

SECURITY AND PRIVACY REQUIREMENTS

Published January 2015

These Security and Privacy Requirements are incorporated into and subject to the terms and conditions of the Agreement by and between ServiceMaster Consumer Services Limited Partnership (“SVM”) and Company. The Security and Privacy Requirements apply to all Statements of Work under the Agreement. In the event of a conflict between the Agreement and the Security and Privacy Requirements, the Security and Privacy Requirements will control. Any capitalized term used but not defined herein will have the meaning assigned to it in the Agreement.

Part One: Definitions & Contact Information

1. Definitions

“*Authorized Persons*” means Company’s employees, Company’s contractors, agents, outsourcers, and auditors who have a need to know or otherwise access SVM Information to enable Company to perform its obligations under the Agreement.

“*Cardholder Data*” means at minimum, the full Primary Account Number (PAN) imprinted on the credit/debit card, or embedded within the magnetic stripe of the card. When any of the following elements are with the PAN, they are also considered cardholder data: cardholder name, expiration date, service code. Magnetic stripe data (also known as track data) from a credit or debit card contains this type information and is considered cardholder data.

“*Payment Card Brand Organization*” means an organization (e.g., Visa, MasterCard, JCB, American Express, Discover, etc), that promulgates operating rules for the payment processing workflow from purchase/authorization to clearing and finally payment/settlement for their branded cards. These organizations include all processing workflows and networks debit, credit, prepaid, e-purse/virtual, ATM, and POS cards branded with their organizational logo..

“*Confidential Information*” is SVM’s Confidential Information as defined in the Agreement.

“*Electronic Communications Resource (“ECR” or “SVM ECR”)*”: means any SVM owned, authorized or provided computer, computer network, email (both internet and Intranet-based), telephone system (including voicemail), fax, mobile device (pager, cell phone, smartphone, PDA, tablet, etc.), software and hardware resources, Intranet, Internet, video conferencing (webinars and conference calls), closed-circuit television, radios, wireless devices or other handheld devices, photocopiers, or other resource that allows Authorized Persons access to the Internet and documents, files or other information contained within these resources.

“*Encryption*” means the conversion of data into an unreadable form without the use of a decryption key. Strong Encryption means Encryption that meets then current industry standard, relating to the strength of the commercially available or tested algorithm, not internally developed, with it being

understood that the level of such strength shall change during the course of the Agreement as algorithms become more complex and sophisticated.

“Hosting Services” means the collective term used for describing web hosting, infrastructure as a service, platform as a service, software as a service, collocation services, cloud servers, etc. provided by Company or used by Company to deliver services under the Agreement. Hosting Services are typically off premise, one-host to many users scenario, where the user pays for resources consumed or allotted.

“Information Security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

“Information Security Program” means the comprehensive collection of policies, standards, procedures, and controls used to deliver and assure Information Security across the Company.

“Payment Card Industry (“PCI”)Requirements” means the security standard for all entities involved in the payment card processing functions and the security-related functions involved in protecting cardholder data for the major debit, credit, prepaid, e-purse, ATM, and POS cards as defined by the Payment Card Industry Security Standards Council. Current versions of the standards may be obtained from <https://www.pcisecuritystandards.org/>.

“Personally Identifiable Information (“PII”) means one or more piece of SVM Information that:

- (i) identifies and/or distinguishes or can be used to trace an individual’s identify (including, but not limited to, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers, date and place of birth, social security number, or biometric records)
- (ii) can be used to authenticate an individual (including, without limitation, passwords, passcode, or PINs, biometric data, answers to security questions and other personal identifiers)
- (iii) can be linked to an individual, such as medical (i.e., HIPAA), financial (i.e., account numbers, PINs, security codes, service codes, credit report information), and employment information (including but not limited to benefits, hiring information, salary, performance reviews, employment terms, etc.)

Note: specific PII and/or certain combinations of pieces of information create Sensitive Personally Identifiable Information. Refer to definition below.

“Privacy Laws” means all federal, state, and local U.S. (and, which applicable foreign) laws, regulations, and/or rules relating to Personal Information and other data privacy and data protection, as they may be enacted, adopted or amended from time to time.

“Process” or *“Processing”* means a series of actions used to perform a purposeful output, including but not limited, to collecting, retaining, storing, transferring, using, compiling, destructing, operating, etc.

“Record” means any recorded or documented form of SVM Information in any medium. This includes information created or received in any form, including e-mails, paper documents, electronic documents, database or application information, call center recordings, and other electronic or photographic media.

“*Security Incident*” means the suspected access to SVM Information that is unauthorized and intended to or reasonably likely to compromise the security, confidentiality or integrity of SVM Information or the controls put in place to protect the security, confidentiality or integrity of SVM Information, including any suspicion of SVM Information being copied, transmitted, viewed, stolen, or used by an individual not authorized to do so.

“*Security Breach*” means any confirmed Security Incident or any Security Incident involving Restricted SVM Information.

“*Sensitive Personally Identifiable Information (“Sensitive PII”)*” means specific PII or combinations of PII that require additional security provisions as required by contractual agreement, Privacy Laws or as otherwise deemed necessary by SVM. This includes the following:

- (i) Use of an individual’s first and last name or first initial and last name, combined with any of the below:
 - a. financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account
 - b. an individual’s government-issued identification number (including social security number, driver’s license number or state-issued identified number)
- (ii) Use of an individual’s primary account number (PAN) alone, or as described in the definition for Cardholder Data.
- (iii) Biometric or health data.

“*Software*” means the programs and other operating information used by a computer, server, router, network device, or similar computing device.

“*SVM Data Classification*”: means the classification of SVM Information by SVM to ensure that appropriate security controls, labeling, and the granting of access are maintained. A data type or element may move from a lower classification to a more restrictive classification, or vice versa, when combined with other data types or elements. SVM maintains four (4) Data Classifications from least restrictive to most restrictive:

- (i) “*Public*”: is information that has been cleared by SVM’s management for general use and public knowledge.
- (ii) “*Internal*” or “*Internal SVM Information*”: is SVM Information that is proprietary to SVM, disclosure of which would result in unnecessary burden to SVM.
- (iii) “*Confidential*” or “*Confidential SVM Information*”: is critical SVM Information, disclosure of which would be detrimental to SVM.
- (iv) “*Restricted*” or “*Restricted SVM Information*”: is SVM information that is highly sensitive to the operation and organizational well-being of SVM.

“*SVM Information*”: means the collective information provided to Company by or at the direction of SVM, or to which access was provided to Company by or at the direction of SVM, in the course of services provided for performance under the Agreement, including but not limited to any PII, Sensitive

PII, Confidential Information, or any other data or information defined under the Agreement. SVM Information is, and will remain, the sole and exclusive property of SVM.

“SVM Network” means the system of computers, peripherals and other devices, that are interconnected to each other physically or logically, which enable SVM ECR and users of SVM ECR to perform job duties and/or services under this agreement. This includes all SVM owned or operated LANs, WANs, extranets, intranets, wireless, or any other network which SVM would consider used for SVM purposes.

“Vulnerability” means a weakness at the network services, operating system, or application level, or within associated functions of networks, computer systems, or Software that could allow a Security Incident to occur. Vulnerabilities also include physical vulnerabilities (such as broken locks, malfunctioning key or proximity cards) to the premises containing or permitting access to SVM Information.

2. Contact Information. For Security Incidents or inquiries, the following contact information for SVM and Company will be used:

SVM	E-Mail	security@servicemaster.com
	Telephone	(901) 833-7831

Company	E-Mail	
	Telephone	

Part Two: General Security and Privacy Requirements

3. Changes and/or Modifications to Security and Privacy Requirements. From time to time, it may be necessary to review and make changes to these Security and Privacy Requirements.

- 3.1 SVM will provide notice of such changes to the Company contact reference in Section 2 hereof. Upon such notice, Company will have 15 days to review and agree, or provide notice of non-acceptance and provide appropriate revisions.
- 3.2 Should Company provide revisions, SVM will review revisions and will work with Company for mutually agreed upon revisions to these Security and Privacy Requirements.
- 3.3 In the event Company and SVM cannot agree on the revised Security and Privacy Requirements, SVM may choose to: (i) continue to use the requirements herein, (ii) continue to use the requirements herein for all existing SOWs under this Agreement and not engage in future SOWs under the Agreement, or (iii) suspend all activities and services currently in operation under any SOW under the Agreement.

4. Information Security Program. Company shall, at all times during the terms of the Agreement (including normal operations, disaster recovery and business continuity), maintain effective and comprehensive Information Security that meets or exceeds then current industry standards, with respect to all SVM Information under Company’s protection (including all SVM information in Company’s possession or to which Company has access). Company shall implement, maintain, and

monitor a comprehensive written Information Security Program that includes reasonable administrative, technical, physical, organizational, and operational safeguards and other security measures, including policies and procedures, designed to (i) ensure the security and confidentiality of SVM Information, (ii) protect against any established or emerging threats to the Information Security of SVM Information under Company protection, and (iii) protect against unauthorized processing, destruction, loss, alteration, use of, disclosure, or access to SVM Information. Said Information Security Program shall be reviewed whenever there is a material change in practices and not less than annually. Company shall monitor its Information Security Program to ensure that it is operating in a manner reasonably calculated to ensure effective Information Security.

4.1 Information Security Program Requirements: At minimum, Company's Information Security Program shall incorporate policies and procedures consistent with then current industry standards for the following:

- Access Control (including the use of unique IDs and passwords for all users)
- Malware Prevention and Protection
- Patch and Vulnerability Management
- System Configuration and Hardening
- Logging of Security Events and Access to SVM Data
- Network Security and Firewall Management
- Security of Wireless Technology and Wireless Networks
- Application and Network Security Testing, as applicable

5. Personnel Security.

4.1 Background Checks. Company shall perform or cause to be performed background checks for all Authorized Persons with access to SVM Information.

4.2 Security Awareness Training. Company shall provide periodic and mandatory Information Security training for all Authorized Persons. Said training shall be designed to impart to each person an awareness of his or her responsibilities regarding Information Security, and associated Company Information Security Program.

6. Access to SVM Information. Company will ensure only Authorized Persons access SVM Information.

6.1 Removal of Access. Company shall ensure that all accounts are promptly disabled or removed (or provide notice to SVM to have account permissions revoked) following the removal of Authorized Persons from services provided under the Agreement for any reason, including but not limited to termination.

6.2 Physical Protections. As appropriate for SVM Data Classification or data type, as defined herein, Company shall appropriately secure SVM Information to prevent any physical access by unauthorized users.

7. Use of SVM Information.

7.1 Acceptable Use of SVM Information. Company will use SVM Information only for the benefit of SVM and only to the extent necessary to perform Company’s obligations under an executed SOW under the Agreement. Company may not take any actions that in any manner adversely affect the integrity, security or confidentiality of such SVM Information.

7.2 Expressly Prohibited Uses. Except as specifically permitted in a SOW or otherwise in writing, Company may not undertake any of the following actions with respect to SVM Information:

- Send out of the originating country to another country.
- Remove or copy from an SVM environment to a non-SVM environment, or otherwise initiate such extractions.
- Access any SVM production data or any SVM environments that are considered by SVM to be production environments.
- Access any SVM system that is considered by SVM to be in-scope for PCI Requirements.

8. Information Retention and Disposal. Upon written request from SVM, Company shall return or if authorized by SVM, discard, destroy and otherwise dispose of Records in a secure manner. Destruction methods shall ensure any paper or electronic storage media containing SVM Information is destroyed in such a way as to ensure the media cannot reasonably be reconstructed. Company shall provide SVM with a certification of destruction to the E-Mail address provided in 2. Contact Information.

9. Incident Response. Company will maintain a documented response process to manage and to take appropriate corrective action(s) for any Security Incident or Security Breach. This process must be reviewed by the Company for sufficiency at least annually. In the event of a Security Incident, Company shall use continuous efforts to correct the Security Incident until resolved and closed. In the event of a Security Breach, Company will ensure the following procedures are included in its Incident Response procedures.

9.1 Security Breach Notification and Communication: Company will promptly notify SVM of a Security Breach occurring that directly affects SVM Information or the systems that store, process, or transmit SVM Information based on the chart below.

Response	Classification		
	Internal	Confidential	Restricted
SVM Contact	Section 2.0	Section 2.0	Section 2.0
Notification	72 hours	48 hours	24 hours
Initial Notification Status Report	Within 48 hours	Within 24 hours	Within 8 hours
Update Communication	Mutually Agreed Upon	Mutually Agreed Upon	Mutually Agreed Upon
Report	Within 10 days of incident closure	Within 5 days of incident closure	Within 5 days of incident closure

- (a) Initial Notification Status Report. Within the above defined hours of the initial notification to SVM, Company shall provide SVM a written status report for each Security Breach. Each report will include, at a minimum, the following information:
- The date of occurrence
 - A brief description of the Security Incident, including known or suspected cause,
 - Contact information for the Company coordinator
 - Description of steps taken to date to contain or correct the Security Breach.
 - Next action steps to contain or correct the Security Breach.
 - Current status
 - Expected timeframe for full service restoration or resolution
- (b) Update Communications: After delivery of Initial Notification Status Report, Company shall provide SVM with interim written status reports for each Security Breach. Reports will be delivered at mutually agreed upon intervals. Reports will include, at a minimum, the same requirements from 7.1(a) plus:
- Third parties that are involved with Security Breach handling
- (c) Final Report. Company shall provide SVM, in writing, with a final written report for each Security Breach within the above defined business days of Security Breach closure. Such report shall include:
- Company's incident coordinator name and contact information
 - Date Security Breach occurred
 - Security Breach Executive Overview
 - Security Breach Details
 - How/when the Security Breach was detected and initially reported to SVM
 - Third parties that were involved with Security Breach handling
 - Description of what resources/services were impacted
 - Permanent corrective actions taken to prevent further occurrences.
- (d) Post Mortem Review. SVM reserves the right to schedule a review of the Final Report with Company.

9.2 Public Notification of Security Breach. Company shall not notify any third party of any Security Breach, except as may be strictly required by law, without first obtaining SVM's prior written consent and incorporating in good faith any feedback that SVM may have as to the content and manner of executing the third party notification.

9.3 Right to Security Assessment Following a Security Breach. Notwithstanding the SVM rights as set forth in Section 14, SVM shall have the right to have an independent third party perform a Security Assessment of reasonable and appropriate scope to validate that all necessary and timely remedial actions have been taken by Company following a Security Breach. Such Security Assessment shall be at Company's sole cost and expense; provided, however, that in the event that Company has engaged a third party to perform a similarly scoped Security Assessment prior to a request by SVM under this Section, Company will not be required to engage an additional

third party to provide a Security Assessment and the existing engagement will be deemed to comply with the requirements of this section.

10. Security Testing. Company will ensure its Information Security Program addresses application security testing as it relates to applications developed by Company and/or under the control or support by Company on behalf of SVM. Additionally, the Information Security Program will address network security testing as applicable to any systems under the control of Company in which Sensitive PII and/or Restricted SVM Information is stored, transmitted or processed. An executive report of tests will be provided to SVM annually. SVM reserves the right to request security testing requirements as it relates to Confidential SVM Information.

11. Encryption of Data. Company shall encrypt, at minimum, Sensitive PII, and Restricted SVM Information using Strong Encryption when transmitted over the internet or any other un-trusted network. Company shall also encrypt, using Strong Encryption, at minimum, Sensitive PII and/or Restricted SVM Information when stored on any system including but not limited to servers, workstations, mobile devices, backup tapes, removable media, or any other electronic storage medium. SVM reserves the right to request implementation of data encryption requirements as it relates to Confidential SVM Information.

12. Third Party Service Providers. Company must ensure that third party Authorized Persons must adhere to the terms and conditions hereof. Company shall ensure that agreements with third parties include appropriate safeguards to enforce these requirements.

13. Compliance with Privacy and Security Laws. Any SVM Information, specifically PII and Sensitive PII, used by the Company in the course of performing services under the Agreement will be used and protected in accordance with all applicable Privacy Laws. Company expressly warrants that its use of PII and/or Sensitive PII will comply with all applicable Privacy Laws. Company will at all times perform its obligations under the Agreement in such a manner as to not, by its actions, or inaction contrary to the Agreement, cause SVM to be in violation of applicable Privacy Laws and/or any other applicable laws.

14. Right to Audit. SVM reserves the right to cause a qualified, independent third party to conduct an annual security assessment or audit for verification of Company's compliance with the requirements hereof.

14.1 Assessment Details. Assessments will be conducted during Company's regular business hours with reasonable notice to Company. SVM will work in good faith with Company to avoid impact to Company systems that support the Company's other customers. All assessments will be subject to non-disclosure and confidentiality obligations hereof and the Agreement.

14.2 Assessment Findings and Remediation. SVM shall provide a written report summarizing the assessment results to the Company. Should deficiencies be noted, Company will correct any reported deficiencies within thirty (30) days, or as otherwise mutually agreed. If the Company fails to implement such corrections in the agreed upon timeframes, then SVM, at its option, may terminate any or all SOWs under the Agreement at no cost or penalty to SVM.

15. Periodic Attestation of Compliance with these Requirements. Promptly following receipt of a written request from SVM, Company will attest to the then current status of compliance with the requirements hereof.

16. Security on SVM Premises. – At all times the Company and Company’s Authorized Persons are on SVM premises, Company will comply with all applicable SVM policies and procedures of which Company has notice.

17. Acceptable Use of SVM ECR Systems.

17.1 At all times, Company and Company’s Authorized Persons will comply with all applicable SVM ECR policies and procedures of which Company has notice.

17.2 Company and Company’s Authorized Persons are responsible for managing, maintaining, and guarding the security of SVM ECR to which they have access or control, including the equipment that stores SVM Information. Users of ECR should have no expectation of privacy as SVM routinely monitors all communications activity made on ECR.

17.3 In safeguarding SVM ECR, Company and Company’s Authorized Persons will:

- Comply with SVM security policies and procedures for password utilization and maintenance.
- Log off ECR, or utilize password-protecting mechanisms to protect computer terminals when unattended.
- Safe guard User IDs and passwords and not share with others.
- Not install any software, or change the provided configuration, unless authorized and assisted by IT.
- Not leave mobile devices, including laptops, unattended or unprotected.
- Not allow others to use SVM ECR.
- Report lost/stolen SVM ECR immediately to the SVM Help Desk (866-597-4321) as well as to the contact information listed in Section 2.

17.4 Company and Company’s Authorized Persons in using SVM ECR will:

- Refrain from engaging (including access or transmissions of) in any activities that are soliciting, illegal, hostile, defamatory, gambling, or offensive, including suggestive, obscene, harassing, pornographic, off-color, racist, sexist, “hate”, or discriminatory towards others.
- Refrain from transmitting or accessing destructive programs (including malware) with intention to damage or place an excessive load on a computer system or network.
- Refrain from altering the configuration of any anti-malware software.
- Not use another Authorized Persons’ user ID and/or Password, or one of a SVM associate.
- Not circumvent any SVM security provision (firewalls, software, or other access controls) to access, transmit, or Process unauthorized SVM Information.
- Not grant access to SVM Information, SVM Network, or SVM ECR to any third-party computer system or other unauthorized party.
- Refrain from storing Confidential SVM Information, PII, Sensitive PII, Restricted SVM Information on external devices (including laptops, thumb drives, external hard drives, etc.).

- 17.5 Only SVM ECR, using direct or wireless connection, are permitted access to the SVM Network.
- 17.6 All SVM ECR must have the required information security suite of tools installed and function properly before access is granted.
- 17.7 Non-SVM electronic communication resources are prohibited from connecting to a SVM Network via direct or wireless connection, or storing SVM data. Company may be granted an exception, provided the scope of services provided under the Agreement aligns to a documented exception within the SVM Acceptable Use Policy.
- 17.8 Refrain from attaching non-SVM-owned wireless access points to the SVM Network and/or SVM ECR.

Part Three: Additional PCI Requirements

18. Payment Card Industry Security If Company stores, processes, or transmits Cardholder Data on behalf of SVM, provides security in protecting Cardholder Data, or affects the security or integrity of Cardholder Data under the Agreement, the following requirements will apply.

- 18.1 **Maintain PCI Compliance.** Company must continuously maintain compliance with Payment Card Industry Requirements as long as Company stores, processes, or transmits SVM Cardholder Data.
- 18.2 **Attestation of PCI Compliance.** Company must provide a current PCI attestation of compliance at time of signing any SOW under the Agreement involving Cardholder Data, and annually thereafter. Acceptable forms of attestation include either of the following:
- Company inclusion in the Visa Global List of PCI DSS Validated Service Providers
 - Providing a copy of Company's Attestation of Compliance and executive summary from either the Company's (a) PCI DSS Service Provider Report On Compliance ("ROC") or (b) PCI DSS Service Provider Self-Assessment Questionnaire ("SAQ"), whichever is applicable based on Company's PCI vendor level, as determined by the Card Organizations
- 18.3 **Security Breach of Cardholder Data.** Notwithstanding the requirements in Section 9, in the event that any Security Breach at Company is alleged or confirmed to involve Cardholder Data then Company shall cooperate with SVM and/or any Card Organization in investigating. Company will, upon request from SVM, and at Company's sole cost and expense, engage a forensic investigator approved by SVM no later than forty-eight (48) hours following Company's notice of the event to SVM to investigate the Security Breach. Company shall allow such forensic investigator to conduct promptly an examination of Company's systems, procedures and records, orally report and discuss the investigator's initial findings with SVM, and thereafter issue a written report of its findings to the Company and SVM. For avoidance of doubt, Company shall provide such access, information, and assistance as is necessary for the forensic investigator, SVM and/or Payment Card Brand Organizations to complete the investigation of the Security Incident. Company will provide to SVM all information related to Company's or any Card Organization's investigation related to any unauthorized use, access, or Processing of Cardholder Data including but not limited to forensic reports and systems audits.

Part Four: Software Development and Hosting Requirements

19. Software Development. If Company provides software development services for SVM, or provides Hosting Services using proprietary software written by or on behalf of Company, under the Agreement, then the following requirements apply:

- 19.1 Software Development Life Cycle (SDLC). Company shall have implemented a SDLC using industry acceptable development methodology. SDLC will include, at minimum, code reviews, change management, source code back up, code versioning, code testing for Vulnerabilities and other security flaws, defects testing, and documentation of activities. SDLC will also include regular post deployment of Software to ensure Vulnerabilities and defects are remediated.
- 19.2 Coding Standards. Company will develop Software using secure coding standards relevant to the development languages and technologies in use. Code developers will use code reviews, manual or automated, to ensure secure coding practices are validated and other security flaws and Vulnerabilities are removed.
- 19.3 Developer Training. Company will only use developers trained in secure development standards and practices relevant to development languages and technologies used to provide services under the Agreement. Notwithstanding the SVM rights as set forth in Section 14, SVM reserves the right to request validation of knowledge and training of developers as it relates to secure coding and development practices.

20. Hosting Services. If Company will be providing any Hosting Services for SVM under the Agreement then:

- 20.1 Security Certifications with Industry Standards. At least annually, Company shall conduct site audits of the information technology and information security controls for all facilities used in complying with its obligations under the Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices. Upon SVM's written request, Service Provider shall make available to SVM for review all of the following, as applicable: Company's Statement on Standards for Attestation Engagements (SSAE) No. 16 Type II audit report for Reporting on Controls at a Service Organization and any reports relating to its ISO/ICE 27001 certification. SVM shall treat such audit reports as Service Provider's Confidential Information under this Agreement.
- 20.2 Should the Hosting Service Provider be providing services that fall under PCI, requirements under Section 18 would also be applicable.