) Use of Customer Data for Statistical Purposes: Samaritan may extract data (including Customer Data) stored on Samaritan Servers and compile or create general bulk statistical information about volunteerism and other subjects, and may publish, copy, use, distribute, license and/or sell such general bulk statistical information and authorize others to do so. Such general bulk statistical information must not include PII, PHI, or PCI.

5.3 Confidential Information of Customer. Samaritan (and its contractors, if any) will keep confidential, and will not use except in the performance of Services, any other information (i.e., information other than Customer Data) disclosed by Customer to Samaritan in connection with the
Services, provided that such other information when given to Samaritan is marked or identified in writing as “Confidential” or “Proprietary.” If Customer discloses such other information orally to Samaritan, and if Customer desires to have such other information protected under this Section 5.2, then Customer must reduce such other information to writing, mark it as “Confidential” or “Proprietary” and deliver such writing to Samaritan within two weeks of the first oral disclosure of such other information to Samaritan. This requirement does not apply to Customer Data.

5.4 Confidentiality of Samaritan Information. Customer will keep confidential, and will not use for any purpose other than this Agreement, any information disclosed by Samaritan to Customer about, or that is learned or observed by Customer from, the technologies, methodologies, equipment, software and processes used by Samaritan as well as the Licensed Software, Client Software, Documentation, and Services. Customer will ensure that its employees, agents, representatives and contractors comply with these obligations. Any exceptions to this paragraph may only be granted in writing by Samaritan. This paragraph will not prohibit the Customer from making general comments regarding its user experiences with Services and Licensed Software.

5.5 Exceptions. Neither Party will have any obligation under Sections 5.3 and 5.4 above with respect to information that is publicly known at the time of first disclosure to the receiving Party or that is in the receiving Party’s possession prior to first disclosure by the disclosing Party to the receiving Party. If through no fault of the receiving Party, any confidential information of the disclosing Party subsequently becomes publicly known, then the receiving Party will thereafter have no obligation under Section 5.3 or 5.4 with respect to such publicly known information. If any information is lawfully disclosed or licensed by a third party to a receiving Party, then Sections 5.3 and 5.4 will not restrict the receiving Party from making any use or disclosure thereof that is lawfully authorized by the third party. If any disclosure of confidential information is required by law, government regulation, or court order, the receiving Party may make such disclosure, but the receiving Party must first give notice thereof to the disclosing Party and cooperate with the reasonable request of the disclosing Party, at the disclosing Party’s expense, in seeking and obtaining any protective orders or other protections that might be available. This Section does not apply to or excuse any infringement of copyrights or patent rights. Notwithstanding anything to the contrary, Samaritan has no obligation or restriction with respect to any Feedback - see Section 5.8 below. Notwithstanding anything to the contrary, the restrictions and obligations in this Agreement (or in any other agreement) applicable to Customer Data or any confidential or proprietary information of Customer do not apply to any Licensed Global Publishing Content under Appendix F.

5.6 Pricing and Terms. Customer will not disclose any of the fees or other pricing or other terms or conditions of this Agreement to any third party or any Authorized User who is not an employee of Customer.

5.7 No Hire. For the Term of this Agreement plus two years, Customer will ensure that Customer and its affiliates do not hire or engage any of Samaritan’s employees as employees or contractors, without the advance written consent of Samaritan in each case. Such consent may be withheld.

5.8 Feedback. Customer and its Authorized Users are invited to provide Feedback to Samaritan. As used in this Agreement, “Feedback” means any feedback, recommendations, criticisms, enhancements, improvements, ideas, features, functionality, capabilities, methods, processes, and
information relating to any Licensed Software, Client Software, Services or Samaritan’s business. Samaritan has the right, but not the obligation, to incorporate any Feedback into any products, software or services and to otherwise use, implement, make, practice, modify, enhance, and commercialize Feedback without any obligation to account to Customer or Authorized Users. This right also applies to any Affiliates, successors and designees of Samaritan.

Section 6 - Term and Termination

6.1 Term and Termination. The “Term” of this Agreement is the “Initial Term” plus any Renewal Period(s). The Initial Term and Renewal Periods are defined in Appendix D attached hereto. At the end of the Initial Term, this Agreement may be renewed on a renewal period-to-renewal period basis thereafter, but only if and for each Renewal Period that is agreed to by the Parties in writing or for which Customer pays an invoice from Samaritan. This Agreement will terminate and expire at the end of the Term of this Agreement. The Agreement (including the Term) is subject to earlier termination only as described below or elsewhere in this Agreement.

6.2 Breach. If either Party breaches this Agreement and fails to cure said breach within 30 days after receiving notice of said breach from the non-breaching Party, then the non-breaching Party may terminate this Agreement. This Section will not limit the relief, remedies and damages to which the non-breaching Party may be entitled. A failure to make payment is considered a material breach of this Agreement. A party will be deemed in breach of this Agreement for the purposes of this Section if such Party is or becomes insolvent or unable to pay its debts in a timely manner.

6.3 Effect of Termination. In the event of any termination or expiration of this Agreement, the following will apply: (a) Sections 4.3, 4.4, 4.5, 5, 6, 7, and 8 and all obligations to indemnify or hold harmless and all provisions relating to the protection of Licensed Software, Client Software, Documentation or Samaritan’s intellectual property will survive termination or expiration and remain in effect; (b) Termination or expiration of this Agreement will not affect or delay any payment under this Agreement that accrues or is payable prior to, or that is for any right or Services performed prior to, such expiration or termination; (c) All licenses and rights of Customer under this Agreement will terminate and all access to and use of the Licensed Software, Documentation and Client Software by Customer will terminate; and (d) Services will cease. Customer must ensure compliance of all Authorized Users, employees, agents, representatives, contractors and affiliates with these obligations.

6.4 Data Storage Without Access Following Termination. If and as mutually agreed in writing, Samaritan may continue to store Customer Data on Samaritan Servers following termination of this Agreement for an agreed-upon temporary period of time and without Customer or Authorized Users having any license or right to use any Licensed Software or Client Software or to transmit or access Customer Data to or from Samaritan Servers (the “Temporary Customer Data Storage Services”). If the Parties do not reach agreement on Temporary Customer Data Storage Services within 30 days of the termination or expiration of this Agreement or if the Customer declines Temporary Customer Data
Storage Services, then Samaritan may erase or destroy the Customer Data. No later than 27 days after the termination or expiration of this Agreement Customer may request and be granted by Samaritan a temporary access to the Licensed Software not to exceed 72 hours in order to export the Customer Data, but for no other purpose. Such Temporary Customer Data Storage Services will be considered Services under this Agreement and the provisions of this Agreement that are relevant to the Customer Data Storage Services will survive termination and remain in effect for such purpose for the duration of the temporary storage. If the License and this Agreement are fully reinstated by mutually written agreement of the Parties, then the stored Customer Data will be available to Customer for access and use in accordance with the reinstated License and Agreement.

Section 7 - Disclaimers, Limitations, Warranties, and Indemnification

7.1 Disclaimer. SAMARITAN MAKES NO WARRANTY, REPRESENTATION OR PROMISE NOT EXPRESSLY SET FORTH IN THIS AGREEMENT. EXCEPT AS EXPRESSLY WARRANTED IN THIS AGREEMENT, THE LICENSED SOFTWARE, CLIENT SOFTWARE, DOCUMENTATION, AND SERVICES ARE PROVIDED ON AN “AS IS” BASIS. THERE IS NO WARRANTY THAT THE LICENSED SOFTWARE, CLIENT SOFTWARE, DOCUMENTATION OR SERVICES ARE ERROR FREE OR THAT THEY WILL BE UNINTERRUPTED. SAMARITAN DISCLAIMS AND EXCLUDES ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. SAMARITAN MAKES NO WARRANTY WITH RESPECT TO ANY HARDWARE, SOFTWARE OR PRODUCT OF ANY THIRD PARTY. Samaritan shall have no liability under any provision of this Agreement or otherwise with respect to any performance problem, claim of infringement, or other matter to the extent attributable to: (a) any unauthorized or improper access, use or modification of the Licensed Software, Documentation, Client Software or Services, or (b) any combination of any of the Licensed Software, Documentation, Client Software and/or Services with anything not provided by Samaritan (other than as specified in the Specified Configuration provided by Samaritan), or (c) any third party data, or (d) any act or omission by Customer, its affiliates or its Authorized Users, employees, agents, representatives, contractors, clients or customers, or (e) any breach of this Agreement by Customer. Customer is solely responsible for the results obtained from the use of the Licensed Software, Documentation, Client Software, and Services and any reliance thereon.

7.2 Limitation on Liability. SAMARITAN’S AGGREGATE LIABILITY ARISING FROM OR RELATING TO THIS AGREEMENT OR THE LICENSED SOFTWARE, LICENSE, CLIENT SOFTWARE, DOCUMENTATION, OR SERVICES (REGARDLESS OF THE FORM OF ACTION OR CLAIM - E.G. CONTRACT, WARRANTY, TORT, MALPRACTICE, AND/OR OTHERWISE) WILL NOT EXCEED A LIMIT EQUAL TO THE ANNUAL SUBSCRIPTION FEE RECEIVED BY SAMARITAN FROM CUSTOMER FOR THE FIRST YEAR OF THIS AGREEMENT. SAMARITAN WILL NOT IN ANY CASE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, INDIRECT, EXEMPLARY, OR PUNITIVE DAMAGES OR FOR LOSS OF PROFITS, REVENUE, OR BUSINESS, EVEN IF SAMARITAN HAS BEEN ADVISED OF THE POSSIBILITY THEREOF. SAMARITAN IS NOT RESPONSIBLE FOR LOSS OF USE OF ANY WEBSITE, INTERNET ACCESS, HARDWARE OR SOFTWARE, LOSS OF DATA, COSTS OF RE-CREATING LOST DATA, THE COST OF ANY SUBSTITUTE PERFORMANCE,
EQUIPMENT, SOFTWARE, OR SYSTEM, OR CLAIMS BY ANY PARTY OTHER THAN CUSTOMER. THIS
AGREEMENT, AND SECTION 7 IN PARTICULAR, DEFINES A MUTUALLY AGREED UPON ALLOCATION OF
RISK AND THE FEES AND OTHER CONSIDERATION HAVE BEEN SET TO REFLECT SUCH ALLOCATION. IF
CUSTOMER DOES NOT GIVE SAMARITAN NOTICE OF ANY CLAIM BY CUSTOMER AGAINST SAMARITAN
WITHIN ONE YEAR OF THE DATE THE CLAIM ARISES, THEN SUCH CLAIM IS WAIVED AND RELEASED BY
CUSTOMER.

7.3 Responsibility for Results and Third Party Web Sites, Content, Services, and Products.
Customer acknowledges that the Licensed Software is a complex software application and that Customer
and its Authorized Users, and anyone else relying thereon are cautioned and expected to verify any results
or work product obtained through use of the Licensed Software, Client Software, Services, and
Documentation. Samaritan will not be responsible or liable for such results or work product. The Licensed
Software or its use may enable or invite links to the websites of third parties or the use of third party
content, data, services, or products. Samaritan makes no warranty, express or implied, concerning such
third party web sites or third party content, data, services, or products, or third party privacy or use
policies or practices, and they are accessed, used and relied upon at the sole risk of Customer and its
Authorized Users. Samaritan will have no liability or obligation relating to any such third party or any third
party websites or third party content, services, data, or products, or third party privacy or use policies or
practices even if such third party content and/or data are stored on or served from Samaritan Servers.

7.4 Reliance on Instructions from Customer. Samaritan may rely on and act in accordance
with any instructions, request or information provided to Samaritan by Customer or any of its employees,
officers, agents, volunteers, affiliates or contractors, and will incur no liability in doing so. Customer will
indemnify Samaritan and its officers, managers, employees and representatives against, and hold them
harmless from, any and all claims, actions, damages, liabilities, costs and expenses, including without
limitation reasonable attorneys’ fees and expenses, arising out of or resulting from Samaritan acting in
accordance with such instructions, request or information.

7.5 Other Limitations. The warranties made by Samaritan in this Agreement, and the
obligations of Samaritan under this Agreement, run only to Customer and not to its Authorized Users,
affiliates, agents, representatives, contractors, clients, customers, or any other persons. Under no
circumstances shall any Authorized User, affiliate, agent, representative, contractor, client, customer or
other person be considered a third party beneficiary of this Agreement or otherwise entitled to any rights
or remedies under this Agreement. Customer shall have no rights or remedies against Samaritan except
as specifically provided in this Agreement. Samaritan shall not be deemed Customer’s official record
keeper for regulatory, government or other purposes and shall have no obligation to retain any records
or data on Customer’s behalf during the Term or after termination or expiration of this Agreement, but
this does not negate or alter Samaritan’s obligations with respect to Data Storage Services and Temporary
Customer Data Storage Services as expressly stated in this Agreement.
7.6 Third Party Licensors and Providers. The limitations, disclaimers and protections of Sections 7.1 to 7.5 may be extended by Samaritan to any third party who licenses or provides to Samaritan any software, data, services, products, or intellectual property relevant to Licensed Software, Client Software, Documentation, Services or this Agreement.

7.7 Warranties of Customer.

(a) Customer Materials. Customer warrants that any trade names, service marks, trademarks, logos, text, works of authorship, designs, data, and other materials provided by or on behalf of Customer to Samaritan for inclusion in, or for use with, the Licensed Software, Documentation or Services (“Customer Materials”) do not and will not (and such inclusion and use do not and will not) infringe, misappropriate, breach or violate any trade name, trademark, service mark, copyright, patent, trade secret or other intellectual property or right of or obligation to a third party and that Customer has provided and granted to Samaritan all rights necessary for such inclusion and use of Customer Materials. Customer shall indemnify and defend Samaritan and Samaritan’s affiliates, directors, officers, employees, shareholders, and representatives against, and hold them harmless from, any such claim and any liabilities, judgments, awards, settlements, damages, losses, attorneys’ fees, and costs arising from or attributable to such claims or relating to Customer Materials.

(b) No Unlawful or Disreputable Purpose. Customer warrants that Customer and its Authorized Users will not access or use any of the Licensed Software, Documentation, Client Software or Services for any unlawful, dishonest, disreputable, illegitimate, or immoral purpose and will not disparage Samaritan or its Licensed Software, Client Software or Services to others. Any breach of this warranty will entitle Samaritan to terminate this Agreement under Section 6.2 effective immediately upon notice and the 30 day cure period will not apply.

7.8 Warranty by Samaritan.

Samaritan warrants that if the Licensed Software does not comply with its then-current Documentation in any material respect and Customer gives notice of such non-compliance to Samaritan, then Samaritan will correct the Licensed Software or provide a work-around solution as the sole and exclusive remedy. If the Documentation is in error, then Samaritan may correct the Documentation.

7.9 Indemnification by Samaritan.

In the event that the Customer’s licensed use of the Licensed Software or the Services infringe any U.S. patent, trade secret, copyright, trademark or service mark of a third party, Samaritan shall indemnify Customer as follows:

(a) Indemnification. In any litigation by the third party against Customer, Samaritan shall pay any monetary judgments (unless otherwise settled as provided below), including damages, attorneys’ fees and costs that are awarded by a court of competent jurisdiction to the third party for such infringement claim. Samaritan shall pay any amount paid to settle such infringement claim or litigation,
provided that the settlement is approved in writing by Samaritan. Samaritan shall defend Customer in any such litigation against claims of such infringement and shall pay all attorneys’ fees and other costs of such defense. Samaritan does not have any obligation to pay for any other damages of Customer or for any loss of profits or business.

(b) **Conditions.** Samaritan’ obligations hereunder are conditioned on the following: (1) Customer must promptly give written notice to Samaritan of any claim against Customer alleging such infringement, (2) Customer must allow Samaritan to control the defense and settlement of such claim and any litigation or arbitration of such claim or infringement and the venue thereof, and (3) Customer must fully cooperate with Samaritan in connection with such defense, settlement, litigation and arbitration. Samaritan shall have no obligation or liability if the infringement or claim arises from or is based upon: (i) any change, modification or addition to the Licensed Software or Services, or (ii) the use or existence of the Licensed Software or Services in combination with anything not sold or provided by Samaritan to Customer, or (iii) the use of the Licensed Software or Services other than as described in the Documentation provided by Samaritan, or (iv) specifications, requirements, trademarks or other Customer Materials requested, specified or required by Customer for the Licensed Software or the Services, or (v) any patent that issues after the date of this Agreement, or (vi) the law of any foreign country or jurisdiction. Customer must mitigate damages in the event of infringement and cooperate with the reasonable request of Samaritan for mitigation. If requested by Samaritan, Customer shall cease access to and use of any infringing Licensed Software or Services. Samaritan shall have no obligation or liability with respect to claims brought by third parties who are affiliated with Customer.

(c) **Injunction or Cessation of Use.** If Customer is enjoined from continued use of any infringing Licensed Software or Services or if Customer ceases use of any Licensed Software or Services at the request of Samaritan under (b) above, then Samaritan shall (at its expense and option): (i) obtain the right for Customer to continue to use the Licensed Software or Services in accordance with the user documentation which accompanied the Licensed Software and this Agreement, (ii) modify the infringing Licensed Software or Services to eliminate the infringement, or (iii) terminate this Agreement and the License.

(d) **Clarifications.** In the event that Samaritan and the third party agree to arbitration, then the foregoing shall apply to such arbitration in the same manner as litigation. Any reference in this Section to “infringement” shall mean, when used in the context of a trade secret, the “misappropriation” of a trade secret.

(e) **Warranties.** WITH RESPECT TO EXPRESS OR IMPLIED WARRANTIES OF NONINFRINGEMENT BY SAMARITAN, IF ANY, THIS INDEMNIFICATION SECTION 7.9 SHALL GOVERN AND SHALL CONSTITUTE CUSTOMER’S SOLE AND EXCLUSIVE REMEDY AND SAMARITAN’S SOLE AND EXCLUSIVE LIABILITY FOR ANY BREACH OF SUCH WARRANTY AND FOR ANY INFRINGEMENT CAUSED BY OR ATTRIBUTABLE TO THE LICENSED SOFTWARE OR SERVICES.
(f) **Documentation and Client Software.** This Section 7.9 shall also apply to Documentation and Client Software in the same manner that it applies to the Licensed Software.

(g) **Entire Obligation and Liability.** Samaritan shall have no obligation or liability to Customer other than this Section 7.9 for, or in the event of, any infringement or misappropriation of intellectual property.

Section 8 - General Provisions

8.1 **Assignment and Successors.** This Agreement is not assignable or transferable, except that this Agreement may be assigned or transferred by Samaritan to any third party who acquires substantially all of Samaritan’s intellectual property in and to the Licensed Software and who will continue to provide the Services to Customer in accordance with the Agreement for the Term. Any assignee or transferee to whom this Agreement is assigned or transferred must assume the assigning Party’s duties and obligations under this Agreement.

8.2 **Governing Law and Forum.** This Agreement will be governed by the laws of the State of Utah without giving effect to conflict or choice of law principles. Any litigation between the Parties will be conducted exclusively in a state or federal court of competent jurisdiction within Utah and such court’s appellate courts. The Parties agree and submit to such exclusive jurisdiction and venue.

8.3 **Force Majeure.** Except for obligations to make payment, neither Party will be deemed in breach of this Agreement or liable for any failure to perform an obligation where such failure is caused by an Act of God, fire, flood, earthquake, storm, terrorism, war, crime, change in law or regulation, any disruption, outage or malfunction of or interference in communications, network, equipment or software, act of any military, civil or regulatory authority, the Internet, any third party, any disruption or delay in supplies, power, or other utilities, any labor dispute or shortage, or circumstances beyond the control of that Party (each of the foregoing is referred to as a “Force Majeure”). It is also understood that downtime of Samaritan Servers and Licensed Software for maintenance, re-location, and other purposes will be necessary from time to time and that unintended interruptions and unscheduled downtime may also occur and are not a breach of this Agreement.

8.4 **Waiver.** Any waiver of any breach or obligation under this Agreement must be in writing and any waiver of a breach will not be construed as a waiver of subsequent or similar breaches.

8.5 **Construction.** This Agreement represents the wording selected by the Parties to define their agreement and no rule of strict construction will apply against or in favor of either Party. This Agreement is written in, and will be governed by, the English language.
8.6 **Relationship.** Neither Party is the partner, joint venturer, agent or representative of the other Party. Each Party is an independent contractor. There is no employment relationship between the Parties. Neither Party has the authority to make any representations or warranties or incur any obligations or liabilities on behalf of the other Party. Neither Party will make any representation to a third party inconsistent with this Section.

8.7 **Contractors.** Samaritan may subcontract its obligations or responsibilities to subcontractors, but this will not excuse Samaritan from its obligations and responsibilities under this Agreement.

8.8 **Export Laws and Use Outside of the United States.** Customer shall comply with all export laws and regulations and government orders applicable to the Licensed Software, Documentation, Client Software or this Agreement. Customer shall not export or re-export directly or indirectly (including via remote access) any part of the Licensed Software, Documentation or Client Software or any confidential or proprietary information to any jurisdiction, country or person in violation of such laws, regulations or government orders. Unless expressly stated otherwise in Appendix D, the License, all use by Customer of the Licensed Software, Documentation, and Client Software is limited to the United States of America.

8.9 **Injunctive and other Equitable Relief.** Each party acknowledges that the restrictions and protections in this Agreement relating to the protection of Licensed Software, Documentation, Client Software, Customer Data and confidential information are reasonable and necessary to protect the other Party's legitimate business and intellectual property interests. Each party acknowledges that any breach of any such restrictions will result in irreparable injury to the other Party for which money damages could not adequately compensate. If there is a breach, then the injured party shall be entitled, in addition to all other rights and remedies which it may have at law or in equity, to have a decree of specific performance and preliminary and permanent injunctions issued by any court of competent jurisdiction, requiring the breach to be cured and enjoining all persons involved from continuing the breach. The existence of any claim or cause of action that a Party or any other person may have against the other Party shall not constitute a defense or bar to the enforcement of any of the provisions of this Section 8.9.

8.10 **Entire Agreement.** This Agreement (including the Appendices): (i) represents the entire agreement between the Parties relating to the subject matter of this Agreement, (ii) supersedes all prior agreements, understandings, representations and warranties applicable to the subject matter of this Agreement, and (iii) may only be amended, canceled or rescinded by a writing signed by both Parties. Any terms or conditions of any purchase order or other document submitted by Customer in connection with this Agreement, the License, any Licensed Software or any Services, which are in addition to, different from or inconsistent with the terms and conditions of this Agreement are not binding on Samaritan and are ineffective.

8.11 **Notices.** Notices under this Agreement will be directed to the other Party’s notice address provided in Appendix C attached hereto. Either Party may amend the name, information and address for
its contact person by notice to the other Party, and such notice will constitute an amendment of Appendix C. Any notices required by this Agreement must be in writing.

8.12 Special Conditions and Exceptions. Special Conditions and Exceptions, if any, are set forth in Appendix E. In the event of any conflict between the Special Conditions and Exceptions and the other provisions of this Agreement, the Special Conditions and Exception will govern.

8.13 Execution and Authority. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. Each person signing below represents that he/she is duly authorized to execute this Agreement for and on behalf of the Party for whom he/she is signing.

AGREED TO AND ACCEPTED BY:

___________________  Samaritan Software, LLC
(“Customer”)  (“Samaritan”)

By (signature):  _____________________  By (signature):  _____________________
Name (print):  _____________________  Name (print):  _____________________
Title:  _____________________  Title:  _____________________
Date:  _____________________  Date:  _____________________
Appendix A

1. **Licensed Software**

<table>
<thead>
<tr>
<th>CLIN</th>
<th>Item</th>
<th>Description</th>
<th>Licensed Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>100A</td>
<td>Samaritan eRecruiter</td>
<td>Web based forms for opportunity searching, volunteer registration, interactive scheduling and surveys.</td>
<td></td>
</tr>
<tr>
<td>102A</td>
<td>Samaritan eCoordinator</td>
<td>Samaritan’s web-server based software and database for managing volunteers, opportunities for volunteer service, and organizations which provide opportunities for volunteer service.</td>
<td></td>
</tr>
<tr>
<td>101G</td>
<td>Sign-In Stations</td>
<td>Capability to set up unlimited designated web-enabled terminals for use as time clocks for volunteers.</td>
<td></td>
</tr>
</tbody>
</table>

As governed by Section 1.7 of this Agreement

2. **Client Software**

As defined in Section 1.10 of this Agreement
B. Specified Configuration

1. Specified Configuration (required on Customer computers):
   - Adobe Reader
   - Some reports are optionally available in Microsoft Excel format.
   - Internet Explorer 11 or later, Microsoft Edge, Google Chrome, Firefox, or Safari
   - And any system software required to run the above software
   - High speed Internet connection
     (at a minimum 100 kbps, higher speeds recommended)

C. Statement of Services

1. Implementation Services
   CLIN 500B “Initial Configuration Hours”

   During the Initial Term Samaritan shall configure the Licensed Software, in accordance with the existing features and functionality of the Licensed Software, and per the project scope and specifications described herein or agreed upon by the Customer’s documented Support Contact(s) and Samaritan’s Support Contact. Total hours purchased for configuration during the initial term is X hours.

   CLIN 500C “Data Conversion Support Time”

   Samaritan shall allow the Customer to do a data conversion from a current flat file into the Licensed Software for the purposes of populating the Customer’s instance of the Licensed Software with current transfer data. X hours have been purchased for this event.

2. Training
   CLIN 600A Basic Training

   Samaritan shall deliver during the initial phase up to 8 hours of basic user training on-site at the Customer’s request as outlined in the final proposal. Classroom training is limited to 15 participants for every 3-4 hour block of time.
CLIN 500E  “Criminal Background Checking Setup Fee”

During the Initial Term Samaritan shall configure the Licensed Software, in accordance with the existing features and functionality of the Licensed Software, and per the project scope and specifications described herein or agreed upon by the Customer’s documented Support Contact(s) and Samaritan’s Support Contact for the purposes of enabling the software to perform background checks.

Total implementation setup fee purchased for configuration during the initial term is 1 setup.

CLIN 803B  “U.S. One Search (BackgroundChecks.com)”

During the Initial Term Samaritan shall configure the Licensed Software, in accordance with the existing features and functionality of the Licensed Software, for the ability to connect with BackgroundCheck.com. Total checks purchased for use during the initial term is X checks.

3. Post Implementation Configuration Change Services

[None at this time]

4. Support and Maintenance Services:

CLIN 500C  “Basic Customer Support Hours”

As described in Sections 3.1 and 3.2 of the Agreement.

Maximum Number of Support Hours per year: X Hours purchased for this agreement.

Standard Customer Support Coverage:

Samaritan shall provide Tier II telephone support via telephone, fax, emails, or Internet chat from 8:00 am to 5:00 pm (Mountain Time) Monday through Friday excluding national and Utah state holidays.

Definitions of Levels of support:

Tier II support, meaning that all support request will be presented to Samaritan’s Customer Support department by Customer’s documented Support Contact(s) listed in Appendix C during the times and days of support availability defined above.
5. **Standard Additional Services (included at no charge)**

Shared Server, Data Center, and FTP Access

The Licensed Software for Customer shall be hosted on a Samaritan Server in conjunction with other of Samaritan’s shared server users at Samaritan’s own or a sub-contracted managed hosting facility that meets or exceeds current industry standards with restricted physical access, backup power sources, and redundant Internet feeds. Customer personnel, upon request to Samaritan, may be granted FTP (or similar) access to facilitate access and/or storage of website files related to the Licensed Software and this agreement.

Firewall and SSL Certificate

To secure access to the Samaritan Server Samaritan shall maintain the Samaritan Server behind a hardware firewall. Samaritan shall provide a 128-bit Secure Socket Layer (SSL) certificate to encrypt data transfer between the Samaritan Server and Authorized Users.

Server Backup

Samaritan shall perform nightly full backups of the server system software with 7 day offsite retention and nightly database backups with 30 day offsite retention.

Anti-Virus

Samaritan shall protect the Samaritan Server with anti-virus software with updates and additional virus signatures installed as they become available.

D. **Assumptions**

1. **Bandwidth allowances:** 2 GB. Samaritan assumes that the Customer data transfer bandwidth usage to and from the Samaritan Server will not use more than 2 GB per month. Monthly data transfer in excess of this amount may incur an overage charge of $1.25 per GB per month.
### E. Customer Deliverables

<table>
<thead>
<tr>
<th>CLIN</th>
<th>Item</th>
<th>Description</th>
<th>Applicable License</th>
</tr>
</thead>
<tbody>
<tr>
<td>900A</td>
<td>General Deliverable</td>
<td>Customer agrees that during all phases of this project they will provide a dedicated point of contact that will participate in weekly conference calls with a dedicated contact client services representative at Samaritan Technologies.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>900B</td>
<td>General Deliverable</td>
<td>Customer agrees that any requests for data, data conversions, graphics or the like needed during the design and implementation phase will be agreed upon in writing with specified due dates.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901A</td>
<td>eRecruiter</td>
<td>Customer will indicate a reference webpage which will provide an example of the look and feel to be used in the design of their eRecruiter.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901B</td>
<td>eRecruiter</td>
<td>Customer agrees to supply any customer owned logos or graphics necessary to achieve the desired look and feel of their eRecruiter.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901C</td>
<td>eRecruiter</td>
<td>Customer will indicate which webpage will contain a link to their eRecruiter.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901D</td>
<td>eRecruiter</td>
<td>Customer will indicate their selection of eRecruiter opportunity search methods.</td>
<td>All Licenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>901E</td>
<td>eRecruiter</td>
<td>Customer will specify their default eRecruiter placement and referral options.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901F</td>
<td>eRecruiter</td>
<td>Customer will supply a list of data items that will included in their volunteer reference surveys which data items are required and the order thereof for eRecruiter and eCoordinator respectively.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901G</td>
<td>eRecruiter</td>
<td>Customer will provide guidance for the graphical design of any volunteer reference surveys.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901H</td>
<td>eRecruiter</td>
<td>Customer will indicate whether or not organizations, opportunities, clients, or volunteers require approval for placement.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901I</td>
<td>eRecruiter</td>
<td>Customer will specify which items of eRecruiter functionality are available to the general public and which require login.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>901J</td>
<td>eRecruiter</td>
<td>Customer will provide a phone number that volunteers should call when they forget their passwords.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>902A</td>
<td>eCoordinator</td>
<td>Customer will supply a list of data items to be included in volunteer profiles which data items are required and the order thereof for eRecruiter and eCoordinator respectively.</td>
<td>All Licenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer will supply a list of data items to be included in opportunity profiles which data items are required and the order thereof for eRecruiter and eCoordinator respectively.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>902B</td>
<td>eCoordinator</td>
<td>Customer will supply a list of data items to be included in organization profiles which data items are required and the order thereof for eRecruiter and eCoordinator respectively.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>902C</td>
<td>eCoordinator</td>
<td>Customer will supply a list of data items to be included in client profiles which data items are required and the order thereof for eRecruiter and eCoordinator respectively.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>902D</td>
<td>eCoordinator</td>
<td>Customer will supply a list of data items that will be included in their volunteer surveys which data items are required and the order thereof for eRecruiter and eCoordinator respectively.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>902E</td>
<td>eCoordinator</td>
<td>Customer will specify a list of volunteer activity status values which are acceptable for volunteer placement.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>902F</td>
<td>eCoordinator</td>
<td>Customer will provide a list of credentials required for opportunity placement.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>902G</td>
<td>eCoordinator</td>
<td>Customer will select from among the available format options for dates, times and phone numbers.</td>
<td>All Licenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>902I</td>
<td>eCoordinator</td>
<td>Customer will indicate which surveys are one time use only.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>903A</td>
<td>Sign-In Stations</td>
<td>Customer will provide guidance for the graphical design of any sign-in stations.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>904A</td>
<td>Background Checks</td>
<td>Customer will indicate their selection of background check packages if integrated background checks are included in the Service Proposal.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>904B</td>
<td>Background Checks</td>
<td>Customer will provide a list of volunteer restrictions based on background check outcomes.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>905A</td>
<td>Administrative Tools</td>
<td>Customer will specify any user role access requirements.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>905B</td>
<td>Administrative Tools</td>
<td>Customer agrees to specify and/or approve the content of any automatic emails to be sent by their volunteer management system.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>905C</td>
<td>Administrative Tools</td>
<td>Customer will supply a list of eCoordinator users including their names, email address and phone numbers and the roles to which each will be assigned.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>905D</td>
<td>Administrative Tools</td>
<td>Customer will provide a banner graphic for their eCoordinator accounts.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>905E</td>
<td>Administrative Tools</td>
<td>Customer will provide information about the organizational hierarchy of their eCoordinator users.</td>
<td>All Licenses</td>
</tr>
<tr>
<td></td>
<td>Administrative Tools</td>
<td>Customer will specify their automatic inactivity logout times.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>---</td>
<td>----------------------</td>
<td>-------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>905G</td>
<td>Administrative Tools</td>
<td>Customer will indicate their preference of social media integration options.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>905H</td>
<td>Administrative Tools</td>
<td>Customer will assist Samaritan in determining the appropriate folder organization for their system and the access and functionality associated there with.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>905I</td>
<td>Administrative Tools</td>
<td>Customer will indicate if any training or test accounts are required.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>906A</td>
<td>Conversion and Integration</td>
<td>Customer agrees to provide access to any data that is part of the data conversion in a mutually acceptable format.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>906B</td>
<td>Conversion and Integration</td>
<td>Customer agrees to specify and approve the mapping of any old data into their new volunteer management system as part of any data conversion.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>906C</td>
<td>Conversion and Integration</td>
<td>Customer agrees to work with Samaritan to determine the interface specifications necessary for any volunteer management system integration.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>907A</td>
<td>Training</td>
<td>Customer will agree upon a time and method for any trainings they have ordered.</td>
<td>All Licenses</td>
</tr>
<tr>
<td></td>
<td>Training</td>
<td>Customer agrees that after training, customer will be primarily responsible for the configuration of eCoordinator accounts, eRecruiters, eRecruiter add-on modules and sign in stations and any functionality associated there with.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>---</td>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>907B</td>
<td>Training</td>
<td>Customer agrees to provide any Tier 1 Support to the authorized end users of its volunteer management system.</td>
<td>All Licenses</td>
</tr>
<tr>
<td>907C</td>
<td>Training</td>
<td>If Samaritan provides Train the Trainer training is complete, customer will provide training to the authorized end users of its volunteer management system.</td>
<td>All Licenses</td>
</tr>
</tbody>
</table>


Appendix B

**Fee and Payment Schedule**

**Initial Term (First Year):**

<table>
<thead>
<tr>
<th>#</th>
<th>Products</th>
<th>Qty</th>
<th>List</th>
<th>(Discount)</th>
<th>Prices</th>
<th>Payment Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>100A</td>
<td>Samaritan eRecruiter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contract Execution</td>
</tr>
<tr>
<td>101G</td>
<td>eRecruiter Sign-in Station Module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contract Execution</td>
</tr>
<tr>
<td>102A</td>
<td>Samaritan eCoordinator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contract Execution</td>
</tr>
<tr>
<td></td>
<td><strong>Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>500B</td>
<td>Configuration Hours</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Monthly</td>
</tr>
<tr>
<td>500C</td>
<td>Technical Support Hours “Telephone Support”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>As Used</td>
</tr>
<tr>
<td>500C</td>
<td>Technical Support Hours “Data Conversion”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>On Delivery</td>
</tr>
<tr>
<td>500E</td>
<td>Criminal Background System: One Time Setup Fee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>On Delivery</td>
</tr>
<tr>
<td>600A</td>
<td>Basic User Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>On Delivery</td>
</tr>
<tr>
<td>803B</td>
<td>U.S. One Search (BackgroundChecks.com)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>On Delivery</td>
</tr>
<tr>
<td></td>
<td><strong>Totals</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Additional Years (optional):

<table>
<thead>
<tr>
<th>#</th>
<th>Products</th>
<th>Qty</th>
<th>List</th>
<th>(Discount)</th>
<th>Prices</th>
<th>Payment Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>100A</td>
<td>Samaritan eRecruiter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contract Renewal</td>
</tr>
<tr>
<td>101G</td>
<td>eRecruiter Sign-in Station Module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contract Renewal</td>
</tr>
<tr>
<td>102A</td>
<td>Samaritan eCoordinator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Contract Renewal</td>
</tr>
</tbody>
</table>

#### Services

| 500C | Technical Support Hours “Telephone Support”  | TBD |      |            |        |                  |

#### Totals

The Annual Subscription Fee, Annual Support Fee, and Other Fees are subject to increase by Samaritan for any Renewal Period.

For Additional Services:

Samaritan’s then-current standard fees and rates will apply.
Appendix C

Notices and Support Contacts

Notices Contacts:

Each Party has designated for itself at least one notice address below. Notices relating to this Agreement will be directed to the other Party’s notice address as follows:

Customer’s Notice Address:

Name:
Address:
Telephone:
Fax:
E-mail:

Samaritan’s Notice Address:

Name: Bruce Behymer
Address: 265 E. 100 South, Suite 290
          Salt Lake City, UT 84111
Telephone: 801.328.3972
Fax: 801.328.3966
E-mail: notices@samaritan.com

Customer’s Support Contact Person:

Name:
Address:
Telephone:
E-mail:
Appendix D

Limits

A. Term

Term = Initial Term plus any Renewal Period(s)

Initial Term = the time period beginning on the date of this Agreement and ending one year after the date that a user ID to the Licensed Software is issued to an Authorized User under this Agreement.

Renewal Period = One (1) year with additional renewal periods as requested by Customer.

B. Authorized Users

Only Authorized Users may access and use the Licensed Software under this Agreement. “Authorized Users” are defined or described separately for each Licensed Software application as follows:

1. Authorized Users of eCoordinator:
   (a) Employees. Employees of Customer who access and use eCoordinator for Customer solely within the scope of their employment with Customer will be Authorized Users of eCoordinator.

2. Authorized Users of Account Management System (“AMS”) and Recruiter Management System (“RMS”) (If any licenses purchased):
   (a) AMS and RMS. Section B. 1. above will apply to AMS and RMS in the same manner that it applies to eCoordinator.

3. Authorized Users of eRecruiter and eRecruiter extension modules (if any licenses purchased):
   (a) Employees. Employees of Customer who access and use eRecruiter for Customer solely within the scope of their employment with Customer will be Authorized Users of eRecruiter.

   (b) Third Parties. Documentation for eRecruiter contemplates that persons (who are not employees of Customer) may access and use eRecruiter. Such persons include potential volunteer coordinators, volunteers, referencers, donors, and approvers who have a relationship with Customer. Such persons will be Authorized Users of eRecruiter, provided that they access and use eRecruiter only as described in the applicable Documentation and only in connection with their relationship with
Customer. They may not access or use eRecruiter for any other purpose.

4. Authorized Users of Sign-In (if any licenses purchased):

(a) Employees. Employees of Customer who access and use Sign-In for Customer solely within the scope of their employment with Customer will be Authorized Users of Sign-In.

(b) Third Parties. The Documentation for Sign-In contemplates that persons (who are not employees of Customer) may access and use eRecruiter. Such persons include volunteer coordinators and volunteers who have a relationship with Customer. Such persons will be Authorized Users of Sign-In, provided that they access and use Sign-In only as described in the applicable Documentation and only in connection with their relationship with Customer. They may not access or use Sign-In for any other purpose.

5. Authorized System Users of the Application Program Interface (if any licenses purchased):

(a) Programmatic System Users. Non-human programmatic systems of Customer that access and use the Samaritan Application Interface (API) for Customer solely within the scope of their employment with Customer will be Authorized Users of the API. Human users may not use the same User ID and password to access the licensed software as a programmatic system user.

C. Number of Users

The “Number of Users” means the number of users accessing or using the Licensed Software. Each user must be an Authorized User and will be assigned a User ID (e.g., login) and password. The Number of Users must correspond to the number of assigned User IDs.

Number of eCoordinator Users for this License in year: 0
Number of eCoordinator Lite Users for this License in year: 0
Number of AMS and RMS Users for this License: 0
Number of eRecruiter Users for this License in year: 0
Number of Sign-In Users for this License: 0
Number of API System Users for this License: 0
D. **Licensed Features and Functionality**

The License for each Licensed Software application or tool is limited to the applicable Licensed Features and Functionality identified in Appendix A, and may not be exercised for any other features or functionality of the application or tool, i.e., Authorized Users are not entitled to access or use any features or functionality of the Licensed Software other than the Licensed Features and Functionality set forth above or added by amendment of the Parties to Appendix A.
Appendix E

Special Conditions and Exceptions

The following are “Special Conditions and Exceptions” and are part of this Agreement. In the event of any conflict between any Special Conditions and Exceptions and any other provision in the Agreement, the Special Conditions and Exceptions will govern.

1. None at the time of execution of this Agreement.
Appendix F
Global Publishing and Content License Terms and Conditions

Section 1 – Global Publishing

1.1 Global Publishing Folders. Samaritan’s eCoordinator software user interface provides certain folders called Global Publishing Folders. Any opportunity or organization record that an Authorized User of eCoordinator places into a Global Publishing Folder may be shared with, distributed to, and published on any of several websites for the purpose of increasing that opportunity’s or organization’s exposure and improving the likelihood of recruiting volunteers. Samaritan’s eRecruiter software also allows Authorized Users to submit opportunity and organization records for sharing, distribution and publishing through other websites. The term record as used in this Appendix means any record, data, work of authorship, content or information.

1.2 Licensed Global Publishing Content. Any record that Customer or an Authorized User puts into a Global Publishing Folder or otherwise submits through eCoordinator or eRecruiter for sharing, distribution or publishing is referred to herein as “Licensed Global Publishing Content.” Any record or copyrightable material associated with the presentation of volunteer service opportunities or organizations that is part of or linked to by the eCoordinator database records for those service opportunities or organizations is also considered part of the Licensed Global Publishing Content.

Section 2 – Publishing License

2.1 Publishing License. Customer grants to Samaritan a nonexclusive, worldwide, royalty-free license and right to copy, distribute, publish, reformat, modify, create derivative works based on, publicly perform, publicly display, and otherwise use the Licensed Global Publishing Content and to authorize others to do so (the "Publishing License"), with the right to grant sublicenses to others, subject to the restrictions in this Appendix.

2.2 Reservation of Rights. Except for the Publishing License and rights granted in this Appendix or elsewhere stated in this Agreement, Customer does not assign or convey to Samaritan any other rights in or to the Licensed Global Publishing Content. This Appendix does not limit any rights and permissible uses that Samaritan would have independent of this Appendix, including rights under the U.S. Copyright Act or other applicable intellectual property laws. Samaritan and its sublicensees retain all rights in any content created by or for Samaritan or its sublicensees in connection with the exercise of the Publishing License or rights to the Licensed Global Publishing Content. Nothing in this Appendix or the Agreement
will restrict Samaritan from copying, distributing, publishing or otherwise using content Samaritan obtains
from a source other than Customer or its Authorized Users.

2.3 **Links to Customer’s Website.** By providing the Licensed Global Publishing Content, Customer specifically allows Samaritan and its sublicensees to publish or create links from its and their websites to Customer’s website and to publish, distribute and use any links in the Licensed Global Publishing Content. Customer agrees that any web page to which any portion of the Licensed Global Publishing Content is linked will not spawn any pop-up or pop-under windows.

Section 3 – Usage and Changes

3.1 **Use of Licensed Global Publishing Content.** Samaritan may choose to republish or not republish the Licensed Global Publishing Content at Samaritan’s discretion.

3.2 **Changes and Website Terms and Conditions.** It is possible that the terms and conditions of the websites to which Samaritan distributes or published Licensed Global Publishing Content may change from time to time, and Samaritan may make changes or amendments to this Appendix as reasonably needed. If Customer does not agree to any such changes or amendments when notified, then Customer and its Authorized Users must stop all further submissions of Licensed Global Publishing Content and Customer may request that Samaritan disable the Global Publishing feature of Customer’s eCoordinator and eRecruiter accounts. Samaritan may discontinue any websites as recipients of Licensed Global Publishing Content from Samaritan and may do so at any time and without notice. Links to the terms and conditions of other websites (but not necessarily all) to which Samaritan may distribute or publish Licensed Global Publishing Content may be found on Samaritan’s website or, if not there, may be obtained by request from Samaritan and should be reviewed by Customer and Authorized Users before submitting Licensed Global Publishing Content. Samaritan is not responsible for ensuring compliance of Licensed Global Publishing Content with the terms and conditions of other websites.

Section 4 – Consent and Responsibility

4.1 **Consent.** Placing Licensed Global Publishing Content into a Global Publishing Folder or otherwise submitting Licensed Global Publishing Content is considered a request for distribution and publication and is consent to the exercise of the Publishing License and rights under this Appendix. The distribution or publication of Licensed Global Publishing Content and the exercise of any license or right under this Appendix will not be a breach of confidentiality or other breach of the Agreement by Samaritan.

4.2 **Disclaimer and Responsibility.** LICENSED GLOBAL PUBLISHING CONTENT SHOULD BE LIMITED TO RECORDS RELATING TO VOLUNTEER SERVICE OPPORTUNITIES OR ORGANIZATIONS AND SHOULD ONLY BE SUBMITTED BY AUTHORIZED USERS. SAMARITAN IS NOT RESPONSIBLE FOR ANY UNAUTHORIZED SUBMISSIONS OR FOR THE CONTENT OF ANY SUBMISSIONS. LICENSED GLOBAL PUBLISHING CONTENT SHOULD NOT INCLUDE ANY PII, PCI, OR PHI, AND IT IS CUSTOMER’S RESPONSIBILITY (NOT SAMARITAN’S RESPONSIBILITY) TO PREVENT THE SUBMISSION OF PII, PCI AND PHI. SAMARITAN HAS NO OBLIGATION TO SCREEN, EDIT, CENSOR, MODIFY, CONTROL, OR MONITOR
ANY LICENSED GLOBAL PUBLISHING CONTENT, EVEN IF DISTRIBUTED OR PUBLISHED BY SAMARITAN TO OTHERS OR TO OTHER WEBSITES. AFTER LICENSED GLOBAL PUBLISHING CONTENT IS DISTRIBUTED OR PUBLISHED BY SAMARITAN OR ITS SUBLICENSEES, IT MAY BE FURTHER DISTRIBUTED OR PUBLISHED BY OTHERS. SAMARITAN AND ITS SUBLICENSEES WILL HAVE NO RESPONSIBILITY OR LIABILITY FOR SUCH DISTRIBUTION OR PUBLICATION OR FOR ANY MODIFICATIONS OR USES THAT SUBSEQUENTLY RESULT THEREFROM. CUSTOMER AND ITS AUTHORIZED USERS HAVE NO OBLIGATION TO SUBMIT ANY LICENSED GLOBAL PUBLISHING CONTENT, BUT CUSTOMER IS RESPONSIBLE FOR ALL SUBMITTED LICENSED GLOBAL PUBLISHING CONTENT AND WILL INDEMNIFY SAMARITAN AND ITS OFFICERS, MANAGERS, EMPLOYEES, CONTRACTORS, REPRESENTATIVES AND SUBLICENSEES AGAINST, AND HOLD THEM HARMLESS FROM, ANY CLAIMS OR VIOLATIONS OF LAW BASED ON OR CAUSED BY THE LICENSED GLOBAL PUBLISHING CONTENT AND ANY JUDGMENTS, SETTLEMENTS, DAMAGES, AWARDS, EXPENSES, COSTS, LOSSES, FINES, PENALTIES, AND ATTORNEYS’ FEES ARISING FROM SUCH CLAIMS OR VIOLATIONS OF LAW. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, THIS INDEMNITY INCLUDES CLAIMS FOR VIOLATION OF PRIVACY, DEFAMATION, FALSE ADVERTISING, UNFAIR COMPETITION, AND OTHER TORTS.

4.3 Post-Termination Distribution and Publication. Even if this Appendix or the Agreement or the Publishing License is terminated, or if Customer removes the Licensed Global Publishing Content from all Global Publishing Folders, or if Samaritan discontinues distribution and publication of Licensed Global Publishing Content, it is possible that display and further distribution and publication by others of the Licensed Global Publishing Content to others may continue and Samaritan has no ability or obligation to terminate or control such further distribution and publication.

4.4 Samaritan Mark and Link. Samaritan may include the “Samaritan Mark” with any Licensed Global Publishing Content that it or its sublicensee distributes, displays or publishes. Customer will include the “Samaritan Mark” on Customer’s eRecruiter web pages. This will include a link from the Samaritan Mark (and Customer’s eRecruiter web pages) to Samaritan’s website as reasonably requested by Samaritan. The “Samaritan Mark” means the following:

Samaritan, by notice to Customer, may change the Samaritan Mark from time to time, and Customer or Samaritan will update Customer’s eRecruiter web pages with the then-current Samaritan Mark.