



# Supplier Security Requirements and Expectations for Confidential Data Standard

## Table of Contents

<b>1. Purpose</b>	<b>3</b>
<b>2. Scope</b>	<b>3</b>
<b>3. Target Audience</b>	<b>3</b>
<b>4. Roles and Responsibilities</b>	<b>3</b>
<b>5. Compliance</b>	<b>3</b>
5.1 Document Review	3
<b>6. Standard</b>	<b>4</b>
6.1 General Undertakings	4
6.2 Cloud Services and Systems	5
6.3 Vulnerability Management	5
6.4 Server Security - System Hardening	6
6.5 Application Development	7
6.6 Security Reviews	7
6.7 Security of System Files	8
6.8 Application Availability	8
6.9 Network & Client Security	8
6.10 Firewall Security	9
6.11 Privacy Management	9
6.12 Data Security	10
<b>7. Deviation from Use</b>	<b>11</b>
<b>8. Duration</b>	<b>11</b>
<b>9. References</b>	<b>11</b>
<b>10. Definitions and Acronyms</b>	<b>11</b>

## 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 (which includes Trellix and Skyhigh Security and herein known as the "Company") confidential information, including Company personal data (collectively "Company 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 Company's network, including web-based applications, or who use data owned, licensed by, or in the possession, custody, or control of the Company. End-users with access to Company data include Supplier employees, contractors, consultants, interns, service providers, partners, suppliers, vendors, third parties, and entities acting on behalf of the Company.

## 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 Company Internal and Company Confidential.

The Company 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 the Company.

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

## 6. Standard

### 6.1 General Undertakings

**6.1.1** Suppliers shall notify the appropriate Company business owner of full compliance of security controls in writing authorized by a company official.

**6.1.2** Existing Suppliers that have complied with a previous version of the SSRE must review and adhere to instructions in this document as the Company may have included important updates/changes from previous versions.

**6.1.3** 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 time-committed plan-of-action detailing when the requirements will be fully met.

**6.1.4** During a contract review the following will be evaluated:

- Supplier's performance of the SSRE security requirements,
- Remediation of non-compliant security controls, and the
- Supplier's track record for prompt remediation of vulnerabilities.

**6.1.5** Suppliers shall agree to fully comply with:

- [Trellix Code of Conduct](#) / [Skyhigh Security Code of Conduct](#), as set forth in the [Trellix Supplier Portal](#) / [Skyhigh Security Legal Portal](#) and the [Responsible Business Alliance](#).
- The Company's corporate and security policies while performing services in the Company's owned or operated facilities
- The Company's safety, health and hazardous material management rules, and rules prohibiting misconduct on the Company's premises.

**6.1.6** Suppliers will perform only those services identified in a duly executed statement of work and will work only in areas designated for such services.

**6.1.7** The Supplier agrees to implement data protection by design and by default and appropriate [Trellix Technical & Organizational Measures](#) / [Skyhigh Security Technical & Organizational Measures](#) to ensure a level of security appropriate to the risk.

**6.1.8** Taking into account 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 Company 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.

**6.1.9** 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**

**6.2.1** Cloud-based systems may only contain Company data subject to the prior written approval of the Company and must conform to ISO/IEC 27001 standards as a minimum.

**6.2.2** The Company reserves the right to perform a security review and risk assessment of applications and services containing Company data in the cloud prior to implementation.

**6.2.3** Applications that require physical separation cannot be on a cloud-based service unless duly segregated. The Supplier shall ensure Company data is fully segregated from the Supplier's other customers and/or third-parties.

**6.2.4** In addition, the Supplier agrees to allow any regulated Company 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 the Company or by a regulated End-User Customer, to audit the Supplier.

**6.2.5** The Supplier also agrees to allow the Company to provide any such reports to its End-User Customers, where required.

## **6.3 Vulnerability Management**

**6.3.1** The Supplier is responsible for running its own vulnerability management.

**6.3.2** The Company requires regular vulnerability scans performed on all internet-facing websites where the Company has branded content and is the primary site owner or "Trellix/Skyhigh Security" is part of the URL. The Company uses Company secure vulnerability scanning solutions.

- 6.3.3** 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.
- 6.3.4** The Company requires regular access to penetration testing reports.
- 6.3.5** The Company will not charge the Supplier for Company secure scanning service. Upon identification of security vulnerabilities in a production application, Supplier must remediate according to the rationalized risk rating using NIST [National Vulnerability Database CVSS v4.0](#) as the basis:
- (i) Urgent or Critical, Company threat rating [10.0 - 9.0] must be remediated in 1 - 7 calendar days;
  - (ii) High, Company threat rating [7.0 - 8.9] must be remediated within 30 calendar days and
  - (iii) Medium, Company threat rating [4.0 - 6.9] must be remediated within 90 calendar days.

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

- 6.3.6** Applications that require physical separation cannot be located in a cloud-based service.
- 6.3.7** 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.
- 6.3.8** The Company will notify Suppliers any time the Company's security standards are not met.

## **6.4 Server Security - System Hardening**

- 6.4.1** All production servers must be located in a secure, access-controlled location.
- 6.4.2** 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.
- 6.4.3** 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.

- 6.4.4** Test accounts and user accounts must be removed/revoked when no longer required.
- 6.4.5** Development and test systems must be isolated from the production environment and network.
- 6.4.6** All non-required ports and services on server operating systems and firewalls must be disabled.
- 6.4.7** 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.
- 6.4.8** Systems should have the ability to detect a potential attack. Examples include but are not limited to: Network Intrusion Detection (NID) or Host Intrusion Detection/Prevention (HID).
- 6.4.9** Applications that require physical separation cannot reside on the same host system.

## **6.5 Application Development**

- 6.5.1** The application and associated databases must:
  - Enforce security validation of all inputs.
  - 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.
  - Incorporate security controls, i.e., built-in access controls, security auditing features, fail-over features, etc.
  - Prevent buffer overflows.
  - Avoid arithmetic/algorithmic errors.
  - Must use non-production, simulated data in development.
  - Implement protocols (TCP/IP, TLS, etc.) and cryptographic modules without deviation from standards.

## **6.6 Security Reviews**

- 6.6.1** Web application vulnerability assessments must be performed during the application development and the deployment lifecycle.

**6.6.2** All third party software included in the application must meet all security requirements outlined herein.

**6.6.3** Secure interfaces for user login and user data input of Personal Data must utilize certificates signed by a trusted Certificate Authority (CA).

## **6.7 Security of System Files**

**6.7.1** Access to source code must be limited and controlled.

**6.7.2** During and after development, all applications must ensure the security of system files and access to source code and test data.

**6.7.3** All back-door, maintenance hooks must be removed from the application before production use.

**6.7.4** Application architecture must prohibit databases containing Company Data from residing on the same server as the application.

## **6.8 Application Availability**

**6.8.1** All applications must have defense measures to manage the risk from denial-of-service attacks.

**6.8.2** All applications should limit resources allocated to any user to the minimum necessary to perform the task.

**6.8.3** All applications must prevent unauthenticated users from accessing data or using vital system resources.

## **6.9 Network & Client Security**

**6.9.1** All client systems that access Company data, whether in use or not, must be physically secured.

**6.9.2** Patching of operating system and software security vulnerabilities to the must meet or exceed the service level interval defined by the vendor for the established threat level of the vulnerability.

**6.9.3** Client systems must have malware protection with automatic signature updates.

**6.9.4** Systems located in an unsecured area and attached to the Supplier network must not access systems and network segments containing Company data.

**6.9.5** Client systems which access Company data from secured locations must have a password protected screen saver or enforce idle session timeout after no more than 15 minutes. This includes any third-party vendors that may contract with those vendors.

## **6.10 Firewall Security**

**6.10.1** Network segments connected to the Internet must be protected by a firewall and configured to secure all devices behind it.

**6.10.2** All system security and event logs must be reviewed regularly for anomalies.

**6.10.3** Unused ports and protocols must be disabled.

**6.10.4** Firewalls must be configured to prevent address spoofing.

## **6.11 Privacy Management**

**6.11.1** All Supplier applications, such as "Software as a Service," used by the Company to collect Personal Data must have the URL for the Company's Website *Privacy Notice* embedded into the website, available in all languages.

**6.11.2** Where applicable, individuals must be given the opt-in choice to participate prior to providing their Personal Data. Opt-in selection forms must not be pre-selected by default.

**6.11.3** 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.

**6.11.4** Supplier's system must not transfer Personal Data to other systems or be used for purposes other than those specified.

**6.11.5** Supplier's system must have appropriate security controls to avoid unauthorized access, disclosure, and/or use or modification of individuals' Personal Data.

**6.11.6** Supplier's system must adhere to the [Federal Trade Commission's CAN-SPAM Act](#) if it:

1. Requests input of personal data from an individual to complete "Email to a Friend" notifications, or
2. The system offers online, subscription-based communication services.

## 6.12 Data Security

- 6.12.1** Appropriate security measures must be in place to address data handling, access requirements, data storage and communications.
- 6.12.2** Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.
- For data classified as "Company Confidential," "Company Internal" or "Company Restricted," data should be encrypted using AES-128 cipher strength or stronger.
- 6.12.3** To protect data integrity, data should be hashed using SHA-256 or a stronger hash algorithm.
- 6.12.4** All Company data which is captured in hard-copy that is no longer required must be physically destroyed by use of a cross-cut shredder.
- 6.12.5** Printer processes must be adequately secured to prevent unauthorized disclosure/access.
- 6.12.6** Extra precautions must be in place to protect any Company data stored on mobile devices. Mobile devices and resident data must be stored securely when not in use.
- 6.12.7** Websites and applications and underlying data must be backed up in accordance with Business Continuity and Disaster Recovery requirements.
- 6.12.8** The Supplier must secure any physical backup media during transportation and storage.
- 6.12.9** The Supplier should catalog all physical 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.
- 6.12.10** The Supplier should maintain system and application backups that support a total system restore for a 30-day period, as a minimum.
- 6.12.11** The Supplier must destroy all Company data within 30 days of termination of the Supplier's contract (unless the Agreement defines otherwise).

## 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.

## 8. Duration

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

## 9. References

- [Responsible Business Alliance](#)
- [Federal Trade Commission's CAN-SPAM Act](#)
- NIST [National Vulnerability Database Common Vulnerability Scoring System \(CVSS\) v.4.0](#)
- ISO/IEC 27001 International Standard
- [Trellix Code of Conduct / Skyhigh Security Code of Conduct](#)
- [Trellix Privacy Notice / Skyhigh Security Privacy Notice](#)
- [Trellix Legal Supplier Portal](#)
- [Skyhigh Security Legal Portal](#)
- [Trellix Technical & Organizational Measures / Skyhigh Security Technical & Organizational Measures](#)

## 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.

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

**EU Data Protection Laws:** EU GDPR and any regional or local data protection laws applicable in the European Economic Area and Switzerland (EEA) and/or EU member states.

**External Facing (Public):** Information generally made available or broadcast without approval or user authentication.

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

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

**Mission Critical:** Loss that directly impacts the Company's ability to book, build, ship, order, pay, close or communicate is considered mission critical.

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

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

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

**Company Data:** Company 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.