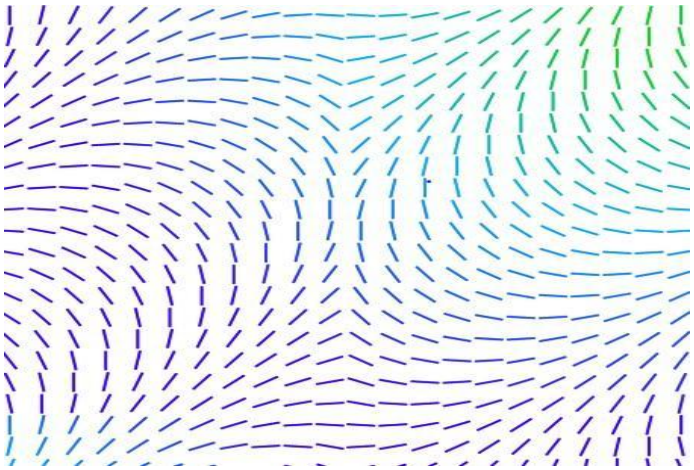
Trellix

TRESTAND 1504

Supplier Security Requirements and Expectations for Confidential Data Standard



Trellix

Table of Contents

1. Purpose

The Supplier Security Requirements and Expectations (SSRE) for Confidential Data establishes Supplier's minimum-security standard for the protection of Musarubra LLC's (DBA Trellix) confidential information, including Trellix Personal Data (collectively "Trellix Data").

2. Scope

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.

3. Target Audience

This policy applies to all Supplier end-users who have access to the Trellix network, including web-based applications, or who use data owned, licensed by, or in the possession, custody, or control of Trellix. End-users with access to Trellix data include Supplier employees, contractors, consultants, interns, service providers, partners, suppliers, vendors, third parties, and entities acting on behalf of Trellix.

4. Roles and Responsibilities

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 Trellix Internal and Trellix Confidential.

The Trellix business owner is responsible for classifying the data and communicating it to the Supplier. At a minimum, Suppliers must be capable of implementing security controls required to protect data classified as confidential.

5. Compliance

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 Trellix.

The 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 to Trellix. Examples include, but are not limited to, GDPR, CCPA and CAN-SPAM Act compliance. Suppliers are responsible for compliance with any laws and regulatory requirements applicable to their use of the Trellix system.

5.1 Document Review

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 Trellix or on behalf of Trellix and to ensure subcontractor's compliance herewith.

6. Standard

6.1 General Undertakings

- Suppliers shall review all security controls cited in this document and may request clarification where needed.
- Suppliers shall notify the appropriate Trellix business owner of full compliance in writing authorized by a company official.
- Existing Suppliers that have complied with a previous version of the SSRE must review and adhere to instructions in this document as Trellix 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 a committed plan of action detailing when the requirements will be fully met.
- Trellix's Information Security team shall evaluate a Supplier's security capabilities. If approved by Trellix, the Supplier's 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, and the Supplier's track record for prompt remediation of vulnerabilities will be evaluated.
- Suppliers shall agree to fully comply with the Trellix *Code of Conduct*, as set forth in Trellix's Supplier portal and the *Responsible Business Alliance* (https://www.responsiblebusiness.org/code-of-conduct/). Additionally, while performing services in Trellix owned or operated facilities, Suppliers shall agree to abide by all Trellix 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 Trellix 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 Trellix premises and shall keep Trellix's site free from hazards.
- The 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.
- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier agrees to implement the following measures:
    - the pseudonymization and/or 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 Trellix data in a timely manner in the event of a physical or technical incident; and
  - a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- The 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.

6.2 Cloud Services and Systems

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

6.3 Vulnerability Management

- If the Supplier is hosting a public-facing Trellix website, Trellix shall perform regular vulnerability scans on all internet-facing web sites where Trellix has branded content, or where Trellix is the primary site owner or "Trellix" is part of the URL.
- Vulnerabilities will be reported to the Supplier for remediation. The Supplier can request further information regarding the vulnerability reports, demonstration of the vulnerabilities (when available), and remediation support.
- Trellix will not charge the Supplier for the Trellix Secure scanning service. Upon identification of security vulnerabilities in a production application, Supplier must remediate within the minimal following timelines:
  (i) Urgent or Critical, Trellix threat rating [5] or [4] must be remediated in 1 to 5 calendar days;

(ii) High, Trellix threat rating [3] must be remediated within 10 calendar days and
(iii) Medium, Trellix threat rating [2] must be remediated within 30 calendar days.

If the security vulnerabilities identified by the Trellix vulnerability scanning process have not been addressed in the above timelines by the Supplier, Trellix may request to shut down the web site until the vulnerabilities are remediated. Returning the web site to production status requires the site to pass a scan for Trellix compliance.

- Trellix considers a web site compliant when Trellix security standards are met.
- Trellix will notify Suppliers any time the Trellix security standards are not met.

6.4 Organizational Measures

The implementation and operational effectiveness of all below controls are mandatory. The below organizational measures are derived from Trellix's Third-Party Information Security Risk requirements, which align to leading industry standards.

Unless the Supplier informs Trellix and requires specific modifications to the below, the following Organizational Measures will be deemed agreed upon by the Supplier.

Organizational Measures

- The Supplier has a specific resource assigned that is accountable for security management.
- All systems have malware management which includes up to date signature files running on all production systems.

If administration of any systems or applications is performed outside the Suppliers secured intranet, it must be done through a secure channel (VPN or SSL)

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
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 applicable guidelines. Supplier is certified against (at a minimum) the ISO 27001 standard and has a periodic cycle of internal and external audits to ensure the continued compliance of all applicable security controls. Supplier shall submit a copy of any	ISO 27001 A.12.7.1	Yes

	industry standard accreditation applicable to the products or services it is providing to Trellix (e.g., ISO27001 or SSAE18-SOC 2 audits performed by an independent auditor within the last year) and provide annual updates of the accreditation during the term of the Agreement. Supplier shall also inform Trellix of its adherence to data protection certification.		
Privacy & Protection of Personal Data	Supplier takes measures to ensure protection of Personal Data as required with relevant legislation such as the GDPR. At a minimum, the Supplier encrypts data at rest and in transit according to standards and applicable guidelines.	ISO 27001 A.18.1.4	Yes
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 to ensure their continued effectives to the organization.	ISO 27001 A.5.1.1 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 ISO 27001 A.12.1.4	Yes

Information Security & Privacy Awareness

- The Supplier personnel must be trained in the Supplier security policies and be required to know changes or updates to these policies.
- Security training, including new threats and vulnerabilities, is required for all developers and system administration staff.
- All personnel with access to confidential data will have information security training for their respective roles.
- All personnel receive regular updates to their training for their respective roles.
- 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. Refresh training is required annually.

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.			
Control Title	**Control Description**	**Reference to Industry Standard**	**Implemented? (Yes/No)**
Employee Screening	Checks on all job applicants will be performed in compliance with applicable rules, legislation, and ethics and should be proportionate to business criteria, classification of the information to be obtained, and potential risks.	ISO 27001 A.7.1.1	Yes
Contractual Obligations	Contracts with both employees and contractors shall state employee obligations for information security and data privacy both during and after termination of employment.	ISO 27001 A.7.1.2 ISO 27001 A.7.3.1	Yes
Information Security & Privacy Training	All employees shall receive appropriate education on the topics of 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
IT Asset Management • All data provided by Trellix shall be considered Confidential.			
Control Title	**Control Description**	**Reference to Industry Standard**	**Implemented? (Yes/No)**
Asset Register	A dedicated IT asset register is operational and is maintained which identifies key information at asset-level such as owner.	ISO 27001 A.8.1.1 ISO 27001 A.8.1.2	Yes
Acceptable Use	Formalized policy exists and is available to all employees on the 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 handling information as part of operational activities.	ISO 27001 A.8.2.1 ISO 27001 A.8.2.2 ISO 27001 A.8.2.3	Yes
Removable Media Devices	Sensitive information on media leaving the Supplier's premises should be protected to ensure	ISO 27018 A.11.4	Yes

	access is restricted to the appropriate personnel (E.g., by means of encryption).		
Management & Destruction of Media	Formalized procedures shall be implemented to ensure lifecycle management of removable media in accordance with Information Security Policies.	ISO 27001 A.8.3.1 ISO 27001 A.8.3.2 ISO 27001 A.8.3.3	Yes

User Access Management

- The Supplier has a duty to limit access to Personal Data on a "need to know" basis.
- The Supplier is required to assess the nature of access allowed to an individual user.
- The Supplier agrees that individual staff members shall only have access to data which they require in order 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.
- The 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.
- The Supplier agrees to have strict controls on the ability to download Personal Data from an organization's systems.
- The 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 manage 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 ISO 27001 A.9.2.2 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	ISO 27001 A.9.1.2	Yes

	requires access to a specific IT application, the minimal level of access required to perform their duties should be granted.		
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: ● Minimum length of 14 characters ● Must contain at least 1 upper-case character ● Must contain at least 1 number ● Must contain at least 1 special character ● Must not be the same as the last 24 passwords used ● Accounts are locked after 5 incorrect login attempts.	ISO 27001 A.9.2.4 ISO 27001 A.9.3.1 ISO 27001 A.9.4.2 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

Physical & Environmental Security

In addition to technical security measures, the 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:

- Perimeter security (monitoring of access, office locked and alarmed when not in use);
- Restrictions on access to sensitive areas within the building (such as server rooms);

- Computer location (so that the screen may not be viewed by members of the public);
- Storage of files (files not stored in public areas with access restricted to staff with a need to access particular files); and
- Secure disposal of records (effective "wiping" of data stored electronically; secure disposal of paper records).

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
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 ISO 27001 A.11.1.3 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 ISO 27001 A.11.2.9	Yes

Operational Security

- Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.
- All data provided by Trellix 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.

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	The 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	The 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

- The Supplier must secure all backup media during transportation and in storage.
- The 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.
- The 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.
- The Supplier must destroy all confidential data within 30 days of termination of Supplier contract.

- Copies of Confidential Data on system backup media that is commingled with other system data are not included

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Network Security	Corporate networks are controlled to protect information by means of security mechanisms and resourcing (incl. segregated where appropriate).	ISO 27001 A.13.1.1 ISO 27001 A.13.1.2 ISO 27001 A.13.1.3	Yes
Encryption of Data	Sensitive information shall be encrypted during transmission.	ISO 27001 A.13.2.1	Yes

Incident Management

As part of a data security policy, the 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 in order to cover the requirements of mandatory breach reporting (where applicable) under applicable Data Protection Laws.

- Any security event involving or impacting Trellix and/or a Trellix website must be reported to Trellix. Notification must be within 48 hours from detection if Trellix data, the Trellix brand, logo or trademarks are involved or compromised.
- Any security event where a Trellix website had unauthorized access or was compromised must be reported to Trellix.
- 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.
- In the event of an incident, audit trails must be available to assist investigations. Trellix may request to cooperatively work with the Supplier on security forensics for some incidents.

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
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 ISO 27001 A.16.1.2 ISO 27001 A.16.1.3 ISO 27001 A.16.1.4 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 (BC/DR)

- Cloud-based services require a non-cloud-based solution as one of the Business Continuity / Disaster Recovery options in the event of an incident.
- The Supplier must have a disaster recovery plan in place in the event that a major disruptive incident impacts their ability to provide service.
- Mission or business critical functions must have a recovery or continuity plan in place per the mutually agreed upon Service Level Agreement (SLA).
- Defined strategies must be tested annually and revised where necessary.

• All system media has a regularly scheduled backup and restore capability implemented and tested. • The Supplier's personnel responsible to support business and disaster recovery functions must be identified to Trellix upon request.			
Control Title	**Control Description**	**Reference to Industry Standard**	**Implemented? (Yes/No)**
BC/DR Processes	The 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

6.5 Server Security

6.5.1 System Hardening

- All production servers must be located in a secure, access-controlled location.
- All systems must be hardened prior to production use, including but not limited to patching known vulnerabilities and disabling 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 must be removed/revoked when no longer required.
- Development and test systems must be isolated from the production environment and network.
- All non-required ports and/or services on server operating systems and firewalls must be disabled.
- Consoles with keyboards must have password protected screen savers that logoff unattended.

6.5.2 Intrusion Detection

- All intrusion detection systems (IDS) in place should be configured to provide data on demand and 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 (NID) or Host Intrusion Detection/Prevention (HID).
- Any single image of Trellix 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.
- Applications that require physical separation cannot be on the same host system.

6.5.3 Virtualized System

- Any single image of Trellix data classified as confidential defines the minimum-security requirement for all virtual instances in the cloud.
- Cloud-based systems may contain confidential data. Trellix reserves 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 interact with data exceeding the Trellix classification of “Confidential.”
- Existing services containing confidential data may not be pushed to the cloud or transferred to cloud service vendors without Trellix approval, which will be provided following a security review and risk assessment by Trellix.

6.6 General Requirements

6.6.1 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.
- Provide log data to support general troubleshooting, audit trail investigative requirements, and regulatory requirements, with support for centralized monitoring where appropriate.
- Built-in security controls, i.e., 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.

6.6.2 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.

6.6.3 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 and 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 Trellix Data from residing on the same server as the application.
- Databases must be secured, as well as the applications and servers on which they reside.
- Trellix Data is prohibited from residing on systems that have Peer-to-Peer (P2P) applications or Personal Area Networks (PAN).

6.6.4 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.

6.6.5 Vulnerability Management

- The Supplier is responsible for running its own vulnerability management.
- In addition, Trellix requires regular vulnerability scans performed on all internet facing web sites where Trellix has branded content and is the primary site owner or “Trellix” is part of the URL. Trellix uses the Trellix 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. Trellix does not charge the Supplier for the Trellix Secure Scanning service.
- Trellix requires regular 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 Trellix Vulnerability Scanning process have not been addressed in the above timelines, Trellix 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 Trellix compliance.

- Trellix considers a web site compliant when Trellix security standards are met. Trellix Security will notify Suppliers of each of the Trellix 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 Trellix.
- 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.

6.7 Network & Client Security

6.7.1 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.

6.7.2 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.
- Client systems 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 Trellix Data.
- All client systems that access Trellix Data, whether in use or not, must be physically secured.
- Client systems which access Trellix 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.

6.8 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 must be reviewed regularly for anomalies, and available to Trellix 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.
- The Supplier’s firewalls must be configured to allow Trellix scanning of Trellix web applications. Trellix scanning of source IP addresses will be provided to Suppliers.

6.9 Data Security

6.9.1 Data Classification and Handling

- Appropriate security measures must be in place to address data handling, access requirements, data storage and communications (in transit).
- All Trellix data is classified as "confidential."

6.9.2 Privacy Management

- All Supplier applications, such as "Software as a Service," used by Trellix to collect Personal Data must have the URL for the Trellix *Website Privacy Notice* embedded into the web page. The Notice 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 must not be pre-selected by default.
- Where applicable, Supplier's system should have the capability of allowing individuals to access, update or delete their Personally Identifiable Information (PII) or unsubscribe when requested. This capability can be enabled via an automated or manual process. The process must be clearly explained to the individual.
- Supplier's system must not transfer Personal Data to other systems or be used for purposes other than specified.
- Supplier's system must have appropriate security controls to avoid unauthorized access, disclosure, and / or use or modification of individuals' Personal Data.
- Supplier's 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.

6.9.3 Data Protection Security

- Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.
    a) For data classified as "Trellix Confidential," "Trellix Internal" or "Trellix Restricted," data should be encrypted using AES-128 or stronger.
- To protect data integrity, data should be hashed using SHA-256 or stronger protocol.
- All Trellix Data which is captured in hard-copy 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 any Trellix Data stored on portable systems or mobile devices. Devices and data must be stored securely when not in use.
- Portable systems containing Trellix 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.
- The Supplier must secure all backup media during transportation and while in storage.
- The 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.
- The 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.
- The Supplier must destroy all Trellix Data within 30 days of termination of the Supplier's contract. Copies of Trellix Data on system backup media that are commingled with other system data are not included.

7. Deviation from Use

Exceptions to this policy must be requested to and approved by the Office of the Chief Information Security Officer (OCISO) via the Security Exception Request process in the Enterprise Services Portal.

8. Duration

This standard will remain in effect until canceled or modified by the Trellix Chief Information Security Officer (CISO).

9. References

- *Responsible Business Alliance:* https://www.responsiblebusiness.org/code-of-conduct/
- *Federal Trade Commission's CAN-SPAM Act*
- ISO 27001
- Trellix *Code of Conduct*
- Trellix *Privacy Notice*

10. Definitions and Acronyms

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.

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 Trellix or a Trellix representative with the appropriate training before it is viewable by others.

Content Monitoring: A business process where content is reviewed (and removed if necessary) by Trellix or a Trellix representative with the appropriate 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: GDPR and any local data protection laws applicable in the European Economic Area and Switzerland (EEA).

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

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

Information Security Incident: Any occurrence involving the compromise of Trellix Data through the accidental or unlawful destruction or loss of Trellix Data or the unauthorized collection, use, copying, modification, disposal, disclosure, or access of Trellix Data.

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

Moderation: A business process where Trellix 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 after it 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.

Trellix Data: Trellix Confidential Information, including Personal Data.

Unsecured Area: Areas that are not controlled by physical access security measures. Some examples are 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.

11. Revision History

VERSION	DATE PUBLISHED	PREPARED BY	CONTRIBUTORS	SUMMARY OF CHANGES
1.1	August 2024	Stephanie Lewis	Thomas Crouch - Legal Clark Lovrien - GRC	Annual review and update.
1.0	August 2022	Stephanie Lewis	Patrick McEnany	Initial publication.

12. Approvals

VERSION	DATE PUBLISHED	PREPARED BY	BUSINESS UNIT OWNER(S)	APPROVER(S)
1.1	August 2024	Stephanie Lewis	OCISO - GRC	Harold Rivas - CISO DocuSigned by: Harold Rivas 9DA470D3ECBD47E...
1.0	August 2022	Stephanie Lewis	OCISO - GRC	Howard Israel - vCISO