HP Standard 14-04 for Information Protection and Security for Suppliers/Partners

© Copyright 2019 HP Development Company, L.P.
This is an uncontrolled copy when in printed form.

TABLE OF CONTENTS

1. INTRODUCTION – 2
2. PURPOSE AND USE – 2
3. SECURITY NOTIFICATIONS – 2
4. DATA BREACH – 3
5. SUPPLIER EVALUATION AND OVERSIGHT – 3
6. PRODUCT AND SERVICE SECURITY REQUIREMENTS – 4
7. SUPPLIER THIRD PARTIES – 5
8. REPRESENTATION AND WARRANTIES – 6
9. LEGAL HOLD – 6
10. DEFINITIONS – 6

EXHIBIT A – 8
1. SYSTEM SECURITY – 8
2. PHYSICAL SECURITY – 9
3. MALICIOUS USE OF PRODUCT OR HARDWARE – 9
4. PASSWORDS – 10
5. NETWORK SECURITY – 11
6. PATCHING VULNERABILITIES – 11
7. CHANGE MANAGEMENT – 11
8. EVENT LOGGING – 12

EXHIBIT B – 13
1. SOFTWARE – 13
2. RECORDING CAPABILITIES – 13
3. NOTICE – 13
4. NOT RECORDING – 13
5. USE AND ACCESS – 13
6. STORAGE AND TRANSMISSION – 14
7. COPIES – 14
8. SCREENING QUESTIONS – 14
This Global INFORMATION PROTECTION AND SECURITY SCHEDULE (“IPSS”) forms part of the Agreement. Compliance with this Standard does not relieve or diminish Supplier’s obligation to comply with other HP contractual requirements nor its obligation to comply with all applicable laws. A SOW or SLA may not change any of the terms of this IPSS as the terms apply to other SOWs.

Capitalized terms not specifically defined herein shall have the meaning set forth in the Agreement. Where terms or conditions are in conflict, then the term or condition of the IPSS shall take precedence and control over any conflicting term in the Agreement. Other terms used in this Agreement are defined in the context in which they are used. Undefined terms, acronyms and phrases used in the information technology (“IT”) industry or other specific context shall be interpreted in accordance with their generally understood meaning in such context.

1. PURPOSE AND USE

1.1 Supplier shall adhere to the provisions of the IPSS where Supplier:

1.1.1 Processes Personal Data and/or HP Data (in the event that Supplier processes either, Supplier shall also adhere to the terms of the HP Data Processing Standard, found at: https://h20168.www2.hp.com/supplierhandbook/HX-00027-001.pdf;)

1.1.2 Develops, provides or creates software, application(s), website(s), device(s) or other tangible Product(s); or

1.1.3 Provides hosting of an application, website, or system, or where network connectivity to HP’s network occurs, or where Services are otherwise dependent on the integrity of Supplier’s environment;

1.2 Supplier will only access and use HP information systems in the manner and to the extent necessary to provide the Products or Services. Supplier shall not rent, transfer, distribute, disclose, copy, alter or remove HP Data unless authorized to do so in writing by HP. Supplier will ensure its provisioning of Products and Services complies with all Applicable Laws, including but not limited to obtaining or making any legally required notifications, filings, registrations, and permits.

2. SECURITY NOTIFICATIONS

2.1 Contacts. Supplier shall ensure that all notifications related to Security Breach or IPSS non-compliance, shall be made to HP Cybersecurity Security Operations Center via (a) email sent with read receipt to: SOC@hp.com and (b) telephone at: 1-(888) 843-6367.

2.2 Supplier shall ensure all Authorized Supplier Employee access is terminated immediately when such Authorized Supplier Employee no longer requires access to HP information systems or network connectivity.

2.3 Supplier will designate in writing a primary and an alternate information security program manager or team to act as Supplier’s security contacts. Supplier will provide each contact’s name where
relevant, title, email and phone number to the email address in section 2.1 prior to commencing services. Supplier will notify HP of any changes to the information as applicable during the engagement.

2.4 Supplier shall reasonably assist HP with any requests and/or notifications from third-parties (including regulatory authorities) and will perform all acts necessary to enable HP to comply with such requests. Supplier shall promptly notify HP of such requests or notifications where relevant to the Services or Products provided and shall not respond until prompted to do so in writing by HP.

3. SECURITY BREACH

3.1 Notification of Security Breach. In the event that Supplier experiences or becomes aware of (a) a Security Breach, or (b) a critical security vulnerability or zero day exploit in a released Product or Service or solution provided by Supplier, or used by Supplier in providing services to HP, Supplier shall use best efforts to provide HP with notification as set out in Section 2.1 as soon as possible, but in no event more than 12 hours after Supplier becomes aware of such Security Breach, or vulnerability or exploit.

3.1.1 In the event of a Security Breach and upon one calendar day prior written notice, HP reserves the right to review daily updates from the Security Breach investigations involving HP Data, including remediation activities and expected timelines for remediation.

3.2 In the event of a Security Breach, Supplier shall not make any public announcements or inform any external party without notifying HP in writing at least five business days prior, except as may be required by applicable laws.

3.3 Security Breaches which require Supplier to contact HP include but are not limited to: Distribution Denial of Service, Advanced Persistent Threat, Data Corruption, Data Leakage, Ransomware, or Money Fraud, where such incidents affect HP Data or where they threaten the continuity of Supplier’s network, Services or Products provided to HP under this Agreement.

4. SUPPLIER EVALUATION AND OVERSIGHT

4.1 At HP’s sole discretion, and before a Supplier begins to provide Services or Products under the Agreement or executes any Amendments to this IPSS, HP may conduct an Information Security Assessment ("ISA") to assess the Supplier’s security practices.

4.2 Prior to conducting an ISA, HP will: (1) confirm a Non-Disclosure Agreement is in place, (2) define the ISA scope, and (3) confirm details regarding the ISA. During the ISA, HP will not view or access records or processes not directly related to or supporting HP Data Processes, architecture, policies, Products, or Services provided by Supplier or Supplier Personnel to HP.

4.3 Supplier shall address any ISA findings in a remediation plan. Supplier shall provide a confidential copy of any remediation plan to HP and shall complete the plan within a commercially reasonable timeframe set forth therein.

4.4 If HP determines from the initial ISA that a more comprehensive assessment is required, HP will notify Supplier. Supplier shall confirm receipt of HP’s notification no more than ten calendar days after its receipt and shall then support HP’s reasonable requests related to the comprehensive assessment.
4.4.1 Supplier agrees to maintain systems and processes as needed in response to the most recent ISA throughout the term of the Agreement. Any ISA findings, obligations or remediation plans may be utilized by HP to amend the terms of this IPSS.

4.4.2 Control deficiencies and areas of non-compliance will be remediated using industry standard processes and tools within a reasonable period, the timeframe of remediation being subject to negotiation between HP and the Supplier. This includes, but should not be considered limited to, areas of concern identified by HP prior to the commencement of the Agreement.

4.5 At HP’s sole discretion, Supplier may, in lieu of an ISA, provide a controls audit report and remediation effort, such as SOC 2 Type 2 or other relevant information security audit performed within the past 12 months, where applicable to the Services or Products provided. The audit shall include an assessment of Supplier’s general controls and security processes to ensure compliance with applicable laws and the IPSS. The audit should be performed at Supplier’s expense.

4.6 At HP’s request and on reasonable notice, no more than once per calendar year except in the event of a Security Incident (in which case the date of the last audit shall not prevent HP from requesting an additional single audit specific to such Security Breach to ensure that the cause of such Security Breach has been remediated), Supplier shall permit HP or its designee to audit Supplier’s relevant security practices or processes in person to determine Supplier’s compliance with its obligations under the IPSS, the Agreement and all Applicable Laws, regulations, directives, ordinances, and relevant industry standards. Should HP request an audit, Supplier shall permit HP or its designee to enter onto Supplier’s premises during normal business hours at a date and time mutually agreeable to the Supplier and HP, to the extent required for such purposes. HP reserves the right to have such audits performed by an independent third party on HP’s behalf. HP shall not utilize an independent party that is a competitor of Supplier to perform the audit. Audit activities shall be planned and agreed upon in advance by stakeholders. The results of such audit, in so far as they are relevant to the Products or Services will be shared with HP. The audit shall be conducted in such a manner that it will not jeopardize or expose the Supplier’s other customers’ data. HP or a third party on HP’s behalf may, during an audit, inspect Supplier’s facilities and view copies or extracts of Supplier’s records and processes resulting from Supplier’s fulfillment of the requirements of this Agreement. Any Audit findings will be set out in a mutually agreed upon remediation plan. Supplier shall comply with and complete the remediation plan within a mutually agreeable timeframe set out therein.

5. PRODUCT AND SERVICE SECURITY REQUIREMENTS

5.1 Where applicable to the Services or Products provided, Supplier shall implement industry-standard or higher protocols pertaining to asset management, access control, awareness and training, 256-bit encryption, and any other safeguards applicable to the Services or Products provided. For clarity, “industry standard” here refers to NIST Cybersecurity Framework, SSAE 18, or industry equivalent. Where Supplier provides Hardware to HP, Supplier shall also adhere to the Security Standard for Product Security at https://h20168.www2.hp.com/supplierhandbookrestricted/HX-00014-03.pdf

5.2 Supplier shall provide training for employees at time of hire and repeatedly on an annual basis. Training shall cover cybersecurity and privacy requirements, as applicable to the employee role and Services or Products provided to HP.
5.3 Where Supplier is providing software, Supplier shall meet or exceed security industry best practices (for example, Security by Design) throughout the software development lifecycle for software developed for HP, incorporated into an HP Product or Service, resold as an HP product, or used by HP for its internal business purposes. In the event of a Security Breach, Supplier shall obtain and provide to HP a copy of source code scanning results (e.g. Black Duck, OWASP, SANS, etc.) and associated remediation efforts.

5.4 Where Supplier is hosting or providing an online Product or Service, Supplier shall address any vulnerability findings in a remediation plan. Supplier shall provide a confidential copy of any remediation plans to HP upon request. Supplier shall implement remediation for any known or identified vulnerabilities with a Common Vulnerability Scoring System (CVSS) rating of 4 or higher which impact the confidentiality, integrity, or availability of the Product, Service or HP Data. Such remediation shall be completed prior to commencement of Services or within 3 days after the release of the patch or remediation where the risk is rated 9 or higher, 14 days where rated 7 or higher, 30 days where rated 4 or higher. For websites not branded as an HP website, Supplier shall clearly and conspicuously communicate to users that they are not on an HP site, and clearly communicate Supplier’s privacy policy to the users. Where the website is exclusive to Services provided under this Agreement, Supplier shall post any informational language reasonably required by HP.

5.5 If Supplier is interacting with, accessing, using or processing Payment Card Data in relation to Products or Services, Supplier shall do so in compliance with the terms of Exhibit C, attached to this Agreement.

5.6 If Supplier is utilizing a remote network connect, a connectivity method into HP information systems, or is located within an HP facility, Supplier must use an HP-approved Information Technology standard remote access solution. Duration of access shall be restricted to periods where access is necessary for provision of Services.

5.7 Supplier shall create and maintain a fully implemented access control policy and process to prevent against unauthorized access to HP’s Network or HP Data, or any network or data necessary for the provision of Services under this Agreement. Supplier shall use industry-standard or better practices to protect against compromise or damage to HP’s network.

5.8 Supplier shall not store HP Data on any Portable Computing Device including, but not limited to, cell phones, Smartphones, laptops, unless HP Data stored on such Portable Computing Devices is Encrypted. Supplier shall not store HP Data on any Removable Media, such as compact disc, flash drive, tape (each a “Removable Media”) stored on such Removable Media is Encrypted.

5.9 When leveraging a shared hardware environment, implement information protection measures throughout the information lifecycle to ensure that one customer’s information is never accessible to another customer sharing that same hardware.

5.10 Supplier shall physically secure facilities by card key access, biometric scans or video surveillance where appropriate.

5.11 Supplier shall apply a clean desk policy to facilities and conduct regular visual exceptions to ensure personnel compliance.
5.12 Supplier shall maintain a disaster recovery/business continuity plan for restoring critical business functions and operations. Upon request, Supplier shall allow HP to review executive summaries of disaster recovery/business continuity plans.

6. **SUPPLIER THIRD PARTIES**

6.1 Supplier shall ensure that Supplier’s subcontractors, agents, and third parties provide Services and Products under substantially similar security obligations as those imposed on Supplier under this IPSS. Such terms, as relevant to their engagement, shall be in a written contract between Supplier and Supplier’s third-parties.

6.2 Supplier shall take reasonable, ongoing steps to ensure that such subcontractors, agents, and third parties comply with their obligations throughout the duration of the engagement. Supplier shall assess or audit its third parties once per year, and more frequently in the event of a Security Breach or other security incident involving Services or Products. Supplier shall be responsible for the acts and omissions of its subcontractors with regard to Services or Products provided to HP.

7. **REPRESENTATION AND WARRANTIES**

7.1 Supplier warrants and undertakes that has in place and shall maintain appropriate industry standard physical, organizational, and technical processes and procedures to protect against any Security Breach.

7.2 Supplier represents and warrants that it is not and has not been subject to any investigation or legal action related to Supplier’s relevant information security practices that have not been shared with HP prior to commencement of Products or Services.

8. **LEGAL HOLD**

Supplier shall not block, erase or dispose of any HP Data at any time which Supplier has been notified it must retain in response to a Legal Hold. In the event that Supplier believes it is legally required to destroy HP Data on Legal Hold, Supplier must notify, consult and cooperate with HP prior to any destruction. Supplier obligations to retain such HP Data on Legal Hold shall not be limited by any agreed-to records or data retention policies or internal policies of Supplier. If Supplier cannot retain the HP Data on Legal Hold, Supplier shall provide the HP Data to HP for HP to retain.

9. **DEFINITIONS**

9.1 **Advanced Persistent Threat**: a set of stealthy and continuous computer hacking processes to monitor or extract data from a specific target related to the Service.

9.2 **Applicable Laws** means any law, statute, ordinance, regulation, order, rule or decision of any Governmental Authority that is applicable to the subject matter and region in which Services or Products are being provided, utilized, or otherwise provisioned under the Agreement.

9.3 **Authorized Supplier Employees** means Supplier’s employees who are approved by HP to authenticate and access HP information systems or network connectivity.

9.4 **Data Corruption** means the intentional introduction of unauthorized changes to HP Data.
9.5 Data Leakage means the unauthorized transmission of HP data from within an organization to an external destination or recipient.

9.6 Distribution Denial of Service or “DDOS” means an attack that makes a contracted service unavailable to its users, where the attack source is more than one unique IP address.

9.7 Encrypted or Encryption means the process by which HP Data is converted into private code to ensure secure transmission or storage and a method approved by HP.

9.8 HP Data means HP’s Confidential Information, HP’s customer information, HP’s Personal Data, and other non-public HP data provided to, collected by, viewed, or accessed by Supplier in connection with the products, services or solutions provided by Supplier. HP Data includes data-classification terms related to HP data contained within any Agreement to which this IPSS is included by reference.

9.9 Money Fraud means the illicit use of HP’s or its service provider’s IT systems for deliberate deception to secure unfair or unlawful gains. Money fraud includes cybercrimes such as (large-scale) electronic identity theft or unlawful intrusion into a network.

9.10 Personal Data means any information relating to an identified or identifiable individual or as otherwise defined by applicable Data Protection and Privacy Laws; this includes data generated by the online tracking of users or consumers where it can be used to identify an individual.

9.11 Data Protection and Privacy Laws means all current and future applicable laws and regulations relating to the processing, of security, protection, and retention of Personal Data and privacy that may exist in the relevant jurisdictions.

9.12 Process(es), Processing or Processed means any operation or set of operations which is performed upon Personal Data whether or not by automatic means, including, without limitation, accessing, collecting, recording, organizing, structuring, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning, combining, blocking, restricting, erasing and destroying Personal Data and any equivalent definitions in applicable Data Protection and Privacy Laws to the extent that such definitions should exceed this definition.

9.13 Product means any materials or products, including hardware or software or solutions and/or third-party components, websites, and Supplier-controlled components on HP websites provided to HP pursuant to the Agreement.

9.14 Ransomware means form of malware that holds a user’s computer, system, or data hostage until a “ransom” fee is paid.

9.15 Recording Notice means a notice to the party being recorded that Supplier is recording the conversation.

9.16 Security Breach means an actual or reasonably suspected breach (gap in defense) of security leading to the accidental or unlawful destruction, loss, theft, exfiltration, alteration, unauthorized disclosure of, or access to HP Data, product(s), service(s), network(s), or solution(s).

9.17 Service means any services provided to HP or HP’s customers pursuant to the Agreement.
Exhibit A: Supplier Security Standards

System Security:

1. Use administrator accounts only for the purpose of performing administrative activities, where such activities cannot be performed by an account with lesser-privileges.

2. Be able to trace each account (including those with administrative privileges) to a uniquely-identifiable individual.

3. Batch system administration activities, such as daemons, jobs, and scripts, should not be run with administrative privileges unless no alternative exists.

4. Authenticate all access to information systems, including console access, individual accounts, administrative accounts, and any automated relationships with other systems.

5. An individual account should not have access to both development and test environments as well as production environments.

6. Only enable required services and protocols; explicitly disable all others.

7. Identify, track, label and manage all information systems or mobile device assets in accordance with their data sensitivity classification.

8. Disable all unnecessary default system accounts and built-in application accounts wherever possible.

9. No less than annually, review all accounts to determine if they are still required. Disable accounts upon user termination or user change of roles and responsibilities.

10. Securely erase all media electronically by overwriting or degaussing, through cryptographic erasure, or else physically destroyed prior to disposal or reassignment of the system.

11. Media sanitization procedures such as NIST SP 800-88 (Guidelines for Media Sanitization) or equivalent should be followed. The NIST SP 800-88 Revision 1 guidelines may be found at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.
12. Hardcopy materials containing HP Data should be processed, transferred and stored in a secure manner. Hardcopy materials should be destroyed when no longer needed for business or legal purposes in a manner which ensures that HP Data cannot be reconstructed.

13. All hardcopy disposal containers should be secured with tamper proof locks.

14. All information systems should have up-to-date versions of system security agent software which should include host firewall, malware protection and up-to-date patches and virus definitions.

15. Security software should be configured to scan for and promptly remove or fix identified findings on endpoint systems.

16. Any information system or product should have current anti-virus software configured for automatic updates no less than once per week. Such software should be configured to scan for and promptly remove viruses.

**Physical Security:**

1. This section applies where a Supplier has physical control over areas where HP-owned equipment is stored, where information systems are used in processing HP Data, or where services or products are being provided or manufactured.

2. Restrict access to authorized persons only.

3. Utilize identification and authentication controls to authorize and validate the access.

4. Securely maintain an audit trail of all access, including times of entry and departure.

5. Grant visitor access only for specific authorized purposes.

6. Ensure that all visitors are escorted and supervised at all times.

7. Issue instructions to visitors on security and emergency procedures.

8. Access to areas where HP Data is processed, services are provided, or products are developed or stored, should have physical separation, such as cages or secured doors, and should be controlled and restricted to authorized persons only.

9. Do not capture keyboard or console actions and information via video camera surveillance.
Malicious Use of Product:

1. Restrict diagnostic tools to personnel whose job function requires usage and limit such usage to relevant information systems.

2. Do not use tools that may impact the performance of the services provided pursuant to the Agreement through degradation of availability or performance.

3. Properly protect HP Data gathered as a result of sniffing any network traffic by any means against unauthorized disclosure, alteration, and destruction.

4. Only store such HP Data when absolutely necessary, and immediately and securely dispose of the HP Data when no longer needed.

5. Where Sensitive Data is processed on-premises, Supplier personnel may not utilize portable storage devices with the systems used to process Sensitive Data.

Passwords:

1. Protect passwords at all times, including one-way encryption or salted hash in storage and encrypted during transmission.

2. Require initial passwords be changed by the user on first use.

3. Do not use manufacturer-provided default passwords.

4. Change passwords promptly they are suspected of being compromised or known to have been disclosed to unauthorized parties.

5. Provide a method for users to change their own passwords.

6. Passwords should be uniquely identifiable, and each user must be accountable and responsible for any action taken under that user’s ID and password.

7. Users should not share or divulge their password to anyone.

8. Where HP Data is processed, require the use of multifactor authentication.

9. Mask, suppress, or otherwise obscure the display and printing of passwords such that unauthorized parties will not be able to observe or subsequently recover them.

10. Do not log or capture passwords as they are being entered.

11. Restrict size of email transmissions wherever possible; monitor all emails and set size of emails to 1 mb or smaller, with all emails exceeding that size automatically blocked.

12. Verify requestor’s identity for any password changes and ensure password change processes do not circumvent password security controls.

13. Do not hard code passwords and usernames in clear text into shell scripts, or embedded in error messages, dial-in communications programs, browsers, or any executable program or file.
14. Passwords complexity should at least three out of four-character classes (upper case letters, lower case letters, numeric digits or special characters) or equally-secure alternative methods.

15. Password length should be configured to be at least twelve characters.

16. Prevent the reuse of at least the last six passwords.

17. Lockout accounts on not more than six consecutive failed login attempts.

18. Set an expiration for passwords no longer than every 90 days.

Network Security:

1. Maintain an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other security risks to HP Data.

2. Implement any changes required to maintain the security of the HP Data and information system in an expedited manner.

3. Capture actual and suspected access exceptions from the intrusion detection system data for audit purposes and make such data available to HP upon request.

4. Networks used in the provisioning of services for HP should have dedicated, separately-defined logical domains or network compartments, each protected with suitable security perimeters and access control mechanisms.

5. Services for HP should be completely segregated from other customers in multi-tenant environment as well as from “test” or other non-production networks.

6. Where applicable to Services provided, conduct regular and recurring penetration testing.

7. Continuously harden systems by removing or terminating any nonessential programs or services on Supplier systems.

Patching Vulnerabilities:

1. Maintain security products on a supported version, no more than one version behind, including implementing any security-related updates made available by security product vendors.

2. Monitor and implement any necessary changes to enhance the security status of the product, service or solution.

3. Review and assess the risk and threat to the environment of all vendor security directives and advisories in a timely and effective manner.

4. Implement patches in a timeframe commensurate with the risk level.

5. Implement remediation for any known or identified vulnerabilities with a Common Vulnerability Scoring System (CVSS) rating of 4 or higher which impact the confidentiality, integrity, or availability of the product, service or HP Data prior to commencement of services or within 14 days from release of the patch or remediation.
6. Remediation for vulnerabilities with a rating less than 4 should be implemented within 30 days.

**Change Management:**

1. Perform sufficient analysis and testing prior to an implementation which may affect the availability of products, services or solutions in use by HP.

2. Ensure changes have been documented, communicated appropriately and include the process to roll-back changes if necessary.

**Event Logging:**

1. Institute processes and programs to log, detect, retain, report, and resolve any system or security events which may compromise the security of the system.

2. Capture sufficient log information to recreate events and activities in support of forensic activities.

3. Devices and systems requiring security event logging.

4. When used as part of the security controls in support of the product, service or solution provided to HP, capture auditable logs of security events for Network, domain, application and services infrastructure.

5. Upon request by HP, make available the processes and procedures for automated or manual reviews, monitoring, and alerting of security-significant events.
Exhibit B - Call Centers Data Security Standards

If Supplier is Processing Call Recording Data on behalf of HP, then Exhibit 2 shall apply to Supplier

1. Software Requirements for Collecting Call Recording Data
   a. Software used for Processing Call Recording Data must provide individual, authenticated accounts with an access audit trail.
   b. Software used for Processing Call Recording Data must have the Capability to turn recordings on or off

2. Enablement of Supplier’s Call Recording Capabilities
   a. Supplier shall not enable, activate, nor make operational any call recording capabilities for Data collected and processed on behalf of HP unless (1) requested by and (2) approved by HP in writing.
   b. The percentage of Call Recording Data recorded by Supplier must comply with the percentage allowed in writing by HP. Specific permission must be obtained for 100% recording.
   c. If Supplier intends to use Call Recording Data for Supplier’s internal training purposes, Supplier shall use technical mechanisms to redact all Personal Data and Sensitive Data from Call Recording Data.

3. Notice of Recording
   a. Prior to recording Data, Supplier shall notify a party that Supplier is about to record the conversation ("Recording Notice").
   b. Recording Notice shall comply with Applicable Laws.
   c. Recording Notice must include the clear and specific purpose of the recording such as for quality monitoring, workforce management, agent and customer service representative training, evaluation and verification, dispute resolution or accurate incident reconstruction.
   d. Recording Notice is required for both inbound calls received by and outbound calls made by Supplier.

4. Option Not to Record: Supplier’s processes shall include the ability not to record inbound calls if so requested by the initiator of the call while still providing the requested service(s) to HP.

5. Use of and Access to Call Recording Data
   a. Use of the Call Recording Data must be Consistent with the Notice of Recording Given
   b. Call Recording Data must be accessed only by authorized users
   c. Call Recording Data must not be shared through email or stored using other electronic distribution methods such as file shares unless otherwise authorized in writing by HP.

6. Storage and Transmission of Call Recording Data
a. Filed or electronically stored Call Recording Data must be protected in accordance with this Agreement and the Law

b. Sensitive Call Recording Data must be encrypted in storage and in transit

7. Copies of Call Recording Data

a. Supplier shall have HP’s written authorization prior to making any copy, archival copy, or reproduction of Call Recording Data Processed on behalf of HP.

b. Copies, archival copies and reproductions of Call Recording Data are subject to the same access control and Data protection requirements as the original Call Recording Data.

8. Customer Screening Questions

a. Ensure that customers calling call centers respond correctly to security questions by the agent. The agent shall screen customer calls by requesting information that only an authorized customer would possess the ability to answer. Account information should only be provided to customers who successfully pass through all the Q&A security protocols.

b. Customer screening questions should prompt responses that are unique and specific to the customer and that are strong enough to enforce the protection of their data in Supplier’s control.

9. Call Recording Data Retention

a. Call Recording Data must be promptly deleted after Supplier satisfies the specific purpose stated in the Recording Notice, which must in no case be longer than sixty (60) calendar days after the original recording was made unless otherwise authorized by HP in writing.

b. Supplier shall comply with Applicable Laws when Processing Call Recording Data on behalf of HP including, but not limited to, Applicable Laws concerning Recording Notice, consent, and transfer of Call Recording Data outside country borders.
Exhibit C – Payment Card Processing Security

Where Supplier processes or will be Processing payment card information on behalf of HP and/or the cardholder, then Supplier shall adhere to the terms of this Exhibit.

A. Supplier represents and warrants that Supplier is and will remain fully compliant with the Payment Card Industry Data Security Standards ("PCI DSS") and any other applicable payment card data security standards, as may be updated during the term of this Agreement.

B. No less than annually, Supplier shall provide (i) a copy of the executive summary from its current Report on Compliance ("RoC"); or (ii) an Attestation of Compliance ("AoC"), which includes a description of the scope and services assessed, signed by a certified QSA under the standards set by the Payment Card Industry Security Standards Council (PCI SSC). Upon HP’s written request, Supplier will share with HP its PCI Scan Certificates for the quarterly network scans of Supplier’s network.

C. Where Supplier becomes aware of non-compliance with the Payment Card Industry Data Security Standard ("PCI DSS") related to HP Data or any third-party claim regarding PCI DSS non-compliance against Supplier, Supplier shall notify HP immediately. Where Supplier does not pursue resolution of a claim or provide HP with reasonable assurances that it will pursue resolution, then HP may defend the Claim(s) at Supplier’s expense without in any way limiting HP’s other rights and remedies.

D. Supplier warrants that Supplier shall use (i) an Approved Scanning Vendor (ASV) to perform quarterly network scans (of their network) and (ii) a Qualified Security Assessor (QSA) to perform the annual onsite PCI Data Security Assessment.

E. Supplier warrants that upon completion of the Services under any statement of work or at the termination of this Agreement, Supplier will promptly remove all PCI Data from Supplier’s systems in accordance with the required process under PCI DSS or other applicable standard no later than the earlier of seventy-two (72) hours from cessation of the services or any required time period under the relevant PCI standard.
# 8. Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Brief Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, 25-February 2016</td>
<td>Initial release of document</td>
</tr>
<tr>
<td>B, 18-April 2016</td>
<td>Corrected numbering in section 5; updated section 3.3 to clarify the position; section 9.2.4 removed trailing parenthesis; Capitalized beginning of second sentence in 4.3 (addendum; spelling correction in 6.1.</td>
</tr>
<tr>
<td>C, 02-November 2016</td>
<td>Changed Contact information to include updated Contact on Section 5 Security Notification. Changed language on 8.2 to clarify correct assessment process.</td>
</tr>
<tr>
<td>D, 1-October 2017</td>
<td>Updated terms to clarify scope of applicability (Section 2), remove redundant terms covered in the Privacy Template (throughout), updated Subcontractor language to align with FTC guidance (section 6), and align warranties language with the approved language for SW IPSS templates (section 7)</td>
</tr>
<tr>
<td>E, 1-April, 2019</td>
<td>Incorporated engagement-specific cyber addenda (Addenda B, C, and D); updated contact phone number; added inco by ref for product security and data privacy policies; review of changes by Legal, Cyber, and Privacy</td>
</tr>
</tbody>
</table>