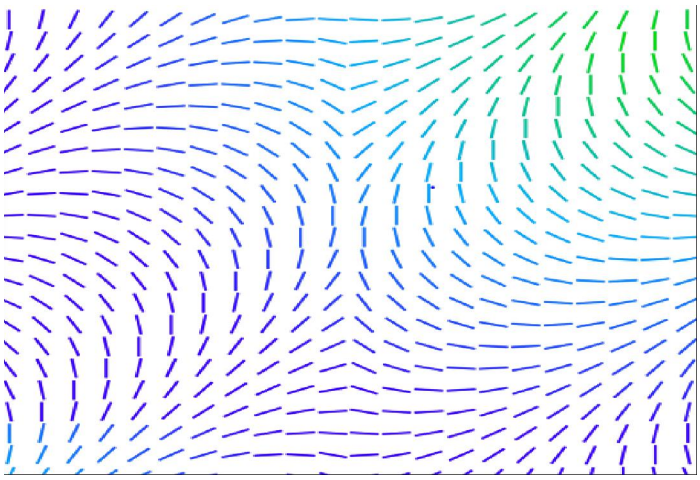
Trellix



# Supplier Security Requirements and Expectations (**SSRE**):

## For Confidential Data

## 1. INTRODUCTION

These Supplier Security and Privacy Requirements ("**SSPRs**") establish Supplier's minimum-security standards for protection of Trellix (the "Company," "We," "Us," or "Our") Confidential Information, including Personal Data.

To achieve security compliance, Suppliers and their subcontractors are wholly responsible for implementing all the security controls defined herein to protect the data they manage, host or process for any function or activity implemented on behalf of Us. This SSRE is not intended to be an all-inclusive list of security requirements. Each solution may generate unique or specific requirements that must be addressed with the appropriate security controls and defined in the applicable statement of work executed by the parties. This SSRE should be reviewed by the Supplier's Chief Information Officer (CIO) or Security Officer responsible for contracted services. It is the responsibility of the primary Supplier to review the SSRE with its subsidiaries and subcontractors responsible for service delivery to Us or on Our behalf and to ensure subcontractor's compliance herewith. The Supplier is responsible for conformance to the SSRE when services are performed by itself, its subsidiaries, or its subcontractors. This version of the SSRE covers data classified up to Confidential. The Company business owner is responsible for classifying the data of their web application and communicating it to the Supplier. At a minimum, Suppliers must be capable of implementing security controls required to protect data classified as Confidential.

Supplier must ensure their subsidiaries and subcontractors are compliant with all regulatory and local governing laws as well as Data Protection Laws for the services under contract with Us. Examples include, but are not limited to, GDPR, CCPA and CAN-SPAN Act compliance. Suppliersare responsible for compliance with any laws and regulatory requirements applicable to their use of the system.

## 2. GENERAL UNDERTAKINGS

Suppliers shall review all security controls cited in this document and may request clarification where needed. Suppliers shall notify the appropriate Company business owner of full compliance in writing authorized by a company official. Existing Suppliers that complied with a previous version of the SSRE must review and adhere to instructions in this document as We may have included important updates/changes from previous versions. If a Supplier, their subsidiaries, or subcontractors are not fully compliant to all minimum-security requirements, the Supplier shall provide in writing the extent of non-compliance and give committed plan of action detailing when the requirements will be fully met. The Company Information Security team shall evaluate a Supplier's security capability. If approved by Us, the Supplier plans will be documented in the contract. During a contract review, a Supplier's performance of the SSRE security requirements, the completion of non-compliant security controls plus the Supplier's track record for prompt remediation of vulnerabilities will be evaluated.

Suppliers shall agree to fully comply with the Company Code of Conduct, as set forth at the Supplier Ethics Expectations portal and the Electronic Industries Code of Conduct. Additionally, while performing services in Our owned or operated facilities, Suppliers shall agree to abide by all Company Corporate and Security Policies while performing such services including,but not limited to, safety, health and hazardous material management rules, and rules prohibiting misconduct on Buyer's premises including, but not limited to, use of physical aggression against persons or property, harassment, and theft. Suppliers will perform only those services identified in a duly executed statement of work and will work only in areas designated for such services. Suppliers shall take all reasonable precautions to ensure safe working procedures and conditions for performance on Our premises and shall keep Our site neat and free from debris.

Supplier agrees to implement data protection by design and by default and appropriate technical and

organizational measures to ensure a level of security appropriate to the risk.

Considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk ofvarying likelihood and severity for the rights and freedoms of natural persons, Supplier implements the following measures:

- the pseudonymization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing, and evaluating the effective of technical and organizational measures for ensuring the securityof the processing.

Supplier acknowledges that Personal Data retention and replication should always be assessed against business need and minimized, either by not collecting unnecessary data or by deleting data as soon as the need for it has passed and that holding any Personal Data presents security risks.

## 3. CLOUD SERVICES AND SYSTEMS

Cloud-based systems may only contain Confidential Information subject to the prior written approval of Us and must be certified to ISO 27001 standards as a minimum. We reserve the right to perform a security review and risk assessment of applications and services containing Confidential Information in the cloud prior to implementation. Any changes to the architecture or function of a service or data model in the cloud that stores Confidential Information must first be reviewed and approved by the Company Information Security Department. Applications that require physical separation cannot be on a cloud-based service unless duly segregated and approved in writing by Us. Supplier shall ensure Confidential Information is fully segregated from Supplier's other customers and/or third parties. In addition, Supplier agrees to allow any regulated End-User Customers (i.e., when a government or regulatory body with binding authority ("**Regulator**") regulates such entity's regulated services such as (*for example - financial services*) or any independent or impartial inspection agents or auditors selected by Us or a regulated End-User Customer, to audit Supplier and Supplier agrees to allow Us to provide any such reports to its End-User Customers where required.

## 4. VULNERABILITY MANAGEMENT

If Supplier is hosting a public-facing Company website, Supplier shall perform daily vulnerability scans on all internet facing web sites where We have branded content. We are the primary site owner when 'Trellix' is part of the URL. We use the Secure vulnerability scanning solution. Vulnerabilities will be reported to the Supplier for remediation. Supplier can request information for vulnerability reports, demonstration of the vulnerabilities (*when available*) and remediation support. We will not charge Supplier for the Company Secure scanning service. We require daily access to the reports. Upon identification of security vulnerabilities in a production application, Supplier must remediate within the minimal following timelines: (i) Urgent or Critical, Company threat rating [5] or [4] must be remediated in 1 to 5 calendar days; (ii) High, Company threat rating [3] must be remediated within 10 calendar days and (iii) Medium, Company threat rating [2] must be remediated within 30 calendar days.

If the security vulnerabilities identified by the Company vulnerability scanning process have not been addressed in the above timelines, We may shut down the web site until the vulnerabilities are remediated. Returning the site to production status requires the site to pass a scan for Our compliance. We consider a web site compliant when Our security standards are met. We will notify Suppliers any time the security

standards not met.

## 5. ORGANIZATIONAL MEASURES

The implementation and operational effectiveness of all below controls are mandatory. The below organizational measures are derived from Company Third-Party Information Security Risk requirements, which align to leading industry standards. ***Unless Supplier informs Us and requires specific modifications to the below, the following Organizational Measures will be deemed agreed upon by the Supplier***.

| Control Title | Control Description | Reference to Industry Standard | Implemented? (Yes/No) |
|---|---|---|---|
| **Organizational Measures**<br>▪ Supplier has a specific resource assigned that is accountable for security management.<br>▪ All systems have malware management which includes up to date signature files running on all production systems.<br>If administration of any systems or applications is performed outside the Suppliers secured intranet, it must be done through asecure channel (**VPN** or **SSL**) | | | |
| **Governance Personnel** | Supplier has appointed designated governance staff on the topic of Information Security and Data Privacy to ensure compliance with industry requirements (e.g., Data Protection Officer, Information Security Officer) | ISO 27701 6.3.1.1 | Yes |
| **Industry Standards** | Supplier follows industry standards and laws, regulations, and applicable guidelines. Supplier is certified against (*at a minimum*) the ISO 27001 standard and has a periodic cycle of internal andexternal audits to ensure the continued compliance of all applicable security controls. Supplier shall submit a copy of any industry standard accreditation applicable to the products or services it is providing to Us (e.g., ISO27001, PCI-DSS or SSAE16/18-SOC 2 audits performed by an independent auditorwithin the last year) and provide annual updates of the accreditation during the term of the Agreement. Supplier shall also inform Us of its adherence to data protection certification. | ISO 27001 A.12.7.1 | Yes |
| **Privacy & Protectionof Personal Data** | Supplier takes measures to ensure protection of Personal Data as required with relevant legislation such as the GDPR.<br>At a minimum, Supplier encrypts data at rest and in transit as required by law, regulation, and applicable guidelines. | ISO 27001 A.18.1.4 | Yes |

| Control Title | Control Description | Reference to Industry Standard | Implemented? (Yes/No) |
|---|---|---|---|
| **Information Security Policies** | Information security policies are implemented within the Supplier and available to all employees. Such policies are reviewed at planned intervals by appropriate personnel toensure their continued effectives to the organization | ISO 27001 A.5.1.1<br>ISO 27001 A.5.1.2 | Yes |
| **Segregation of Duties** | Conflicting duties shall not be granted to an employee, e.g.,roles/permissions in an IT application. In addition, IT environments should be segregated where appropriate (development vs test environment etc.) | ISO 27001 A.6.1.2<br>ISO 27001 A.12.1.4 | Yes |
| **Information Security & Privacy Awareness**<br>▪ Supplier personnel must be trained in Supplier security policies and be required to know changes or updates to these policies.<br>▪ Security training, including new threats and vulnerabilities, is required for all developers and system administration staff.<br>▪ All personnel with access to confidential data will have information security training for their respective roles.<br>▪ All personnel receive regular updates to their training for their respective roles.<br>▪ All personnel with access to Personal Data will complete a privacy training class and be knowledgeable and of any specific privacy requirements for the data being handled. This training will be provided by the Supplier or by accessing https://www.trellix.com/en-us/about/legal.html.<br>▪ Refresh training is required annually.<br>▪ All development staff should be trained on secure coding principles and best practices. Training materials are updated on an ongoing basis to include new threats and vulnerabilities. | | | |
| **Employee Screening** | Supplier has appointed designated governance staff on the topic of Information Security and Data Privacy to ensure compliance with industry requirements (e.g., Data Protection Officer, Information Security Officer) | ISO 27001 A.7.1.1 | Yes |
| **Contractual Obligations** | Contracts with both employees and contractors shall state employee obligations for information security and data privacyboth during and after termination of employment | ISO 27001 A.7.1.2<br>ISO 27001 A.7.3.1 | Yes |
| **Information Security & Privacy Training** | All employees shall receive appropriate education on the topicsof information security and data privacy, and remain informed on updates to organizational policies such as the Information Security Policy | ISO 27001 A.7.2.2 | Yes |

| Control Title | Control Description | Reference to Industry Standard | Implemented? (Yes/No) |
|---|---|---|---|
| **IT Asset Management**<br>▪ All data provided by Us shall be considered Confidential. | | | |
| **Asset Register** | A dedicated IT asset register is operational and is maintainedwhich identifies key information at asset-level such as owner | ISO 27001 A.8.1.1<br>ISO 27001 A.8.1.2 | Yes |
| **Acceptable Use** | Formalized policy exists and is available to all employees onthe topic of acceptable use of IT assets such as company laptops/desktops | ISO 27001 A.8.1.3 | Yes |
| **Return of IT Assets** | Upon termination of employment, end users return all company-owned IT assets | ISO 27001 A.8.1.4 | Yes |
| **Information Classification** | All data provided to the Supplier shall be considered Confidential. Such rules should be adopted organization-wide in a dedicated policy/procedure document, and should be considered when handlinginformation as part of operational activities | ISO 27001 A.8.2.1<br>ISO 27001 A.8.2.2<br>ISO 27001 A.8.2.3 | Yes |
| **Removable Media Devices** | Sensitive information on media leaving the Supplier's premisesshould be protected to ensure access is restricted to the appropriate personnel (e.g., by means of encryption) | ISO 27018 A.11.4 | Yes |
| **Management & Destruction of Media** | Formalized procedures shall be implemented to ensure lifecyclemanagement of removable media in accordance with Information Security Policies | ISO 27001 A.8.3.1<br>ISO 27001 A.8.3.2<br>ISO 27001 A.8.3.3 | Yes |

**User Access Management**

Supplier has a duty to limit access to personal data on a "*need to know*" basis. Supplier is required to assess the nature of access allowed to an individual user. Supplier agrees that individual staff members shall only have access to data which they require to perform their duties, prevent use of shared credentials (multiple individuals using a single username and password) and detect use of default passwords. Access control must be supported by regular reviews to ensure that all authorized access to personal data is strictly necessary and justifiable for the performance of a function. Supplier has policies in place regarding vetting and oversight of the staff members allocated these accounts. A staff member with similar responsibilities should have separate user and administrator accounts. Multiple independent levels of authentication may be appropriate where administrators have advanced or extra access to personal data or where they have access or control of other's account or security data. Supplier agrees to have strict controls on the ability to download personal data from an organization's systems. Supplier agrees to block such downloading by technical means (disabling drives, isolating network areas or segments, etc.).

| Control Title | Control Description | Reference to Industry Standard | Implemented? (Yes/No) |
|---|---|---|---|
| **User registration and de-registration** | A formal process should exist to management the assignment, adjustment, and revoking of access rights, considering scenarios such as starters/leavers as well as changing of jobs internally within the organization | ISO 27001 A.9.2.1<br>ISO 27001 A.9.2.2<br>ISO 27001 A.9.2.6 | Yes |
| **Least Privileged Access / Role Based Access** | End users shall only be provided with access to IT/network applications based on the requirements of their role within the organization. By default, an end user should have access to a limited amount of IT resources (i.e., email) unless otherwise authorized by appropriate personnel. In circumstances where an end user requires access to a specific IT application, the minimal level of access required to perform their duties should be granted | ISO 27001 A.9.1.2 | Yes |
| **Passwords** | Passwords should be implemented on all IT applications and should not be shared. Passwords should be stored in encrypted form. All passwords must meet the following complexity requirements:<br>- Minimum length of 8 characters<br>- Must contain at least 1 upper-case character<br>- Must contain at least 1 number<br>- Must contain at least 1 special character<br>- Must not be the same as the last 24 passwords used<br>- Accounts are locked after 5 incorrect login attempts | ISO 27001 A.9.2.4<br>ISO 27001 A.9.3.1<br>ISO 27001 A.9.4.2<br>ISO 27001 A.9.4.3 | Yes |
| **Unique Use of User IDs** | End users should each be assigned an individual user ID or identifier for accessing IT resources to ensure accountability. In circumstances where generic user IDs may exist for various business reasons, only one (1) user should have access to such accounts | ISO 27018 A.11.8 | Yes |
| **User Access Reviews** | End user access to IT applications/resources should be reviewed periodically at defined intervals by appropriate personnel (e.g., application owner, line manager) to ensure all end users within the organization have the appropriate level of access to perform their duties, and that excessive access rights are not granted | ISO 27001 A.9.2.5 | Yes |

| Control Title | Control Description | Reference to Industry Standard | Implemented? (Yes/No) |
|---|---|---|---|
| **Physical & Environmental Security**<br>In addition to technical security measures, Supplier has implemented the physical security measures which are necessary to ensure the security and integrity of any Personal Data processed. The physical security measures include at minimum:<br>▪ perimeter security (monitoring of access, office locked and alarmed when not in use);<br>▪ restrictions on access to sensitive areas within the building (such as server rooms);<br>▪ computer location (so that the screen may not be viewed by members of the public);<br>▪ storage of files (files not stored in public areas with access restricted to staff with a need to access particular files); and<br>▪ secure disposal of records (effective "*wiping*" of data stored electronically; secure disposal of paper records). | | | |
| **Building Security (Perimeter)** | Physical security mechanisms for entering the premises are implemented to ensure that only authorized individuals have access | ISO 27001 A.11.1.1 | Yes |
| **Building Security (Internal)** | Additional physical security mechanisms for entering areas which contain critical/sensitive information should be restricted to the appropriate personnel (e.g., server room). Video surveillance/intrusion detection capabilities should monitor access to such working area entry points | ISO 27001 A.11.1.2<br>ISO 27001 A.11.1.3<br>ISO 27001 A.11.1.5 | Yes |
| **User Workspace** | Supplier-managed devices such as laptops should have appropriate mechanisms installed to ensure protection when unattended. In support of such, a clean desk policy shall be implemented to minimize the existence of physically stored information | ISO 27001 A.11.2.8<br>ISO 27001 A.11.2.9 | Yes |
| **Operational Security**<br>▪ Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.<br>▪ All data provided by Us should be encrypted using AES-128 or stronger.<br>▪ To protect data Integrity, data should be hashed using SHA-256 or stronger.<br>▪ All Confidential hard copy data that is no longer required must be shredded by use of a crosscut shredder.<br>▪ The print process must be adequately secured to prevent unauthorized disclosure/access.<br>▪ Extra precautions must be in place to protect the confidential data stored on portable systems or mobile devices. Devices and data must be stored securely when not in use. Portable systems with confidential data must not transfer data by use of Personal Area Networks.<br>▪ Web sites and applications must be backed up in accordance with Business Continuity and Disaster Recovery requirements. | | | |

| Control Title | Control Description | Reference to Industry Standard | Implemented? (Yes/No) |
|---|---|---|---|
| **Information Backup & Restoration** | Backup copies of appropriate information shall be taken as well as tested regularly in accordance with Supplier's backup policy | ISO 27001 A.12.3.1 | Yes |
| **Event Logging** | Event logging should be enabled in IT applications to record actions such as user activities and reviewed periodically to monitor potential information security events | ISO 27001 A.12.4.1 | Yes |
| **Change Management** | Changes to business processes or IT applications should be controlled by means of a formalized process, such as a change request process or governed by a change advisory board (**CAB**) | ISO 27001 A.12.1.2 | Yes |
| **Malware Controls** | Capabilities to prevent against and to detect malware should be implemented which are applicable to all IT resources (e.g., by means of antivirus software, firewalls etc.). All such solutions should be kept up to date. | ISO 27001 A.12.2.1 | Yes |
| **Vulnerability Management** | Supplier shall define a process to identify and remediate vulnerabilities to IT applications (e.g., a patch management process) | ISO 27001 A.12.6.1 | Yes |
| **End-User Software Installation** | Supplier shall define rules to govern the installation of software on company devices by end users. Where possible, software should not be installed on company-managed devices by anyone other than IT administrators | ISO 27001 A.12.6.2 | Yes |
| **Communications Security**<br>▪ Supplier must secure all backup media during transportation and in storage.<br>▪ Supplier should catalog all media so that a missing storage unit (and which unit it is) shall be easily identified. Supplier should not label media in such a way that it discloses the data it contains or its owner company in a manner that is easily identified by an outsider.<br>▪ Supplier should maintain system and application backups that support a total system restore for a 30-day period as a minimum. Backup media must be on separate media from the system.<br>▪ Supplier must destroy all confidential data within 30 days of termination of Supplier contract.<br>▪ Copies of Confidential Data on system backup media that is co-mingled with other system data are not included | | | |
| **Network Security** | Corporate network is controlled to protect information by means of security mechanisms and resourcing (incl. segregated where appropriate) | ISO 27001 A.13.1.1<br>ISO 27001 A.13.1.2<br>ISO 27001 A.13.1.3 | Yes |

| Control Title | Control Description | Reference to Industry Standard | Implemented? (Yes/No) |
|---|---|---|---|
| **Encryption of Data** | Sensitive information shall be encrypted during transmission | ISO 27001 A.13.2.1 | Yes |
| **Incident Management**<br>As part of a data security policy, Supplier has a policy in place describing what it does in case of a data breach, and represents it has the capacity to respond adequately to cover the requirements of mandatory breach reporting (*where applicable*) under applicable Data Protection Laws.<br>▪ Any security event involving or impacting Us and/or a Company website must be reported to Company. Notification must be within 48 hours from detection if Company data, brand, logo or trademarks are involved or compromised.<br>▪ Any security event where a Company website had unauthorized access or was compromised must be reported to Us.<br>▪ All systems and applications must be designed to log, monitor, and report all security events. Logs must be tampered proof and/or off system write only log files.<br>▪ In the event of an incident, audit trails must be available to assist investigations. We may request to cooperatively work with the Supplier on security forensics for some incidents. | | | |
| **Incident Detection & Response** | Supplier has in place a formalized structure (e.g., a security operations center) to ensure detection and response to information security events which may be deemed as an incident | ISO 27001 A.16.1.1<br>ISO 27001 A.16.1.2<br>ISO 27001 A.16.1.3<br>ISO 27001 A.16.1.4<br>ISO 27001 A.16.1.5 | Yes |
| **Employee Reporting** | Employees/contractors have mechanisms available to report potential incidents or security weaknesses observed | | Yes |
| **Business Continuity & Disaster Recovery (BCDR)**<br>▪ Cloud-based services require a non-cloud-based solution as one of the Business Continuity / Disaster Recovery options in the event of an incident.<br>▪ Supplier must have a disaster recovery plan in place in the event that a major disruptive incident impacts their ability to provide service.<br>▪ Mission or business critical functions must have a recovery or continuity plan in place per the mutually agreed upon Service Level Agreement.<br>▪ Defined strategies must be tested annually and revised where necessary.<br>▪ All system media has a regularly scheduled backup and restore capability implemented and tested.<br>▪ Supplier personnel responsible to support business and disaster recovery functions must be identified to Us upon request. | | | |
| **BCDR Processes** | Supplier has in place contingency plans or business recovery strategies, which are inclusive of the concepts of Information Security & Privacy | ISO 27001 A.17 | Yes |

## 6. SERVER SECURITY

### 6.1 Intrusion Detection

- All production servers must be located in a secure, access-controlled location.
- All systems must be hardened prior to production use including patching of known vulnerabilities. Disable all generic, guest, maintenance, and default accounts.
- Patching of security vulnerabilities to the operating system and software must meet or exceed the service level interval defined by the vendor for the threat level of the vulnerability.
- Test accounts and user accounts are removed/revoked when no longer required.
- Development and test systems are isolated from production environment and network.
- Disable all non-required ports and/or services on server operating systems and firewalls.
- Consoles with keyboards have password protected screen savers that logoff unattended.

### 6.2 Virtualized System

- All Intrusion Detection Systems in place should be configured to provide data on demand, to identify sources of a potential attack/intrusion at the network perimeter.
- Systems should have the ability to detect a potential hostile attack. Examples include but are not limited to: Network Intrusion Detection or Host Intrusion Detection/Prevention.
- Any single image of data classified as Confidential defines the minimum-security requirement for all virtual instances on the same host system.
- Virtualized systems may contain data classified as confidential data. (c) Applications that require physical separation cannot be on the same host system.

### 6.3 Cloud Services and Systems

- Any single image of data classified as Confidential defines the minimum-security requirement for all virtual instances in the cloud.
- Cloud based systems may contain confidential data. We reserve the right to perform a Security review and Risk Assessment of applications and services containing confidential data in the cloud before implementation.
- No services will be run from the cloud that interacts with data exceeding the Company classification of "**Confidential**". (d) Existing services containing confidential data may not be pushed to the cloud or transferred to cloud service vendors without Our approval. It is subject to approval following a Security review and Risk Assessment by Us.

## 7. GENERAL REQUIREMENTS

### 7.1 Application Development

- The application and associated databases must validate all input.
- Implement safeguards against attacks (e.g., sniffing, password cracking, defacing, backdoor exploits)
- Protect the data by using a least privilege and a defense-in-depth layered strategy to compartmentalize the data.
- Handle errors and faults by always failing securely without providing non-essential

information during error handling.

- Log data to support general troubleshooting, audit trail investigative requirements, and regulatory requirements, with support for centralized monitoring where appropriate.
- Built-in security controls – built-in access controls, security auditing features, fail-over features, etc.
- Prevent buffer overflows.
- Avoid arithmetic errors.
- Implement an error handling scheme. Error messages should not provide information that could be used to gain unauthorized access.
- Test data used during development must be non-production simulated data.
- Implement protocols (TCP/IP, HTTP, etc.) without deviation from standards.

**7.2** Security Reviews:

- Web application vulnerability assessments must be performed during the application development and the deployment lifecycle.
- All third-party software included in the application must meet all security requirements outlined herein.
- Secure interfaces for USER LOGIN and user data input of Personal Data must utilize certificates signed by a trusted Certificate Authority (CA) only. Examples: HTTPS / TLS / SSH.

**7.3** Security of System Files

- Access to source code must be limited and controlled.
- During and after development, all applications must ensure the security of system files, plus access to source code and test data.
- All back-door maintenance hooks must be removed from the application before production use.
- Application architecture must prohibit databases containing confidential information from residing on the same server as the application.
- Databases must be secured as well as the applications and servers on which they reside. (f) Confidential Data is prohibited from residing on systems that have Peer-to-Peer (P2P) applications or Personal Area Networks (**PAN**).

**7.4** Application Availability

- All applications should be designed to minimize the risk from denial-of-service attacks.
- All applications should limit resources allocated to any user to the minimum necessary to perform the task.
- All applications must prevent unauthenticated users from accessing data or using vital system resources.

**7.5** Vulnerability Management

- Supplier is responsible for running its own vulnerability management.

- In addition, We require daily vulnerability scans performed on all internet facing web sites where branded content and is the primary site owner or 'Trellix' is part of the URL. We use the Company Secure vulnerability scanning solution. Vulnerabilities will be reported to the Supplier for remediation. The Supplier can request information for: vulnerability reports, demonstration of the vulnerabilities (when available) and remediation support. We do not charge the Supplier for the Secure scanning service.
- We require daily access to the reports.
- Upon identification of security vulnerabilities in a production application, the Supplier must remediate within the following timelines:

Critical: 7 days

High: 30 days

Medium: 90 days

Low: 180 days

- If the security vulnerabilities identified by the Company vulnerability scanning process have not been addressed in the above timelines, We may shut down the web site until the vulnerabilities are remediated. Returning the site to production status requires the site to pass a scan for Company Compliance.
- We consider a web site compliant when Company security standards are met. Company Security will notify Suppliers of each of the security standards not met.
- Any changes to the architecture or function of a service or data model in the cloud must first be reviewed and approved by Us.
- Applications that require physical separation cannot be on a cloud-based service.
- Cloud vendors are required to have background checks and validation of employees with privileged account access. This includes any third-party vendors that may contract with those vendors and have privileged access as well.

## 8. NETWORK & CLIENT SECURITY

### 8.1 Remote Access

- There should be no dial-in modems on the network without secondary authentication. (Dial back is not authentication).
- Outbound modems (*such as for paging*) must have inbound calls disabled.

### 8.2 Client Security

- Patching of security vulnerabilities to the operating system and software must meet or exceed the service level interval defined by the vendor for the threat level of the vulnerability.
- Clients must have Malware protection with automatic signature updates.
- Systems located in an unsecured area and attached to the Supplier network must not access systems and network segments containing confidential data.
- All client systems that access confidential data, whether in use or not, must be physically secured.
- Client systems which access confidential data from secured locations must have a password

protected screen saver or automated logoff after no more than 15 minutes of inactivity of account access. This includes any third-party vendors that may contract with those vendors and have privileged access as well.

## 9. FIREWALL SETUP

- Network segments connected to the Internet must be protected by a firewall and configured to secure all devices behind it.
- All system security and event logs are reviewed regularly for anomalies, and available to Us in the event of an incident.
- Unused ports and protocols must be disabled.
- Firewalls must be configured to prevent address spoofing.
- Only TCP ports should be used for web applications.
- Supplier firewalls must be configured to allow scanning of Company Web applications. Company scanning source IP addresses willbe provided to Suppliers.

## 10. DATA SECURITY

### 10.1 Data Classification and Handling

- Appropriate security measures must be in place to address data handling, access requirements, data storage and communications (intransit).
- All Company data is Confidential.

### 10.2 Privacy Management

- Applications such as "Software as a Service" used by Us to collect Personal Data must have the URL for the Company Privacy Statement embedded into the web page where Personal Data is collected. It is available in all languages.
- Where applicable, individuals must be given the opt-in choice to participate prior to providing their Personal Data. Opt-in selection boxes are not pre-selected by default.
- Where applicable, the system should have the capability of allowing individuals to access update or delete their Personally Identifiable Information or unsubscribe when requested. This can be an automated or manual process. The process must be clearly explained to the individual.
- System must not transfer Personal Data to other systems or be used for purposes other than specified.
- System must have appropriate security controls to avoid unauthorized access, disclosure and / or use or modification of individuals' Personal Data.
- The system must adhere to the Federal Trade Commission's CAN-SPAM Act if it:
- Requests input of Personal Data from an individual to complete "Email to a Friend" notifications, or
- The system offers online, subscription-based communication services.

### 10.3 Data Protection Security

- Suppliers are responsible for data protection, privacy compliance, and security control

validation/ certification of their subcontractors.

1. For data classified as Confidential, Confidential – Internal Use Only or Restricted, data should be encrypted using AES-128 or stronger.
   - To protect data Integrity, data should be hashed using SHA-256 or stronger.
   - All Confidential hard copy data that is no longer required must be shredded by use of a crosscut shredder.
   - The print process must be adequately secured to prevent unauthorized disclosure/access.
   - Extra precautions must be in place to protect the confidential data stored on portable systems or mobile devices. Devices and data must be stored securely when not in use.
   - Portable systems with confidential data must not transfer data by use of Personal Area Networks
   - Web sites and applications must be backed up in accordance with Business Continuity and Disaster Recovery requirements.
   - Supplier must secure all backup media during transportation and in storage.
   - Supplier should catalog all media so that a missing storage unit (and which unit it is) shall be easily identified. Supplier should not label media in such a way that it discloses the data it contains or its owner company in a manner that is easily identified by an outsider.
   - Supplier should maintain system and application backups that support a total system restore for a 30-day period as a minimum. Backup media must be on separate media from the system.
   - Supplier must destroy all confidential data within 30 days of termination of Supplier contract. Copies of Confidential Data on system backup media that is co-mingled with other system data are not included.

## 11. EXTRANET REQUIREMENTS

- All extranet connectivity into the Company must be through secure communications.
- All data exchanged with Us for mission or business critical functions, (B2B), require secure intercompany communications (ICC) implemented by Company IT Engineering services. The Company program manager is responsible for communications funding and will arrange for Suppliers to engage with the Company engineering services team.
- Supplier is responsible for implementing the secure protocols at their sites

## 12. DEVIATION FROM USE

Any deviation from the requirements of this standard must be approved in writing by Company Information Security.

## 13. DURATION

This standard will remain in effect until cancelled or modified by the Company Chief Information Security Officer.

## 14. DEFINITIONS AND ABBREVIATIONS

Capitalized terms not defined herein shall have the meaning ascribed to such terms in the Agreement.

**Application Security:** Refers to protecting data processed by an application, as well as the integrity and

availability of services provided by the application.

**Business Critical**: Loss that indirectly impacts a Mission Critical function, or directly impacts a business unit's primary function is considered Business Critical.

**Cloud Computing:** Computing resources, software and data delivered as a hosted service over the Internet. The computing resources are dynamically scalable and often virtualized. The services are accessible anywhere that provides access to networking infrastructure.

**California Consumer Privacy Act of 2018** or "**CCPA**": means Cal. Civ. Code § 1798.100, *et seq.*, as amended

**Confidential Data:** Information with restricted access limited to those individuals with a need to know.

**Content Moderation:** A business process where content is reviewed and approved by Us or a Company representative with the appropriatetraining before it is viewable by others.

**Content Monitoring:** A business process where content is reviewed (and removed if necessary) by Us or a Company representative with theappropriate training after it is viewable by others.

**Data Protection Laws:** means EU Data Protection Laws, the CCPA, and, to the extent applicable, the data protection or privacy laws of any other country.

**EU Data Protection Laws:** means the GDPR and any local data protection laws applicable in the EEA.

**EEA:** means the European Economic Area and Switzerland.

**External Facing (Public):** Information available without approval or authentication.

**GDPR:** means the European Union (EU) General Data Protection Regulation 2016/679.

**Information Security Incident**: means any occurrence involving the compromise of Company Confidential Information through the accidental or unlawful destruction or loss of Confidential Information or the unauthorized collection, use, copying, modification, disposal, disclosure, or access of Confidential Information including Personal Data.

**Mission Critical:** Loss that directly impacts Our ability to Book, Build, Ship, Order, Pay, Close or Communicate is considered Mission Critical.

**Moderation:** A business process where Company personnel or a contracted agent reviews and either approves or rejects user generated content (UGC) based on the business situation. Automated moderation is when computerized searches are performed on UGC to screen the input for unwanted or malicious input. Community moderation for appropriateness of content is reporting by the user community of violations of content afterit is posted.

**Physical Security:** Measures taken to protect systems, buildings, and related support infrastructure against threats from the physical environment.

**Personal Data:** shall have the same meaning as in the Data Protection Laws.

**Privacy:** An individual's right to have a private life, to be left alone and to be able to decide when their personal information is collected, used, or disclosed.

**User Generated Content (UGC):** Content input into a web application either by text input or rich media such as pictures, audio and videos via file uploads or widgets.

**Unsecured Area:** Areas that are not controlled by physical access security measures. Some examples include: the lobby of an access-controlled building or a warehouse delivery dock with PC access to corporate systems.

**Virtualized System:** The use of the term 'virtualized system' includes any of the following: A virtual machine (VM) is a software implementation of a computer that executes programs like a real machine. The virtual machine monitor (VMM) or hypervisor is the software layer providing the virtualization. Platform virtualization and /or hardware virtual machines that allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system.

*-End -*