SECURITY SOLUTIONS
RISK MANAGED SECURITY ASSURED

Information Security Policy

Document Owner	Chief Security Officer
Date	Sep 29, 2025
Version	1.0
Document Classification	In-Confidence

Revision History

Version	Date	Author	Change Details
0.1	Sep 23, 2025	Ali Raza	Initial draft
0.2	Sep 29, 2025	Athar Awan	Revised version
1.0	Oct 06, 2025	Athar Awan/Ali Raza	Final version

Contents

Purpose

The purpose of this information security policy is to safeguard the confidentiality, integrity, and availability of the organization's information assets. This policy applies to all employees, contractors, vendors, and partners who have access to the organization's information assets. This is a high level policy, more information about the topics in this document can be found in the relevant policy linked.

Scope

This policy applies to all systems, assets, facilities, and data owned, leased, or managed by the organization. Specifically, this includes, but is not limited to:

- All employees, contractors, consultants, temporary staff, and any third party with authorized access to the organization's information assets.
- All corporate networks, hardware, and infrastructure.
- All information (electronic and physical) created, stored, processed, or transmitted by the organization, regardless of location (on-premise, cloud, or remote).

Roles and Responsibilities

Role	Responsibilities
IT Security Manager	●Oversight of the IT security policy and its enforcement. ●Regularly review and update the policy to address evolving security threats. ●Ensure that the security policy aligns with organizational goals and compliance standards.
Network Administrators	●Implement, manage, and monitor network security tools and protocols. ●Maintain and regularly update firewalls, intrusion detection systems, and anti-virus software. ●Report any security breaches or vulnerabilities to the IT Security Manager.
System Administrators	●Ensure operating systems and software are regularly updated with the latest security patches. ●Conduct routine security checks and audits on IT systems. ●Backup critical data and ensure effective disaster recovery processes are in place.
Application Developers	●Integrate security measures during the software development lifecycle. ●Regularly test applications for vulnerabilities and resolve any security issues. ●Stay updated on the latest security threats and trends related to software development.
End Users (Employees)	●Adhere to the guidelines and protocols outlined in the IT security policy. ●Regularly update and change passwords, following best practices. ●Report any suspicious activities or potential security threats to the IT department.
Help Desk & Technical Support	●Assist users with any IT security-related queries or concerns. ●Document and escalate any reported security incidents. ●Educate employees on basic IT security best practices.

Vendor Management Team	●Ensure third-party vendors comply with the organization's IT security standards. ●Regularly review vendor contracts for security clauses and requirements. ●Monitor and manage remote access provided to vendors, ensuring it is limited and secure.
Training & Development Team	●Design and facilitate IT security training programs for employees. ●Measure the effectiveness of training programs and adjust as needed.
Executive Management	●Provide the necessary support and resources for IT security initiatives. ●Stay informed about the organization's overall security posture and potential risks. ●Advocate for a culture of security awareness across the organization.

Information Classification

The organization's information assets must be classified based on their sensitivity and criticality. Information must be categorized as public, internal, confidential, and restricted, with appropriate security controls and handling procedures applied to each classification.

Definitions

- **Public:** Information that is intended for general public consumption and disclosure poses no risk to the organization (e.g., press releases, public website content).
- **Internal:** Information intended for use within the organization. Unauthorized disclosure would have a minimal adverse impact (e.g., internal memos, non-sensitive department procedures).
- **In-Confidience:** Information that is intended for restricted use by specific groups, departments, or individuals outside the organization like trusted vendor and partners. Unauthorized disclosure would have a moderate adverse impact on the organization, such as minor reputational damage or limited financial loss. Access to this information must be granted based on job function and should be protected by access controls.
- **Confidential:** Information that, if disclosed without authorization, could cause serious harm to the organization or its partners (e.g., financial forecasts, intellectual property, internal audit reports). Requires password protection and encryption for transfer.
- **Restricted:** Information that is legally protected or highly sensitive, requiring the highest level of security controls. Unauthorized disclosure could result in severe legal, regulatory, or financial consequences (e.g., Personal Identifiable Information (PII), payment card data, critical security findings). Access must be strictly logged and monitored.

Encryption and Network Security

Encryption must be used to protect sensitive information in transit and at rest. The organization must implement network security measures to protect against unauthorized access, including the use of firewalls, intrusion detection and prevention systems, and monitoring of network traffic.

For more information see:

- IT-01-01Firewall and Network Security Controls Policy
- IT-03-01 Cryptographic Controls Policy
- IT-11-01 Wireless Policy

Standard Configurations

The organization must establish standard configurations for all types of systems used within the organization. These configurations should include operating system settings, network settings, security settings, and other relevant configuration settings. These standard configurations must be based on industry best practices and regulatory requirements, as well as the organization's own business needs.

For more information see IT-02-01 System Configuration Standards

Data Retention

The organization must have a data retention policy that outlines how long different types of data must be kept and when it must be disposed of. This policy must take into account any legal or regulatory requirements for data retention and disposal, as well as the organization's own business needs.

For more information see IT-03-03 Data Retention and Disposal Policy

Web Application Security

The organization must have a web application security policy that outlines the procedures for designing, developing, and maintaining web applications to ensure their security. This includes conducting regular vulnerability assessments and penetration testing, implementing secure coding practices, and using secure protocols such as HTTPS to protect data in transit.

For more information see IT-06-01 Secure Development and Web Security Policy

Access Control

Access controls must be implemented to ensure that only authorized personnel have access to sensitive data. This includes the use of strong passwords, two-factor authentication, and access rights based on job responsibilities. Access must be granted on a need-to-know basis and must be revoked promptly when access is no longer required.

For more information see IT-07-01 Access Control Policy

Physical Security

Physical and environmental security controls must be implemented at all organizational facilities to protect information assets, systems, and personnel from unauthorized access, damage, or interference. This includes, but is not limited to:

- Controlling physical access to restricted areas (e.g., server rooms, data centers) using access control systems (key cards, biometric scans).
- Maintaining a formal visitor registration and escort process.
- Implementing surveillance and alarm systems in sensitive areas.
- Protecting equipment from environmental hazards (e.g., fire, flood, power loss).

For more information see IT-09-01 Physical Security Controls Policy.

Incident Response

A plan for responding to security incidents must be outlined, including the procedures for identifying and containing security breaches, and the process for reporting incidents to relevant authorities.

For more information see IT-12-11 Incident Response Plan

Acceptable Use

Employees must be aware of the acceptable use policy for the organization's information assets. Employees must also be trained on best practices for handling sensitive data and protecting against social engineering attacks.

For more information see IT-12-02 Acceptable Use Policy

Antimalware Controls

The organization must implement antimalware controls to protect its information assets from malware and other malicious software. This includes installing antimalware software on all organization-owned devices and performing regular scans and updates to ensure that the software remains effective. The software must be configured to automatically scan all incoming files and email attachments for viruses and other threats.

For more information see IT-05-01 Antimalware Policy

Event Logging and Monitoring

The organization must maintain logs of all significant events related to its information assets, including user access, system changes, and security incidents. These logs must be stored securely and monitored regularly to detect any suspicious activity. The organization must have a policy for reviewing and analyzing these logs and for responding to any security incidents that are identified.

The organization must implement monitoring controls to detect and respond to security incidents in a timely manner. This includes the use of intrusion detection and prevention systems, security information and event management (SIEM) tools, and other monitoring solutions. The policy must outline the procedures for reviewing and responding to alerts generated by these monitoring solutions and for conducting investigations when necessary.

For more information see IT-01-01 Firewall and Network Security Controls Policy and IT-10-01 Event Logging and Monitoring Policy

Compliance

The organization must comply with relevant regulatory and industry standards, including the Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and any other applicable data protection laws and regulations.

Enforcement

All personnel must comply with this policy. Non-compliance with this policy may result in disciplinary action, up to and including termination.

Any violations of this policy must be reported to the IT department immediately. The IT department will investigate all reported violations and take appropriate actions.

Review

This and other relevant information security policies must be reviewed at least once every 12 months and updated as needed to reflect changes to business objectives or risks to the environment.