



Information Security Risk Management Policy

Table of Contents

1. Purpose	3
2. Scope	3
3. Target Audience	3
4. Roles and Responsibilities	3
5. Policy Statement and Compliance	5
5.1 Policy Statement	5
5.2 Compliance	5
5.3 Enforcement and Management	5
5.4 Monitoring and Review of Policy	5
5.5 Policy Approval	5
5.6 Exceptions	5
5.7 Document Location	5
6. Information Security Risk Management	6
7. Information Security Infrastructure	6
7.1 Management Support of Information Security	6
7.2 Information Security Organization	6
7.3 Risk Management Program	6
8. Risk Assessment and Vulnerability Scanning	7
8.1 Compliance and Security Reporting Metrics	7
8.2 Independent Audit of Information Systems	8
9. References	8
10. Definitions and Abbreviations	8
11. Revision History	9
12. Approvals	10

1. Purpose

The purpose of the *Information Security Risk Management Policy* is to define the framework for managing information security risks. This involves identifying, evaluating, assessing, and treating risks to ensure the confidentiality, integrity, and availability of information systems, assets, and infrastructure. This policy will align with all applicable industry-standards and best practices, including but not limited to, the International Standards Organization (ISO) 27001.

2. Scope

The scope of this policy pertains to all Musarubra LLC (which includes Trellix and Skyhigh Security and herein known as the "Company") information systems, data, and assets. Company senior management shall ensure that information systems and assets operated by, or on behalf of the Company, receive adequate security safeguards. This policy and any corresponding procedures, standards, and guidelines are intended to facilitate overall risk management activities for all of the Company systems and assets.

3. Target Audience

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

4. Roles and Responsibilities

Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is the company official responsible for developing and maintaining a company-wide information protection security program and has the following responsibilities for information protection security planning and implementation:

- Develops and maintains information protection security policies, procedures, and control techniques to address system security planning, necessary to identify and successfully manage, mitigate, or accept the enterprise risks to Company information, including business data, customer data, and intelligence data assets
- Manages the identification, implementation, and assessment of common security controls
- Ensures that personnel with significant responsibilities for system security plans are trained
- Assists senior company officials with their responsibilities for system security plans, and

- Identifies and coordinates common security controls for the company.

Information Security Governance, Risk, & Compliance (GRC)

- Establish a framework and program for measuring, managing, mitigating, and communicating information security risk across all lines of business and reporting to company executives on the information security posture of the company
- Lead the development of this policy to align with Company business objectives, risk tolerances, and industry best practices
- Develop awareness training and ensure that all Company personnel are trained regarding company information security policies and requirements
- Assess the risk of non-compliance to this policy and provide direction and guidance for risk remediation.

Company Management

Company management will support security initiatives by providing clear direction and visible commitment of adequate resources. Information security is a fundamental business responsibility shared by all members of the Company management team (inclusive of both Legal and HR). Management is responsible for:

- Promoting the visibility of business support for information security throughout the Company
- Appointing individuals to oversee and maintain an information security program
- Reviewing and collaborating on information security policy and standards
- Ensuring that security is part of the information planning process
- Supporting major initiatives to enhance the Company's information security
- Supporting organization-wide security initiatives (e.g., security awareness programs).

Company Personnel/Users

- Understand the purpose and intent of Company security policies, procedures, standards, and guidelines
- Perform work in compliance with these documents and in accordance with reasonable and customary security practices
- Identify and seek guidance from management and Information Security on suspected deviations from Company security policies, and
- Company personnel include business process owners (BPOs), and system and information owners (e.g. System Administrators).

Business Units

- Help define, understand, and formally acknowledge the security risks to their business
- Establish acceptable levels of risk tolerance in alignment with the risk management program, and
- Participate in risk mitigation activities that result in levels of operating risk acceptable to the organization.

5. Policy Statement and Compliance

5.1 Policy Statement

The Company shall ensure that all information systems, data, and assets operated by, or on behalf of the Company, maintain an acceptable level of risk with an overall strong security posture. The appropriate hardware, software, and procedural mechanisms shall be defined, developed, and implemented in support of a risk management program.

5.2 Compliance

All Company personnel are responsible for reading, understanding, and complying with this policy. Compliance with this policy is of the highest importance to the Company. Noncompliance can lead to serious legal, regulatory, and cost-control issues for the Company. Any violations of this policy shall be reported to the appropriate member of management. Company personnel who willfully violate or fail to comply with this policy may be subject to disciplinary action, up to and including revocation of access and/or termination from the Company.

5.3 Enforcement and Management

Company corporate management, represented by Information Security, will endorse, and enforce all Company security policies. Company security policies will be enforced for all Company information systems, data, and assets both internally and externally.

5.4 Monitoring and Review of Policy

The Company employs a continuous monitoring process to evaluate adequacy and effectiveness of policy and procedure requirements, and exercises continuous improvement as needed. This document will be evaluated at least annually to verify its current applicability and to determine if any changes are necessary.

5.5 Policy Approval

The CISO or assigned designee will be required to provide approval upon the review or revision of this policy.

5.6 Exceptions

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](#).

5.7 Document Location

The latest published version of this document is located on the [Policy Portal](#) intranet site.

6. Information Security Risk Management

The Company shall ensure that all information systems, assets, and resources operated by, or on behalf of the Company, maintain an acceptable level of risk with an overall strong security posture. The appropriate hardware, software, and procedural mechanisms shall be defined, developed, and implemented in support of a risk management program.

The Company's information security risk management approach leverages the ISO 27000 Risk Management Standard's approval, review, and control processes. The information security risk management approach and methodology are detailed in risk management procedures, standards, and guidelines documents.

Risk Management is administered by the Company's Information Security division and is the responsibility of the Company's Chief Information Security Officer (CISO).

7. Information Security Infrastructure

7.1 Management Support of Information Security

As listed above in the Roles and Responsibilities section, Company management will fully review, support, promote, and maintain the information security initiatives that are approved by the Chief Information Security Officer (CISO).

7.2 Information Security Organization

An information security program will be established and maintained to manage the implementation of information security policies and controls.

The Company's Information Security program is responsible for:

- Creating and enforcing information security policy and standards
- Ensuring that authorization regarding security of information and resources are defined and documented
- Monitoring changes in the risk exposure of the Company's information assets
- Monitoring and responding to information security incidents, and
- Managing security initiatives and projects.

7.3 Risk Management Program

The Information Security Risk Management program shall be established and maintained to manage the implementation and oversight of Information Security Risk Management policies and controls. Responsibilities under this program shall include:

- Creating and enforcing risk management policies, standards, and procedures
- Performing security risk assessments, investigations, and audits
- Monitoring changes in the risk exposure of the Company's information assets, and
- Managing security initiatives and projects.

8. Risk Assessment and Vulnerability Scanning

The Company will conduct assessment and vulnerability scanning on a regular basis.

These activities will include:

- Conducting risk assessments, including the likelihood and magnitude of harm (denoting "Critical", "High", "Moderate" or "Low" risk), from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits
- Addressing geographical/location specific risk factors where appropriate, and include geographical/location considerations in risk assessment and treatment results
- Documenting and disseminating risk assessment results in system security plans, risk assessment reports, or similar documentation
- Reviewing risk assessment results with asset owners and provide summaries to Information Security staff annually, or whenever a major change occurs within the information system
- Disseminating risk assessment results to appropriate personnel, and
- Updating the risk assessment at least annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security posture of the system.

Scanning activities include:

- Scanning for vulnerabilities in the information systems and hosted applications at least annually, and when new vulnerabilities potentially affecting the system/applications are identified and reported
- Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - a) Enumerating platforms, software flaws, and improper configurations, and
 - b) Measuring vulnerability impact
- Analyze vulnerability scan reports and results from security control assessments
- Work with stakeholders to ensure remediation of legitimate vulnerabilities in accordance with the Company's assessment of risk, and
- Share information obtained from the vulnerability scanning process and security control assessments with appropriate stakeholders to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

8.1 Compliance and Security Reporting Metrics

The Company will develop and use risk-based compliance and security metrics and update them continuously to highlight action plans and advise appropriate stakeholders on findings. Company information systems will be regularly checked for compliance with security implementation standards.

The Company shall maintain a security audit process and vulnerability assessment program for the continuous monitoring of security control effectiveness including the

potential need to change or supplement the control set, taking into account any proposed/actual changes to the information system or its operating environment.

The vulnerability scanning program will allow the Company to:

- Track the security state of information systems and assets on a continuous basis, and
- Maintain the security posture for systems and assets over time in a highly dynamic operating environment with changing threats, vulnerabilities, technologies, and missions/business processes.

The organization-wide continuous monitoring program shall include:

- Configuration management and control processes for organizational information systems
- Change management processes considering security impact on proposed or actual changes to information systems and environments
- Assessment of selected security controls based on the Company's defined continuous monitoring strategy
- Periodic security dashboards and reporting to appropriate Company executives, and
- Active involvement by system owners and Company executives in the ongoing management of information system-related security risks.

8.2 Independent Audit of Information Systems

The Company's information security policy implementation and operational system compliance shall be audited periodically by an independent organization or third party. Audits may be carried out by the Company's internal audit function, external auditors, or independent third parties. Such audits shall be planned to minimize disruptions to business processes and coordinated with the Company's Information Security.

9. References

None at this time.

10. Definitions and Abbreviations

Availability: Property of being accessible and usable upon demand by an authorized entity.

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Control:

A means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.

Note: Control is also used as a synonym for safeguard or countermeasure.

Integrity: Property of protecting the accuracy and completeness of assets.

Remediation: The act of correcting a vulnerability or eliminating a threat. The three primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting, and (3) removal of affected software.

System: A set of IT assets – hardware and software, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operating environment. When not used in this formal sense, the term is synonymous with the term "host." The context surrounding this word should make the definition clear or else should specify which definition is being used.

Vulnerability: Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the system components directly associated with the cardholder data environment or any other IT resources.

10. Revision History

VERSION	DATE PUBLISHED	PREPARED BY	CONTRIBUTORS	SUMMARY OF CHANGES
2.2	October 2025	Stephanie Lewis - GRC	Ailish Quinlan - GRC	Annual review and update.
2.1	March 2025	Stephanie Lewis - GRC	Ailish Quinlan - GRC	Policy signatory change.
2.0	August 2024	Stephanie Lewis - GRC	Ailish Quinlan - GRC	Annual review and update.
1.2	February 2024	Stephanie Lewis	Ailish Quinlan -	Additional information

		- GRC	GRC Scott Belliston - GRC	in section 8.
1.1	August 2023	Stephanie Lewis - GRC	Ailish Quinlan - GRC Clark Lovrien - GRC	Annual review and update.
1.0	August 2022	Stephanie Lewis - GRC	Ailish Quinlan - GRC Patrick McEnany - GRC	Initial publication.

11. Approvals

VERSION	DATE PUBLISHED	PREPARED BY	BUSINESS UNIT OWNER	APPROVER(S)
2.2	October 2025	Stephanie Lewis - GRC	OCISO - GRC	Michael Green - CISO
2.1	March 2025	Stephanie Lewis - GRC	OCISO - GRC	Clark Lovrien - Head of GRC
2.0	August 2024	Stephanie Lewis - GRC	OCISO - GRC	Harold Rivas - CISO
1.2	February 2024	Stephanie Lewis - GRC	OCISO - GRC	Harold Rivas - CISO
1.1	August 2023	Stephanie Lewis - GRC	OCISO - GRC	Harold Rivas - CISO
1.0	August 2022	Stephanie Lewis - GRC	OCISO - GRC	Howard Israel - vCISO