SPROUTS®
FARMERS MARKET

INFORMATION SECURITY POLICY (ISP)

2025 v2.0

Classification Level: Internal

Last Updated: November 4, 2025

Table Of Contents

Version Control

Version Number	Date Updated	Author(s)	Description of Changes
1.0	10/21/2024	Christopher Rex	Policy Refresh: Initial draft
2.0	10/31/2025	Christopher Rex	Policy Refresh: Annual review

Review Schedule & Approvers

This policy should be annually reviewed and approved by the Senior Manager of IT Security Architecture and Operations, the Vice President of IT Operations and security, and the Chief Technology Officer.

Review Schedule	Approver Name and Role	2025 Version Status	Notes
Approved annually	**Christopher Rex** Senior Manager IT Security & Operations	Reviewed	Signed by: Christopher Rex CF6DF910D1214B4...
Approved annually	**Robert Vyslouzil** Vice President IT Operations & Security	Reviewed	DocuSigned by: Robert Vyslouzil DC7AFB7A1F834B3...

Update Instructions

The Knowledge Base Article Style Guide should be approved annually by the Knowledge Admin and the Enterprise Service Manager before the start of the new year. Once approved, follow the update checklist section below to publish or update the guide on the ServiceNow Knowledge Base. Archive older versions of the document on SharePoint. ServiceNow is the system of record for IT user guides, and SharePoint is used solely as a backup location.

Update Checklist

☐ Rename old Word & PDF copies using naming convention Old_ document name YYYY_V#.# (example: Old__2018_V1.3) archive old drafts.

☐ For minor updates that do not require approval, make edits without tracking changes. For major updates requiring approval, remove old signatures if applicable, turn on track changes, and then make your edits. See the Major Versus Minor updates section for more details.

☐ Remove unneeded fields and update fields highlighted yellow (title, classification level; see KB0014334, version number, headers, footers, title, authors/approvers/owners, dates, etc.). For the version number,

use the format YYYY v#.#. For minor changes, update 1.1 to 1.2, major changes 1.1 to 2.0, etc., and annual updates change the year and then reset the version to 1.0 (example: 2020 v1.0).

☐ For major updates, send the updated draft to any stakeholders for approval. Once all updates are made and the final draft is approved, click the Table of Contents bar, click update, select the update entire table radial button, and click OK. The new L1 to L2 sections will be added to the table.

☐ Check the spacing between sections of your document to ensure the sections didn't shift.

☐ Use Save As PDF to convert to PDF (not print to PDF). This will ensure the Word document Table of Contents & Navigation panel are automatically added when converting to PDF.

☐ From Adobe Pro go to File > Properties > Initial View. For Navigation, select the Bookmarks panel and page. For Page Layout, select Single Page Continuous, Magnification 100%, Window Options only check the box for the center window on the screen, and User Interface Options only check the box for Hide toolbars, then click OK. Go to File, then select Save.

☐ Update the existing article KB0014285, remove old attachments, and attach Word and PDF copies to the article. If no article exists, create a new article, attach the files, and publish.

☐ Save a copy of the updated version in Word and PDF format for your SharePoint page.

☐ Notify the Training team if any updates are needed for existing Sprouts Academy training simulations or request the creation of a new simulation. Notify Communications of any updates that must be communicated to all Sprouts team members or use the distribution lists for affected departments.

Major Vs. Minor Updates

- **Minor Changes** - simple changes to fix spelling, grammatical, and punctuation errors, minor defects, or modifying the wording in a way that does not change the meaning or interpretation of this guide.
- **Major Changes** - complex changes such as adding new rules or guidelines, fixing large defects, or modifying the wording to change the meaning or interpretation of this guide.

Communicating Updates

The Communications team communicates changes to this guide to Sprouts team members via electronic mail and/or another corporate communication method(s). Newly published and approved revisions supersede all previous versions.

Preventing Multiple Versions

Team members should only save copies of this guide in shared locations to prevent outdated versions from being accessed accidentally. You should always access this guide directly from the Sprouts Knowledge Base to ensure you have the most recent version of the document.

1 Introduction

1.1 Purpose of the Policy

This Information Security Policy aims to define the guiding principles and enforceable standards for managing and protecting Sprouts Farmers Market (SFM)'s information assets against all threats. This document serves as a directive for the entire company, establishing the security measures and behaviors required from all employees, contractors, and third-party users.

This policy is designed to:

- Articulate the commitment of SFM to information security and the expectations set upon all individuals with access to SFM's information systems.
- Protect SFM against potential security threats and breaches, ensuring operational integrity and the protection of sensitive data.
- Instill a culture of security awareness and compliance throughout the company, with clear guidelines on handling informational assets.
- Support SFM's strategic and operational objectives by integrating information security into core business processes.
- Provide a framework for establishing a secure environment for managing information, ensuring confidentiality, integrity, and data availability.
- Detail the responsibilities of all stakeholders in maintaining information security and the consequences of non-compliance.
- Guarantee that SFM's business activities comply with relevant laws, regulations, and contractual obligations regarding information security.

By adhering to this policy, SFM affirms its dedication to safeguarding its informational infrastructure and maintaining trust with clients, partners, and stakeholders.

1.2 Scope and Applicability

This Information Security Policy applies to all data, information, information systems, networks, applications, locations, and users of SFM or any third party acting on its behalf. It encompasses all forms of data, including but not limited to:

- Electronic data processed, stored, or transmitted via SFM's IT infrastructure,
- Physical data stored on SFM premises,
- Data that is managed by external entities on behalf of SFM.

The policy covers all SFM's business functions and locations, all employees (full-time, part-time, and temporary), contractors, suppliers, and others granted access to SFM's information systems and services. It extends to all forms of information processing that may impact the security of SFM's assets, including but not limited to:

- Development and maintenance of systems
- Processing and management of information
- Information sharing and communication
- Remote information processing
- Information storage and destruction

The requirements of this policy are mandatory, and by accessing the information or systems of SFM, all users agree to abide by the terms of this policy. Any breach of the Information Security Policy may result in action being taken, up to and including legal action or termination of employment or contracts.

This policy includes all subsidiary companies and business units within the SFM group unless such a unit has an existing and approved equivalent policy that meets or exceeds the requirements stated herein.

1.3 Information Statement

SFM is committed to protecting the confidentiality, integrity, and availability of all SFM's physical and electronic information assets to ensure that regulatory, operational, and contractual requirements are fulfilled.

The overarching goal of our Information Security Policy is to protect our information assets from all threats, whether internal or external, deliberate or accidental, to ensure our competitive edge, cash flow, profitability, legal, regulatory, contractual compliance, and commercial image.

SFM's information assets will be protected against unauthorized access and processing and follow all applicable laws and regulations. We will ensure that all our employees, contractors, and third-party users understand their responsibilities in protecting the security and privacy of information. This includes adhering to our Information Security Policy, compliance with our Information Security Program, and reporting suspected information security breaches.

We will continuously assess and mitigate risks to our information assets while striving to enhance our security measures and procedures. By doing so, SFM aims to ensure business continuity, minimize damage, and maximize return on investments and business opportunities.

The Information Security Policy is a core component of our commitment to high information security standards. It will be reviewed and updated regularly to meet the changing threat landscape and business requirements and to comply with all relevant statutory, regulatory, and contractual obligations.

1.4 Organizational Security

SFM's organizational security is a critical aspect that ensures the integrity, confidentiality, and availability of the company's information assets. This section delineates the security framework and the standards to which all activities involving SFM's information assets must align.

Framework and Structure

- SFM establishes an Information Security Management System (ISMS) that aligns with industry best practices and international information security standards.
- The ISMS framework specifies the roles, responsibilities, and authorities for all SFM employees and third-party users interacting with SFM information systems.
- An Information Security Officer (ISO) is appointed. The ISO governs the ISMS and reports directly to senior management.

Security Culture and Awareness

- SFM is dedicated to cultivating a security-aware culture through consistent training and communication programs that highlight the critical nature of information security.

- Mandatory information security awareness training is provided for all new hires, with regular updates and refresher sessions for all staff.

Incident Management and Reporting

- SFM implements a formal incident response process to manage and mitigate the impact of security incidents effectively.
- All staff and contracted personnel are duty-bound to report any suspected security incidents without delay to the designated authority within the SFM Support Desk.

Asset Management and Classification

- Information assets within SFM are categorized based on their sensitivity, importance, and criticality to the company's business functions.
- Each information asset is assigned an owner accountable for applying the appropriate level of security and managing access rights.

Security Controls and Measures

- SFM adopts comprehensive physical and logical security measures to protect information assets from unauthorized access and potential security threats.
- Security controls are regularly evaluated through assessments and audits to guarantee their adequacy and to address emerging risks.

Compliance and Legal Obligations

- SFM's information security practices align with all relevant legal, regulatory, and contractual obligations regarding data protection and information security.
- Regular reviews ensure that the security policies and practices are updated to meet these obligations.

Continuous Improvement

- SFM is engaged in an ongoing process of enhancing its information security measures.
- The ISMS is regularly reviewed against evolving cyber threats, audit findings, and external feedback to guide its continuous improvement process.

2 Information Security Program Overview

Mission

The mission of the Information Security Program is to protect SFM's information assets against all threats, be they internal or external, deliberate or accidental. The program ensures confidentiality, integrity, and availability of data, systems, and networks. This mission supports the broader goal of maintaining the trust of customers, partners, team members, and shareholders while complying with all legal and regulatory requirements.

As a publicly traded retail organization, there is a heightened responsibility to uphold the highest data security and integrity standards. This includes a specific focus on:

Comprehensive Data Protection: Implementing rigorous data protection measures and privacy practices to secure all sensitive data, including customer, shareholder, and team member information.

Regulatory Compliance and Reporting: Adhering to financial and data protection regulations relevant to publicly traded companies and the retail sector, such as the Sarbanes-Oxley Act and the Payment Card Industry Data Security Standard.

Employee Data Security: Prioritizing the security of team members' personal and professional data and acknowledging the importance of protecting employee information.

Retail Transaction Security: Safeguarding all retail transactions with advanced security technologies to prevent fraud and cyber threats.

Vendor and Supply Chain Security Management: Ensuring supply chain and vendor relationships meet stringent security standards to protect all data within SFM’s ecosystem.

Cybersecurity Awareness and Training: Promoting a culture of security awareness throughout SFM, emphasizing the critical role of everyone in maintaining information security.

Incident Response and Crisis Management: Establishing a robust incident response capability to manage security incidents and minimize their impact effectively.

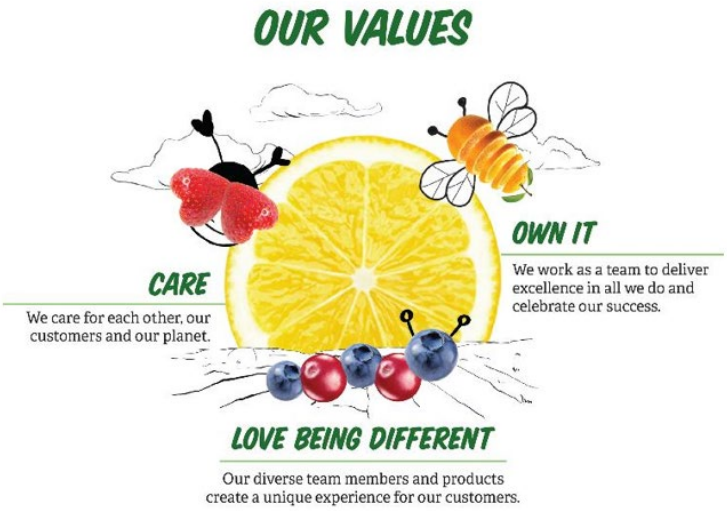
Innovation and Continuous Improvement: Continually evolving security measures to counter emerging threats, especially those targeting the retail sector, and integrating innovative solutions to strengthen SFM's security posture.

Transparent Stakeholder Communication: Engaging in open communication with all stakeholders regarding security initiatives, reinforcing the commitment to protecting all forms of data within SFM.

The Information Security Program is committed to a comprehensive approach to information security, safeguarding SFM's reputation and the trust placed by customers, team members, and shareholders in a dynamic and regulated retail environment.

Vision Statement

Our information security vision is to build a secure and trusted environment where **CARE** drives our responsibility to safeguard our team members, our customers, and the world we share. We take pride in our ability to **OWN IT,** delivering exceptional security through teamwork, accountability, and continuous improvement. With a passion for **LOVING FOR BEING DIFFERENT,** we embrace diverse ideas and innovative approaches to security, ensuring that our unique culture and solutions continue to provide a safe and trusted experience for all. The program is committed to fostering a secure digital environment that protects information assets and aligns with the principles of natural integrity and ethical business practices.



Fundamental aspirations of this vision include:

Excellence in Data Security and Privacy: Achieving a gold standard in protecting customer, shareholder, and employee data, blending rigorous security measures with a commitment to transparency and ethical data stewardship.

Innovative Cyber Resilience: Developing advanced cyber resilience frameworks tailored to address the unique challenges of the retail sector while reflecting a commitment to sustainable and responsible practices.

Security as a Reflection of Brand Values: Ensuring that the approach to information security mirrors the brand values of natural integrity and community engagement, particularly in how customer and employee data is protected and managed.

Leadership in Retail Security: Aspiring to be a globally recognized retail information security leader, setting data protection benchmarks and integrating security with customer-centric business practices.

Sustainable Security Practices: Embracing responsible and sustainable information security practices, reflecting SFM's broader commitment to making thoughtful and ethical choices.

Empowered Security Culture: Cultivating a culture where security awareness is integrated into the fabric of SFM, empowering each team member to contribute actively to the collective digital well-being.

Strategic Partnerships and Collaboration: Building strategic collaborations that enhance collective cybersecurity knowledge and defenses, benefiting from and contributing to the broader community.

Adaptation and Innovation: Continuously adapting and innovating security measures to meet emerging threats, particularly those targeting the retail sector, while aligning with SFM's core values.

Transparent and Responsible Communication: Engaging in transparent and responsible communication with all stakeholders about security initiatives, reinforcing the commitment to protect all forms of data within SFM.

This vision drives the Information Security Program towards a future where security practices safeguard digital assets and embody the values and aspirations of a leading publicly traded retail organization like Sprouts Farmers Market. This would ensure a harmonious balance between protecting information and upholding the principles of health, sustainability, and community trust.

3 Identify: Understanding SFM's Digital Landscape

This section mandates the identification of organizational resources and cybersecurity risks. It requires regular asset inventories, risk assessments, and the establishment of risk management strategies. All personnel must participate in identifying the critical assets and data, ensuring comprehensive risk awareness. This section sets the foundation for SFM's cybersecurity framework by emphasizing a proactive approach to understanding the cyber environment and its inherent risks.

3.1 Asset Management (ID.AM): Overview

Purpose:

This section establishes the foundational framework for inventory management and control of all organizational assets, which are critical to SFM's cybersecurity risk management strategy.

Scope:

This policy applies to all physical and digital assets, including hardware, software, and data owned, leased, or managed by SFM.

Policy Overview:

Asset management is essential for maintaining the integrity and security of organizational resources. This policy outlines the general principles and responsibilities critical for effective asset management. The "Information Security Standard" provides detailed guidelines and procedures.

Key Principles:

- **Inventory Management:**
  An accurate and up-to-date inventory of all organizational assets is required. This inventory should include type, location, owner, and status.
- **Access Control:**
  Access to all assets must be strictly controlled and limited to authorized personnel, as per the established access rights.
- **Audit and Compliance:**
  Regular audits must be conducted to ensure compliance with this policy and verify the accuracy of the asset inventory.
- **Incident Reporting:**
  Any discrepancies, losses, or unauthorized activities related to assets must be reported immediately and investigated according to the incident response guidelines outlined in the "Information Security Standard."

Roles and Responsibilities:

- **Executive Leadership Team (ELT):** This team provides strategic direction and oversight for asset management, ensuring alignment with SFM's strategic security vision and data governance policies.
- **IT - Information Security Architecture & Operations:** Responsible for designing and implementing the security architecture that protects these assets, managing the deployment of security solutions, and overseeing the daily operations of security systems.
- **Department / Team Managers:** Ensure that their teams understand and follow the asset management protocols as outlined, manage access rights within their teams, and ensure compliance with the asset management policy.
- **IT Infrastructure Team:** This team manages IT assets' physical and network security, ensuring that all infrastructure components comply with established security standards.

- **IT Security Compliance:** Monitors compliance with this asset management policy, facilitates audits, and ensures that the policy is up-to-date and in line with legal and regulatory requirements.

Reference to the Information Security Standard:

For comprehensive asset management procedures, including detailed operational guidelines, compliance requirements, and specific responsibilities, please refer to the "Information Security Standard" Section ID.AM-1 through ID.AM-5.

3.2 Business Environment (ID.BE): Overview

Purpose:

This section emphasizes aligning cybersecurity practices with SFM's mission, objectives, stakeholders, and activities, ensuring these elements are securely supported and enhanced through effective cybersecurity management.

Scope:

This policy applies to all organizational activities and any parties affected by SFM's operations, including internal and external stakeholders.

Policy Overview:

Understanding the relationship between SFM's activities and its cybersecurity posture is vital. This section sets out the fundamental principles that guide the integration of cybersecurity into business operations.

Key Principles:

- **Alignment with Organizational Goals:**
  Cybersecurity measures and practices must align with SFM's mission and business objectives to support and enhance operational effectiveness.
- **Regular Assessment:**
  Regular evaluations of cybersecurity implications on business operations are mandatory, ensuring that practices are up-to-date and effective.
- **Employee Awareness:**
  All employees must understand how their roles impact SFM's cybersecurity posture and the broader business context.

Roles and Responsibilities:

- **Executive Leadership Team (ELT):** Provides strategic vision and leadership in integrating cybersecurity with business goals, ensuring that security efforts are aligned with SFM's objectives and stakeholder expectations.
- **Department / Team Managers:** Communicate and enforce the business environment policy within their teams, ensuring all members understand their impact on SFM's cybersecurity posture.
- **IT - Information Security Architecture & Operations:** Develops and maintains systems that support the business environment's security requirements, ensuring these systems align with SFM's mission and objectives.
- **IT Security Compliance:** Ensures that the business environment policies comply with relevant laws and regulations, monitors compliance, and coordinates audits to assess the effectiveness of integrating cybersecurity within business operations.
- **Project Security Integration:** (Typically managed by a Project Manager or in a similar role under the guidance of the ELT) Ensures that all projects incorporate cybersecurity considerations, aligning project objectives with SFM's overall security posture.

Reference to the Information Security Standard:

For detailed guidelines on managing business environment aspects such as supply chain communication, critical

infrastructure identification, and prioritization of mission-critical activities, please refer to the "Information Security Standard" Section ID.BE-1 through ID.BE-5.

3.3 Governance (ID.GV): Overview

Purpose:

This section prescribes establishing a governance framework that aligns with SFM's policies, legal and regulatory requirements, and risk management strategies. It emphasizes defining clear cybersecurity roles and responsibilities, ensuring accountability, and fostering a culture of cybersecurity awareness across SFM.

Scope:

This policy applies to all employees, contractors, and third-party users of SFM's information systems and data.

Policy Overview:

The governance framework ensures that cybersecurity is integrated into organizational operations, supporting a structured approach to managing information security risks and compliance.

Key Principles:

- **Policy Establishment and Management:**
  A formal information security policy, developed under the leadership of the Chief Technology Officer (CTO), sets forth the guidelines for protecting SFM's information assets.
- **Role Coordination and Compliance:**
  Clearly defined and documented information security roles and responsibilities ensure alignment with SFM's structure and external partnerships.
- **Legal and Regulatory Compliance:**
  SFM commits to complying with all applicable legal, regulatory, and contractual cybersecurity, privacy, and civil liberties requirements.
- **Risk Management in Governance:**
  Cybersecurity risk management is integrated into the governance processes to ensure that decision-making at all levels accounts for cybersecurity risks.

Roles and Responsibilities:

- **Executive Leadership Team (ELT):** This team oversees the governance framework, ensuring it aligns with strategic objectives and incorporates comprehensive risk management strategies.
- **Chief Technology Officer (CTO):** Responsible for developing, implementing, and maintaining the information security policy and governance framework.
- **IT Security Compliance:** Monitors compliance with the governance policies, facilitates audits, and ensures alignment with legal and regulatory requirements.
- **Department / Team Managers:** Implement governance policies within their respective areas, ensuring their teams adhere to the guidelines and participate in training programs.
- **Project Security Integration:** Ensures that governance and risk management considerations are embedded in project management practices and that projects align with overall governance objectives.

Reference to the Information Security Standard:

For detailed governance procedures, including specific guidelines for role coordination, legal compliance, and risk management, please refer to the "Information Security Standard" Section ID.GV-1 through ID.GV-4.

3.4 Risk Assessment (ID.RA): Overview

Purpose:

This section mandates regular and comprehensive risk assessments to identify, document, and analyze cybersecurity risks affecting organizational operations, assets, and individuals. It evaluates the likelihood and impact of potential cybersecurity events to inform risk management decisions and strategies.

Scope:

This policy applies to all organizational assets and activities within SFM, covering all employees, contractors, and third-party users.

Policy Overview:

A structured risk assessment process is essential for understanding and mitigating threats to SFM's cybersecurity posture. This process includes systematic identification, prioritization, and management of cybersecurity risks.

Key Principles:

- **Vulnerability Identification and Documentation:**
  Regular identification and documentation of vulnerabilities in IT assets, utilizing tools and threat intelligence to maintain security.
- **Cyber Threat Intelligence and Information Sharing:**
  Active participation in information-sharing forums to enhance SFM's awareness and response to cyber threats.
- **Threat Identification and Documentation:**
  Continuous identification and documentation of internal and external threats, employing various monitoring tools and analysis techniques.
- **Business Impact and Likelihood Assessment:**
  Evaluate potential business impacts and likelihoods of cybersecurity events to prioritize risk management efforts.
- **Comprehensive Risk Determination:**
  Integration of threat analysis, vulnerability data, impact assessments, and likelihood evaluations to determine overall cybersecurity risks.

Roles and Responsibilities:

- **Chief Technology Officer (CTO) or Executive Leadership Team (ELT):**
  Oversees the strategic direction of the risk assessment process, ensuring alignment with organizational goals and compliance with legal and regulatory standards.
- **IT - Information Security Architecture & Operations:**
  Implements and manages the tools and processes for identifying and documenting vulnerabilities and threats. Also responsible for the continuous monitoring of organizational assets.
- **IT Security Compliance:**
  Monitors adherence to risk assessment policies ensures compliance with legal and regulatory requirements and facilitates audits.
- **Department / Team Managers:**
  Ensure that their respective teams understand and comply with the risk assessment processes and participate actively in identifying and reporting potential risks.
- **Project Security Integration:**
  Integrates risk assessment processes into project management to ensure that all projects consider potential cybersecurity risks from the onset.

Reference to the Information Security Standard:

For detailed risk assessment procedures, including specific guidelines for vulnerability management, threat intelligence, and risk prioritization, please refer to the "Information Security Standard," Section ID.RA-1 through ID.RA-6.

3.5 Risk Management Strategy (ID.RM): Overview

Purpose:

This section mandates developing and implementing a comprehensive risk management plan that includes establishing risk tolerance thresholds, prioritizing risk mitigation activities, and ensuring cybersecurity risk management processes are integrated with SFM's overall risk management practices. It emphasizes the need for regular reviews and updates to adapt to the evolving cybersecurity landscape.

Scope:

This policy applies to all risk management activities across SFM, involving all departments, units, and personnel.

Policy Overview:

A proactive and dynamic risk management strategy is crucial for safeguarding SFM's operations and assets from cybersecurity threats. This strategy involves a systematic risk management approach, including assessment, mitigation, and monitoring.

Key Principles:

- **Risk Management Processes:**
  Develop, document, and maintain comprehensive risk management processes that identify, assess, mitigate, and monitor cybersecurity risks.
- **Organizational Risk Tolerance:**
  Determine and clearly express SFM's tolerance for cybersecurity risks, ensuring alignment with SFM's strategic business objectives.
- **Sector-Specific Risk Analysis:**
  Conduct sector-specific risk analyses to understand and manage risks unique to SFM's role in critical infrastructure.

Roles and Responsibilities:

- **Executive Leadership Team (ELT):**
  Provides strategic oversight and ensures the risk management strategy aligns with organizational goals and regulatory requirements.
- **Chief Technology Officer (CTO) or Risk Management Officer:**
  Leads the development and implementation of the risk management plan, overseeing the establishment of risk tolerance levels and integration of risk management into business processes.
- **IT - Information Security Architecture & Operations:**
  Implements risk management tools and processes, conducts regular risk assessments, and continuously monitors cybersecurity threats.
- **IT Security Compliance:**
  Monitors compliance with risk management policies facilitates audits and ensures adherence to legal and regulatory standards.
- **Department / Team Managers:**
  Implement risk management processes within their respective areas, ensuring their teams adhere to the established risk tolerance and participate in risk mitigation activities.

- **Project Security Integration:**
  Ensures that risk management considerations are integrated into project management and that all projects address relevant cybersecurity risks.

Reference to the Information Security Standard:

For detailed risk management procedures, including specific guidelines for managing risk processes, determining risk tolerance, and conducting sector-specific risk analyses, please refer to the "Information Security Standard," Sections ID.RM-1 through ID.RM-3.

3.6 Supply Chain Risk Management (ID.SC): Overview

Purpose:

This section addresses the management of cybersecurity risks associated with the supply chain. It mandates implementing security measures for managing these risks related to suppliers and third-party partners. Policies should ensure due diligence, establish contractual obligations, and maintain ongoing monitoring of supply chain cybersecurity risks.

Scope:

This policy applies to all activities related to managing risks in SFM's cyber supply chain, encompassing interactions with all suppliers and third-party service providers.

Policy Overview:

Effective supply chain risk management is crucial for maintaining the integrity of SFM's cybersecurity standards across all external partnerships. This approach includes systematic risk assessments, integration of security requirements into contracts, and continuous compliance monitoring.

Key Principles:

- **Cyber Supply Chain Risk Management Processes:**
  Develop comprehensive risk management processes, including risk identification, assessment, mitigation, monitoring, and stakeholder engagement.
- **Supply Chain Risk Assessment for Suppliers and Partners:**
  Identify, prioritize, and assess cyber supply chain risks associated with suppliers and partners, integrating risk assessment processes into procurement.
- **Supplier and Partner Security Requirements in Contracts:**
  Ensure all suppliers and partners are contractually obligated to meet specified security requirements aligning with SFM's objectives.
- **Monitoring of Suppliers and Partners:**
  Establish procedures for ongoing monitoring to ensure suppliers and partners fulfill their cybersecurity obligations.
- **Response and Recovery Planning and Testing with Critical Suppliers:**
  Collaborate with critical suppliers to develop and test response and recovery plans for cybersecurity incidents.

Roles and Responsibilities:

- **Executive Leadership Team (ELT):**
  Provides strategic oversight and ensures supply chain risk management aligns with SFM's overall risk management strategy.

- **Chief Technology Officer (CTO) or Chief Risk Officer:**
  Oversees the development of supply chain risk management policies and integration of these policies with other risk management activities.
- **IT - Information Security Architecture & Operations:**
  Supports the implementation of technical measures and monitoring tools for managing supply chain risks.
- **Procurement and Legal Departments:**
  Work together to integrate cybersecurity requirements into supplier contracts and manage the ongoing compliance of these contracts.
- **IT Security Compliance:**
  Monitors the compliance of supply chain risk management policies and facilitates audits of suppliers and third-party service providers.
- **Department / Team Managers:**
  Ensure their teams adhere to supply chain risk management processes and participate in risk assessments and monitoring activities.

Reference to the Information Security Standard:

For detailed supply chain risk management procedures, including specific guidelines for risk assessment, contractual security requirements, and monitoring strategies, please refer to the "Information Security Standard" Section ID.SC-1 through ID.SC-5.

4 Protect: Safeguarding SFM's Digital Assets

The Protect section dictates the implementation of appropriate safeguards to ensure the delivery of critical services. It encompasses access control policies, ensuring only authorized individuals can access sensitive data and systems. This includes employing minimum necessary access principles, robust authentication methods, and ongoing employee training on data protection practices. The section also prescribes measures for maintaining data integrity and confidentiality, outlining specific protocols for data encryption, backup, and secure data handling.

4.1 Identity Management and Access Control (PR.AC): Overview

Purpose:

This sub-section mandates the implementation of robust identity management and access control measures. It requires assigning access rights based on role-based access control (RBAC), least privilege, and separation of duties principles. Access permissions must be regularly reviewed and updated. The policy also dictates robust authentication methods and the management of user identities, credentials, and privileges to ensure that only authorized individuals can access sensitive systems and data.

Scope:

This policy applies to all systems, networks, and processes within SFM that require identity verification and authentication, covering all employees, contractors, and third-party users.

Policy Overview:

Effective identity management and access control are critical for protecting SFM's information assets from unauthorized access and breaches. This approach includes credential management, physical access management, remote access management, and the management of access permissions and authorizations.

Key Principles:

- **Identity and Credential Management:**
  Implement and maintain processes for issuing, managing, revoking, and auditing identities and credentials for all authorized entities.
- **Physical Access Management and Protection:**
  Establish and enforce controls to manage and protect physical access to SFM's assets.
- **Remote Access Management:**
  Define and enforce the management of remote access to ensure secure and controlled access to SFM's networks and systems.
- **Management of Access Permissions and Authorizations:**
  Establish guidelines for managing access permissions and authorizations to ensure adherence to the principles of least privilege and separation of duties.
- **Network Integrity and Segregation:**
  Implement measures to protect the integrity of the network and employ network segregation where necessary.
- **Identity Proofing and Credential Binding:**
  Establish procedures for proofing identities and binding them securely to credentials.
- **Risk-Based Authentication:**
  Apply risk-based authentication strategies to authenticate users, devices, and assets commensurate with the level of risk.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversees the overall strategy and implementation of identity management and access control policies.
- **IT Security Compliance:**
  Ensures compliance with identity management and access control policies, conducts regular audits, and facilitates necessary adjustments to meet policy standards.
- **IT - Information Security Architecture & Operations:**
  Responsible for the technical implementation of identity and access control systems, managing credential lifecycle processes, and ensuring secure authentication and authorization mechanisms.
- **Department / Team Managers:**
  Ensure their teams comply with identity management and access control policies, particularly in managing physical and remote access.
- **Human Resources:**
  Collaborates with IT to manage the provisioning and de-provisioning of access as part of the employee onboarding and termination processes.
- **Facilities Management:**
  Manages physical access controls to secure facilities and monitors physical access logs.

Reference to the Information Security Standard:

For detailed identity management and access control procedures, including specific guidelines for credential management, physical and remote access management, and the application of access controls, please refer to the "Information Security Standard" Section PR.AC-1 through PR.AC-7.

4.2 Awareness and Training (PR.AT): Overview

Purpose:

This sub-section prescribes ongoing cybersecurity awareness programs for all personnel. It requires training initiatives

that cover cybersecurity policies, acceptable use policies, and specific security procedures relevant to employee roles. This approach aims to foster a culture of cybersecurity awareness and reduce risk through educated behaviors and practices.

Scope:

This policy applies to all employees, contractors, and others who access or use SFM's information systems and networks.

Policy Overview:

Cybersecurity awareness and training are critical for ensuring all personnel have the knowledge and skills to protect themselves and SFM from cyber threats. This policy outlines the requirements for comprehensive training programs and regular updates to training content.

Key Principles:

- **User Information and Training:**
  Conduct regular training sessions and awareness programs to inform all users about evolving cybersecurity threats and organizational policy and procedure updates.
- **Understanding of Roles and Responsibilities by Privileged Users:**
  Provide detailed role-specific training to privileged users to emphasize their critical role in maintaining information security.
- **Third-Party Stakeholder Roles and Responsibilities:**
  Ensure all third-party stakeholders understand their information security responsibilities and receive appropriate training.
- **Senior Executive Roles and Responsibilities:**
  Engage senior executives in cybersecurity training and regular briefings to ensure they know their specific roles in upholding SFM's cybersecurity strategies.
- **Roles and Responsibilities of Security Personnel:**
  Deliver role-specific training and ongoing professional development to security personnel to ensure they can effectively manage and respond to cybersecurity incidents.

Roles and Responsibilities:

- **Human Resources (HR):**
  Collaborates with the IT department to integrate cybersecurity training into all employees' orientation and ongoing education programs.
- **VP - Information Security:**
  Oversees developing and implementing cybersecurity training programs, ensuring they align with the latest security practices and threat intelligence.
- **IT Security Compliance:**
  Monitors the effectiveness of training programs and compliance with cybersecurity education requirements.
- **Department / Team Managers:**
  Ensure their team members complete required training sessions and understand their security responsibilities.
- **Procurement and Vendor Management:**
  Manage the inclusion of security training requirements in contracts with third parties and monitor their compliance.

Reference to the Information Security Standard:

For detailed awareness and training procedures, including specific guidelines for user training, roles and responsibilities for privileged users, and engagement of senior executives, please refer to the "Information Security Standard" Section PR.AT-1 through PR.AT-5.

4.3 Data Security (PR.DS): Overview

Purpose:

This sub-section focuses on protecting data at rest, in transit, and during processing. It mandates the use of encryption, data masking, and other appropriate measures to ensure the confidentiality and integrity of data. The policy requires regular backups, data loss prevention strategies, and controls against data leakage to safeguard critical information against unauthorized access and incidents.

Scope:

This policy applies to all forms of data within SFM, including electronic data stored on all systems, transmitted over networks, or processed in any form.

Policy Overview:

Data security is a critical component of SFM's overall cybersecurity strategy. This section outlines the requirements for robust data protection measures across various data states and interactions.

Key Principles:

- **Protection of Data-at-Rest:**
  Implement stringent security controls, including encryption and access controls, to protect data stored on organizational systems and devices.
- **Protection of Data-in-Transit:**
  Secure data during transmission with strong encryption protocols to prevent interception and unauthorized access.
- **Asset Management during Removal, Transfers, and Disposition:**
  Manage the lifecycle of data-bearing assets to ensure data is securely erased or destroyed when assets are repurposed, transferred, or disposed of.
- **Capacity and Availability Management:**
  Ensure sufficient system capacity and availability to maintain data integrity and accessibility, including during peak usage times and after incidents.
- **Protection Against Data Leaks:**
  Implement comprehensive data loss prevention (DLP) strategies to detect and prevent unauthorized data exposures and leaks.
- **Integrity Checking for Software, Firmware, and Information:**
  Use integrity-checking mechanisms to verify the authenticity and integrity of critical software, firmware, and data.
- **Separation of Development, Testing, and Production Environments:**
  Maintain strict separation between development, testing, and production environments to protect the integrity of data and systems.
- **Hardware Integrity Verification:**
  Implement integrity verification measures to secure hardware components from tampering and unauthorized modifications.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversees the implementation and compliance of data security policies and strategies across SFM.

- **IT Security Compliance:**
  Monitors compliance with data security policies facilitates audits and implements corrective measures where necessary.
- **IT - Information Security Architecture & Operations:**
  Responsible for implementing technical data security measures, managing encryption practices, and ensuring secure data transmission and storage.
- **Department / Team Managers:**
  Ensure their departments comply with data security policies, particularly in handling and securing data within their specific operational areas.
- **Human Resources:**
  Manages the training programs related to data security, ensuring all employees understand their responsibilities in protecting data.
- **Facilities Management:**
  Oversees the physical security measures that support data security, particularly in managing access to data storage areas.

Reference to the Information Security Standard:

For detailed data security procedures, including specific guidelines for encryption, data masking, data anonymization, data leakage prevention, and integrity checking, please refer to the "Information Security Standard" Section PR.DS-1 through PR.DS-8.

4.4 Information Protection Processes and Procedures (PR.IP): Overview

Purpose:

This sub-section requires the maintenance of security policies that address the information systems and data lifecycle. This includes implementing secure development practices, change management processes, and measures to protect against data destruction or manipulation. Regular reviews and updates to these processes are mandatory to adapt to evolving cybersecurity challenges.

Scope:

This policy covers all information systems and data managed within SFM, covering their development, maintenance, and disposal.

Policy Overview:

Information protection processes and procedures are essential for ensuring the integrity, confidentiality, and availability of information systems and data throughout their lifecycle.

Key Principles:

- **Baseline Configuration Management:**
  Maintain and manage baseline configurations for all IT and control systems to ensure operational security and compliance.
- **System Development Life Cycle (SDLC) Management:**
  Integrate security throughout the SDLC, from system planning to disposal, to ensure that systems are designed, developed, and maintained securely.
- **Configuration Change Control:**
  Implement stringent change control processes to manage and record all material changes to system configurations and software to prevent unauthorized alterations.

- **Backup and Recovery:**
  Conduct, maintain, and test backups of essential data and systems to ensure rapid recovery and continuity in case of data loss or system failure.
- **Physical Operating Environment for Organizational Assets:**
  Secure the physical environments where critical systems and data are housed to prevent unauthorized access and environmental hazards.
- **Data Destruction:**
  Ensure secure destruction of data and hardware to prevent unauthorized data recovery when no longer needed.
- **Continuous Improvement of Protection Processes:**
  Continuously improve security practices to address new threats and adapt to technological advancements.
- **Sharing Effectiveness of Protection Technologies:**
  Share lessons learned and the effectiveness of security technologies with relevant stakeholders to improve collective security postures.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversees the overall strategy and implementation of information protection processes and ensures compliance with policies across SFM.
- **IT Security Compliance:**
  Monitors the adherence to these policies, conducts audits, and coordinates with other departments to ensure effective implementation of the security measures.
- **IT - Information Security Architecture & Operations:**
  Implements security controls, manages system configurations, and ensures secure development practices are followed throughout the SDLC.
- **Department / Team Managers:**
  Ensures that their teams adhere to the security processes and procedures, particularly in handling data and managing system changes.
- **Human Resources:**
  Collaborates to incorporate security awareness and training programs addressing these policies for all employees.

Reference to the Information Security Standard:

For detailed procedures on baseline configuration, SDLC management, change control, and other protection processes, please refer to the "Information Security Standard" Section PR.IP-1 through PR.IP-12.

4.5 Maintenance (PR.MA): Overview

Purpose:

This sub-section mandates the timely maintenance of information system components, including regular software updates, patch management, and hardware servicing. It emphasizes using authorized and secure tools and procedures for maintenance activities to ensure system integrity and prevent unauthorized access.

Scope:

This policy applies to all maintenance activities related to hardware, software, and network components owned, operated, or managed by SFM.

Policy Overview:

Ensuring the proper maintenance of information systems is crucial for addressing vulnerabilities, enhancing system performance, and maintaining overall security and operational efficiency.

Key Principles:

- **Maintenance and Repair of Organizational Assets:**
  Conduct all maintenance and repair activities using approved tools and procedures. Log and document all activities and ensure third-party involvement complies with organizational security standards.
- **Remote Maintenance of Organizational Assets:**
  Securely manage remote maintenance activities, ensuring they are performed using approved tools, are fully logged, and conducted under strict access controls.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversees and ensures the compliance of the maintenance policy across SFM, including the security of maintenance operations.
- **IT - Information Security Architecture & Operations:**
  Responsible for implementing maintenance procedures, scheduling regular updates and patches, and ensuring secure configuration management.
- **IT Infrastructure Team:**
  Manages IT infrastructure maintenance's physical and hardware aspects, including the secure handling and servicing of IT assets.
- **IT Security Compliance:**
  Monitors compliance with the maintenance policy, conducts audits, and ensures all maintenance activities are logged and documented.
- **Vendor and Third-Party Management:**
  Ensures that external service providers adhere to SFM's security requirements for maintenance activities, including remote maintenance.

Reference to the Information Security Standard:

For detailed maintenance procedures, including specific guidelines for handling updates, patches, and emergency repairs, please refer to the "Information Security Standard" Section PR.MA-1 and PR.MA-2.

4.6 Protective Technology (PR.PT): Overview

Purpose:

This sub-section prescribes appropriate technologies and architectural designs to protect organizational assets. It mandates the deployment of firewalls, intrusion prevention systems, secure configurations, endpoint protection solutions, and controls to secure mobile devices, remote access, and the use of external information systems.

Scope:

This policy applies to all protective technology measures implemented within SFM to safeguard information systems and networks from unauthorized access, use, disclosure, disruption, modification, or destruction.

Policy Overview:

Protective technologies play a crucial role in defending against cyber threats and ensuring the integrity and availability of organizational assets.

Key Principles:

- **Audit and Logging Management:**
  Implement comprehensive mechanisms for logging and monitoring activities across all systems and networks to ensure adequate oversight and security incident analysis.
- **Removable Media Management:**
  Securely manage the use and handling of all forms of removable media within SFM.
- **Implementation of the Principle of Least Functionality:**
  Configure systems to operate with only the essential capabilities required for their intended use.
- **Protection of Communications and Control Networks:**
  Secure all communication lines and control networks to prevent unauthorized access and ensure data integrity in transit.
- **Management of System Functional States:**
  Define and manage different functional system states to ensure their availability and reliability under various conditions.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversees the overall implementation of protective technology policies and ensures compliance with all related standards.
- **IT - Information Security Architecture & Operations:**
  Responsible for deploying and managing firewalls, intrusion prevention systems, and other security measures. Manages audit and logging mechanisms across all IT systems.
- **IT Infrastructure Team:**
  Manages the physical infrastructure and ensures the implementation of secure network architectures and the protection of communication networks.
- **IT Security Compliance:**
  Monitors adherence to protective technology policies, conducts regular audits, and ensures all activities follow legal and regulatory standards.
- **Vendor and Third-Party Management:**
  Oversees third-party vendors that provide technology solutions or services, ensuring they meet SFM's security requirements, especially in managing removable media and remote maintenance.

Reference to the Information Security Standard:

Please refer to the "Information Security Standard," Sections PR.PT-1 through PR.PT-5 for detailed procedures and guidelines on implementing and managing protective technologies.

5 Detect: Vigilance in SFM's Monitoring and Detection Efforts

This policy section prescribes continuous monitoring to detect cybersecurity events promptly. It mandates deploying detection systems such as intrusion detection systems (IDS), regular system and network scans, and real-time alerts for suspicious activities. Employees are required to report anomalies, and IT teams must conduct regular audits to ensure the effectiveness of detection tools and procedures. This section is crucial for the early identification of potential security incidents, reducing the window of opportunity for cyber threats.

5.1 Anomalies and Events (DE.AE): Overview

Purpose:

This sub-section focuses on continuously monitoring network and system activities to detect anomalies, events, or signs

of potential cybersecurity incidents. It mandates using detection systems, such as intrusion detection systems (IDS) and security information and event management (SIEM) solutions.

Scope:

This policy applies to all systems, networks, and data flows within SFM and aims to promptly detect, analyze, and respond to potential security events.

Policy Overview:

Effective detection and analysis of anomalies and events are crucial for the early identification and mitigation of potential cybersecurity threats.

Key Principles:

- **Network Operations and Data Flow Baseline:**
  Establish a comprehensive baseline of normal operations and expected data flows to identify deviations that may indicate security incidents.
- **Event Analysis and Understanding Attack Methods:**
  Develop procedures to analyze detected events comprehensively, enhancing understanding of potential attack vectors and tactics.
- **Aggregation and Correlation of Event Data:**
  Aggregate and correlate data from multiple security systems and tools to improve detection capabilities and threat analysis.
- **Determination of Event Impact:**
  Assess the potential impact of security events on operations and SFM's overall security posture.
- **Incident Alert Thresholds:**
  Define and implement thresholds for security alerts to facilitate timely responses to potential incidents.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversees the overall strategy and implementation of anomaly and event detection systems and policies.
- **IT - Information Security Architecture & Operations:**
  Manages the deployment and operation of IDS, SIEM, and other detection tools. Responsible for setting up and updating the network operations baseline.
- **IT Security Compliance:**
  Conducts regular audits to ensure effective monitoring practices and compliance with established policies.
- **Computer Security Incident Response Team:**
  Analyzes detected events to determine their nature and potential impact and coordinates response actions.
- **Data Analysts and Network Engineers:**
  Involved in continuously analyzing network data, identifying anomalies, and maintaining data flow baselines.

Reference to the Information Security Standard:

For detailed procedures and guidelines on monitoring and responding to anomalies and events, please refer to the "Information Security Standard," Sections DE.AE-1 through DE.AE-5.

5.2 Security Continuous Monitoring (DE.CM): Overview

Purpose:

Establish a robust monitoring strategy that encompasses all aspects of network traffic, user activities, system configurations, and the physical environment, ensuring timely identification and management of potential security risks.

Scope:

This policy applies to all digital and physical monitoring systems and tools SFM utilizes to ensure the integrity and security of its network and physical environments.

Policy Overview:

A comprehensive monitoring strategy is essential for the early detection of potential security incidents and for maintaining SFM's overall cybersecurity posture.

Key Principles:

- **Network Monitoring for Cybersecurity Events:**
  Utilize advanced network monitoring tools to continuously detect unusual activities and potential cybersecurity threats.
- **Physical Environment Monitoring for Cybersecurity:**
  Implement physical monitoring systems to detect and respond to activities that could impact cybersecurity.
- **Monitoring of Personnel Activity:**
  Observe and analyze personnel activity to ensure compliance with security policies and detect malicious or unauthorized actions.
- **Detection of Malicious Code:**
  Employ systems and procedures to detect the presence of malicious code across SFM's networks and devices.
- **Detection of Unauthorized Mobile Code:**
  Implement measures to detect and manage unauthorized mobile code to prevent security breaches.
- **Monitoring External Service Provider Activity:**
  Monitor the activities of external service providers to ensure that their actions do not compromise the security of organizational data and systems.
- **Monitoring for Unauthorized Access and Use:**
  To prevent potential security incidents, unauthorized access and use of SFM's information systems must be detected.
- **Vulnerability Scanning:**
  Regular vulnerability scans must be conducted to identify and address security weaknesses within SFM’s systems and networks.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversee the strategy and policy implementation for security monitoring across SFM.
- **Manager - IT Security Architecture & Operations:**
  Manage day-to-day security operations, including overseeing network monitoring, detecting malicious or unauthorized activities, and coordinating responses to security events.
- **Physical Security Manager:**
  Oversee the monitoring of physical spaces to prevent unauthorized access and ensure the physical security of critical infrastructures.
- **Network Security Analysts:**
  Conduct real-time analysis of network traffic to identify and respond to security threats.
- **Systems Administrators:**
  Manage system configurations and conduct regular reviews to ensure all systems operate within defined security parameters.

- **External Vendor Security Coordinator:**
  Monitor and manage security-related activities of external service providers to ensure compliance with organizational security standards.
- **IT Compliance Manager:**
  Ensure all monitoring activities comply with legal, regulatory, and ethical standards, focusing on privacy and data protection.

Reference to the Information Security Standard:

For more detailed procedures and guidelines on continuous monitoring, please refer to the "Information Security Standard," Sections DE.CM-1 through DE.CM-8.

5.3 Detection Processes (DE.DP): Overview

Purpose:

To establish and maintain robust detection processes that effectively identify cybersecurity threats and events within SFM, ensuring SFM's ability to swiftly respond to and mitigate potential security incidents.

Scope:

This policy applies to all detection activities and systems used across SFM to identify cybersecurity events, encompassing the tools, personnel, and processes involved in detecting anomalies and security threats.

Policy Overview:

Regular testing, updating of detection systems, and comprehensive documentation are critical to maintaining the effectiveness of detection processes against evolving cyber threats. Continuous training is essential to update all relevant personnel on the latest detection techniques and threat intelligence.

Key Principles:

- **Definition of Roles and Responsibilities for Detection:**
  Delineate roles and responsibilities for detecting cybersecurity events, ensuring all personnel understand their duties.
- **Compliance in Detection Activities:**
  To ensure ethical and legal integrity, all detection activities must comply with legal, regulatory, and organizational standards.
- **Testing of Detection Processes:**
  Regularly test detection systems and processes to confirm their effectiveness and readiness to identify cybersecurity events accurately.
- **Communication of Event Detection Information:**
  Ensure that information regarding detected cybersecurity events is communicated efficiently and effectively to facilitate timely responses.
- **Continuous Improvement of Detection Processes:**
  Foster an environment of continuous improvement to enhance the detection capabilities through feedback, testing, and adoption of advanced technologies.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversee the overall strategy for cybersecurity event detection, ensuring integration with SFM's broader security policies and incident response efforts.

- **Security Operations Team:**
  Responsible for the operational management of detection tools and systems, conducting real-time analysis of network traffic and alerts to identify potential security incidents.
- **IT Compliance Manager:**
  Ensure detection activities comply with all applicable regulations and organizational policies, mainly on data privacy and ethical considerations.
- **IT Security Analysts:**
  Perform detailed analyses of detected events to determine the nature, extent, and potential impact of security threats.
- **System Administrators:**
  Implement and maintain the technical infrastructure supporting detection activities, including updates and patches to detection systems.
- **Human Resources:**
  Coordinate training programs for all Team Members regarding detection techniques and policies, ensuring staff know the latest cybersecurity threats and detection strategies.
- **External Security Consultants:**
  Engage with external experts to review and enhance detection strategies, providing insights into industry trends and emerging threat vectors.

Reference to the Information Security Standard:

For more detailed procedures and guidelines on detection processes, please refer to the "Information Security Standard," Sections DE.DP-1 through DE.DP-5.

6 Respond: SFM's Prompt and Effective Incident Response

The Respond section establishes mandatory procedures for addressing detected cybersecurity incidents. It outlines the roles and responsibilities of the Computer Security Incident Response Team, communication protocols during an incident, and steps for containment, eradication, and recovery. This section requires regular drills and updates to the response plan to adapt to evolving cyber threats. All personnel must know their role in incident response to ensure a coordinated and practical approach to managing cybersecurity incidents.

6.1 Response Planning (RS.RP): Overview

Purpose:

To establish a robust and dynamic incident response plan capable of effectively managing and mitigating the impacts of cybersecurity incidents on SFM's operations.

Scope:

This policy covers all procedures and actions for preparing, executing, and revising the incident response plan for cybersecurity events affecting SFM's information systems, networks, and data.

Policy Overview:

The incident response plan must be well-documented, regularly tested, and updated to reflect the evolving cybersecurity landscape and organizational changes. All personnel should be familiar with and trained in their specific roles within the plan.

Key Principles:

- **Execution of the Response Plan:**
  Ensure the incident response plan is actionable and ready to be deployed efficiently during cybersecurity incidents.
- **Roles and Responsibilities:**
  Define and assign clear roles and responsibilities to ensure effective execution and accountability during incident response.
- **Communication Protocols:**
  Establish and maintain effective communication protocols for coordinating within SFM and external stakeholders.
- **Integration with Business Continuity:**
  Seamlessly integrate the incident response plan with business continuity and disaster recovery plans to ensure comprehensive organizational resilience.
- **Training and Drills:**
  Conduct regular training and simulation drills to enhance the preparedness of personnel and ensure the response plan's effectiveness.
- **Continuous Improvement:**
  Continuously evaluate and improve the incident response plan based on feedback from exercises, actual incidents, and changes in the external and internal environments.

Roles and Responsibilities:

- **VP - Information Security:**
  Oversee the development, implementation, and maintenance of the incident response plan and ensure alignment with overall business continuity strategies.
- **Computer Security Incident Response Team:**
  Consisting of IT security professionals tasked with executing the response plan, managing cybersecurity incidents as they arise, and mitigating risks.
- **Human Resources:**
  Coordinate with the Computer Security Incident Response Team to ensure all personnel know their roles within the response plan; manage training schedules.
- **Communications Department:**
  Manage internal and external communications during an incident, ensuring information is conveyed clearly and consistently according to the established protocols.
- **Legal and Compliance Team:**
  Advise on legal obligations and compliance issues during incident handling, especially concerning data breaches or other security incidents requiring regulatory notification.
- **Executive Leadership:**
  Participate in critical decision-making processes, ensure the availability of resources, and support the execution and enforcement of the response plan.
- **IT Infrastructure Team:**
  Provide technical support during incidents, assist with containment and eradication of threats, and recover systems and services.

Reference to the Information Security Standard:

For more detailed procedures and guidelines on response planning, please refer to the "Information Security Standard," Sections RS.RP-1 through RS.RP-5.

6.2 Communications (RS.CO): Overview

Purpose:

To define and implement effective communication protocols that govern the exchange of information during and after a cybersecurity incident within SFM, ensuring that all communications are handled with confidentiality, clarity, and precision.

Scope:

This policy covers all internal and external communications related to cybersecurity incidents within SFM, involving all organizational personnel, partners, customers, and regulatory bodies.

Policy Overview:

The communication strategy during cybersecurity incidents is critical to managing and mitigating the impact on SFM's operations and reputation. This policy mandates structured communications, safeguarding sensitive information while maintaining transparency and compliance with relevant laws and standards.

Key Principles:

- **Clarity of Personnel Roles and Response Order of Operations:**
  Clearly define the communication roles and the sequence of communication activities during incident response to ensure effective information flow and decision-making.
- **Consistent Reporting of Security Events:**
  Standardize the reporting procedures for security events to foster timely and accurate information dissemination within and outside SFM.
- **Consistent Information Sharing in Response to Cybersecurity Events:**
  Outline protocols for sharing information related to cybersecurity events, ensuring alignment with incident response strategies, and maintaining operational security.
- **Stakeholder Coordination in Incident Response:**
  Establish frameworks for coordinating with internal and external stakeholders during incident responses to enhance the effectiveness of communication strategies.
- **Voluntary Information Sharing for Cybersecurity Awareness:**
  Promote sharing information with external entities to improve cybersecurity awareness and defense capabilities across the industry.

Roles and Responsibilities:

- **VP – Information Security:**
  Oversee the development and implementation of communication protocols; ensure integration with the incident response plan.
- **Computer Security Incident Response Team:**
  Execute the communication plan during incidents; provide updates and reports to designated stakeholders.
- **Communications Department:**
  Manage external communications, including press releases and public statements, ensuring consistency and accuracy of information.
- **Legal and Compliance Teams:**
  Advise on compliance issues related to incident communications; oversee communications involving legal or regulatory implications.
- **Human Resources:**
  Communicate with internal stakeholders, particularly employees, ensuring they are informed about incident impacts and response activities as appropriate.

- **IT and Technical Teams:**
  Provide technical details and updates for crafting accurate communications during and after incident response.
- **External Relations:**
  Handle communications with external stakeholders, including partners, customers, and regulatory bodies, ensuring that messages are coordinated and comply with contractual and regulatory obligations.

Reference to the Information Security Standard:

For detailed procedures and guidelines on communication during cybersecurity incidents, please refer to "Information Security Standard," Sections RS.CO-1 through RS.CO-5.

6.3 Analysis (RS.AN): Overview

Purpose:

To establish robust analysis procedures for cybersecurity incidents within SFM, ensuring that incidents are thoroughly investigated, their impacts are accurately assessed, and findings are utilized to strengthen incident response and prevention strategies.

Scope:

This policy applies to all processes related to analyzing cybersecurity incidents at SFM, encompassing forensic investigations, impact assessments, and incident categorization.

Policy Overview:

Effective analysis is crucial for understanding cybersecurity incidents' scope, impact, and nature. This policy outlines the responsibilities and procedures for conducting comprehensive analyses, employing forensic tools and techniques, and ensuring Team Member cooperation.

Key Principles:

- **Investigation of Detection System Notifications:**
  Define procedures for the timely and effective investigation of alerts from cybersecurity detection systems to ensure rapid response to potential security incidents.
- **Understanding the Impact of Cybersecurity Incidents:**
  Assess and understand the impact of cybersecurity incidents on SFM's operations and security posture to inform appropriate response strategies.
- **Conducting Forensic Analysis:**
  Utilize forensic tools and techniques to investigate cybersecurity incidents thoroughly, ensuring that analyses contribute to incident resolution and knowledge enhancement.
- **Categorization of Cybersecurity Incidents:**
  Systematically categorize cybersecurity incidents to tailor response strategies effectively and streamline incident management processes.
- **Management of Disclosed Vulnerabilities:**
  Implement procedures for managing vulnerabilities disclosed from internal and external sources, ensuring these are addressed promptly to mitigate potential risks.

Roles and Responsibilities:

- **VP – Information Security:**
  Oversee the development and implementation of analysis policies; ensure integration with the overall incident response strategy.

- **IT Security Operations:**
  Conduct detailed forensic investigations and analyses of cybersecurity incidents; provide insights to guide the response and recovery efforts.
- **Computer Security Incident Response Team:**
  Collaborate with the forensic team to understand the nature and impact of incidents; adjust response strategies based on analytical findings.
- **IT and IT Security Operations:**
  Monitor systems and networks; initiate the incident analysis phase upon detection of potential security events.
- **Legal and Compliance Departments:**
  Ensure that forensic and incident analysis processes comply with legal standards and corporate policies, particularly in data handling and evidence preservation.
- **Human Resources:**
  Facilitate communication and cooperation across departments during incident investigations; handle personnel-related aspects of incident responses.
- **Communication and Public Relations Team:**
  Work with the Incident Response Team to communicate the nature and impact of incidents to external stakeholders, ensuring messages are clear and accurate.

Reference to the Information Security Standard:

For detailed procedures on conducting forensic analysis, assessing incident impact, and managing disclosed vulnerabilities, refer to "Information Security Standard," Sections RS.AN-1 through RS.AN-5.

6.4 Mitigation (RS.MI): Overview

Purpose:

To define the actions necessary to contain, mitigate, and limit the impact of cybersecurity incidents within SFM, ensuring rapid recovery and minimizing operational disruption.

Scope:

This policy applies to all procedures and actions related to the containment, mitigation, and management of cybersecurity incidents affecting SFM's information systems, networks, and data.

Policy Overview:

Swift and effective mitigation is critical to reducing the damage from cybersecurity incidents. This policy outlines required actions for incident containment, mitigation strategies, and management of newly identified vulnerabilities.

Key Principles:

- **Containment of Cybersecurity Incidents:**
  Implement immediate and effective containment strategies to prevent the spread of cybersecurity incidents and minimize damage.
- **Mitigation of Cybersecurity Incidents:**
  Execute comprehensive mitigation actions to reduce the impact of incidents and support SFM's rapid recovery and continued operation.
- **Management of Newly Identified Vulnerabilities:**
  Address newly discovered vulnerabilities promptly by implementing mitigation measures or accepting the risk based on a formal assessment.

Roles and Responsibilities:

- **VP – Information Security:**
  Oversee the development and execution of the mitigation policy; ensure integration with SFM's broader security strategy.
- **Computer Security Incident Response Manager:**
  Lead the coordination and implementation of containment and mitigation strategies during and after cybersecurity incidents.
- **IT Security Team:**
  Execute technical containment and mitigation measures, such as isolating affected systems, eradicating threats, and applying security patches.
- **Risk Management Team:**
  Manage the assessment and treatment of newly identified vulnerabilities, deciding on mitigation or risk acceptance.
- **Communications Team:**
  Handle internal and external communications related to incident mitigation, ensuring clarity, accuracy, and timeliness.
- **Human Resources:**
  Support communication efforts and ensure all staff understand their roles in mitigation processes through regular training and updates.
- **Legal and Compliance Departments:**
  Provide guidance on regulatory requirements during the mitigation process; handle legal implications of cybersecurity incidents.

Reference to the Information Security Standard:

For detailed procedures on containment strategies, mitigation actions, and vulnerability management, refer to "Information Security Standard," Sections RS.MI-1 through RS.MI-3.

6.5 Improvements (RS.IM): Overview

Purpose:

To systematically refine and enhance SFM's cybersecurity response capabilities by learning from past incidents and adapting to new challenges.

Scope:

This policy covers continuously improving incident response plans and strategies across all operational levels within SFM.

Policy Overview:

Continuous improvement is crucial for maintaining effective defense mechanisms against evolving cybersecurity threats. This policy establishes guidelines for conducting post-incident reviews, updating response plans and strategies, and ensuring ongoing staff training.

Key Principles:

- **Incorporation of Lessons Learned into Response Plans:**
  Systematically integrate findings from post-incident reviews into SFM's incident response plans to enhance preparedness and effectiveness.
- **Updating of Cybersecurity Response Strategies:**
  Regularly refine response strategies to incorporate emerging threats, best practices, and feedback from internal and external stakeholders.

Roles and Responsibilities:

- **VP – Information Security:**
  Oversee the overall policy implementation, ensuring integration of lessons learned and updates to cybersecurity strategies.
- **Computer Security Incident Response Manager:**
  Lead the post-incident review process, facilitate debriefing sessions, and effectively communicate revised plans.
- **IT Security Team:**
  Implement technical changes to response strategies and assist in testing and validating updated plans.
- **Human Resources and Training Departments:**
  Update training programs based on revised response plans and strategies and ensure all personnel receive relevant training.
- **Communications Team:**
  Manage internal and external communications related to incident response strategy and policy changes.
- **Legal and Compliance Departments:**
  Provide guidance on regulatory compliance impacts of changes to response plans and participate in the review process to ensure legal compliance.
- **Business Unit Leaders:**
  Collaborate in the review process to ensure that response strategies align with operational needs and business continuity requirements.

Reference to the Information Security Standard:

For detailed procedures on conducting post-incident reviews, integrating lessons learned, and updating response strategies, refer to "Information Security Standard," Sections RS.IM-1 and RS.IM-2.

7 Recover: SFM's Resilience and Restoration Post-Incident

This final section focuses on resilience and recovery planning to restore any capabilities or services impaired due to a cybersecurity incident. It requires establishing business continuity plans, data recovery procedures, and regular testing of backup systems. This section also mandates post-incident reviews to identify lessons learned and to incorporate these insights into future planning, ensuring SFM’s ability to rapidly adapt and resume operations with minimal impact.

7.1 Recovery Planning (RC.RP): Overview

Purpose:

To establish a robust framework for SFM's recovery operations following a cybersecurity incident, ensuring timely restoration of systems and data while minimizing operational disruptions.

Scope:

This policy mandates the creation, execution, and continuous refinement of a cybersecurity recovery plan that addresses the restoration of SFM's IT infrastructure, critical data, and operational capabilities after a security breach or other disruptive events.

Policy Overview:

Recovery planning is crucial for resuming business operations with minimal downtime and impact on stakeholders. This policy provides guidelines for developing a recovery plan that is comprehensive, effective, and responsive to the evolving cybersecurity landscape.

Key Principles:

- **Execution of Cybersecurity Recovery Plan:**
  Outlines procedures and resources necessary to implement the recovery plan during or after cybersecurity incidents effectively.

Roles and Responsibilities:

- **VP – Information Security:**
  Oversee the development, maintenance, and execution of the cybersecurity recovery plan. Ensure alignment with overall business continuity and disaster recovery strategies.
- **Computer Security Incident Response Manager:**
  Coordinate the execution of the recovery plan, manage resources, and maintain communication with key stakeholders during the recovery process.
- **IT Department:**
  Responsible for the technical aspects of recovery, including system restorations, data recovery, and securing restored operations against further attacks.
- **Human Resources:**
  Ensure that all personnel are familiar with their roles in the recovery process through regular training and updates to the recovery plan.
- **Communications Department:**
  Manage internal and external communications during recovery, ensuring stakeholders are informed of recovery status and expected recovery timelines.
- **Legal and Compliance Teams:**
  Provide guidance on compliance issues related to data breaches and recovery, ensuring adherence to legal and regulatory requirements during recovery.

Reference to the Information Security Standard:

For detailed procedures on the development, testing, and execution of the recovery plan, refer to "Information Security Standard," Section RC.RP-1.

7.2 Improvements (RC.IM): Overview

Purpose:

To strengthen SFM's recovery strategies by continuously incorporating lessons learned from cybersecurity incidents, ensuring the recovery plans evolve in line with emerging threats and organizational changes.

Scope:

This policy mandates systematic updates to recovery strategies and procedures, applying insights gained from incident debriefings and recovery exercises across all operational areas of SFM.

Policy Overview:

Improvements to cybersecurity recovery strategies are vital for maintaining the resilience and agility of SFM's operations. This policy outlines the processes for updating recovery plans and strategies based on real-world experiences and simulated exercises.

Key Principles:

- **Incorporation of Lessons Learned into Recovery Plans:**
  Focuses on refining recovery protocols by integrating lessons learned from past incidents and recovery operations.

Roles and Responsibilities:

- **Chief Information Security Officer (CISO):**
  Oversee the collection and integration of lessons learned into recovery plans and ensure that updates align with organizational objectives.
- **Recovery Manager:**
  Coordinate the debriefing processes and facilitate the cross-functional review of recovery actions and outcomes.
- **IT and Business Continuity Managers:**
  Implement updates to recovery strategies and participate in regular reviews to ensure strategies remain effective under new threat scenarios.
- **Training Coordinator:**
  Update and deliver training programs based on the revised recovery strategies to ensure all personnel know their roles under the updated plans.

Reference to the Information Security Standard:
Refer to "Information Security Standard," Sections RC.IM-1 and RC.IM-2 for detailed procedures on integrating lessons learned and updating recovery strategies.

7.3 Communications (RC.CO): Overview

Purpose:
To establish protocols for managing communications related to recovery operations after a cybersecurity incident, ensuring transparency, efficiency, and compliance with regulatory requirements.

Scope:
This policy covers all internal and external communications during the recovery phase of cybersecurity incidents at SFM.

Policy Overview:
Effective communication is crucial during recovery operations to maintain trust, manage public relations, and ensure coordinated recovery efforts. This policy provides guidelines for engaging with internal teams, external partners, stakeholders, customers, and regulatory bodies.

Key Principles:

- **Management of Public Relations in Cybersecurity Incidents:**
  Focuses on managing external communications effectively to protect SFM's reputation and comply with legal standards.
- **Reputation Management Post-Cybersecurity Incident:**
  Outlines strategies for restoring stakeholder trust and managing the organization's public image following an incident.
- **Communication of Recovery Activities:**
  Details of how recovery activities should be communicated to internal and external stakeholders to maintain transparency and coordination.

Roles and Responsibilities:

- **Communications:**
  Oversee all communication strategies related to cybersecurity incidents and recovery operations. Manage public communications and media relations, ensuring consistent and accurate messaging.
- **Incident Response Coordinator:**
  Ensure communication efforts are synchronized with the overall incident response and recovery strategies.
- **VP – IT Security:**
  Provide critical information and updates for communications regarding the nature of the incident and recovery progress.

Reference to the Information Security Standard:
For detailed communication procedures during and after cybersecurity incidents, refer to "Information Security Standard," Sections RC.CO-1 to RC.CO-3.

8 Privacy Expectation

All content, messages, and information stored or transmitted using SFM IT assets are the property of SFM. Team Members should have no expectation of privacy or confidentiality for Content or information they create, send, receive, store, delete, or transmit via SFM IT assets, consistent with privacy law requirements. This includes personal messages that may be routed to and consequently stored on SFM IT assets via SFM-issued personal computers, laptops, and other devices.

9 Other Related Policies/Standards/Protocols/Guidelines:

- Acceptable Use of Information Technology Resources Policy
- Account Management/Access Control Standard
- Backup Policy
- Change Management Policy
- Data Classification and Protection Standard
- Incident Response Policy
- Patch Management Standard
- Privacy Policy
- Remote Access Standard
- Retention Policy
- Secure Configuration Management Standard and Security Logging Standard
- Secure System Development Lifecycle Standard and Secure Coding
- Vendor Risk Management Policy
- Vulnerability Scanning Standard

10 Terms and Definitions

Term	Definition

Access Control	The methods and processes used to regulate and monitor access to information systems, networks, and data.
Availability	The principle of ensuring that authorized users have reliable and timely access to information and resources when needed, as part of the CIA triad (Confidentiality, Integrity, Availability) in information security. This includes maintaining and ensuring the proper functioning of information systems and networks, and implementing measures to mitigate against disruptions, such as hardware failures, software malfunctions, and cyber-attacks.
Communication Protocol	Guidelines and methods for conveying information, especially during a cybersecurity incident.
Compliance	Adherence to laws, regulations, guidelines, and specifications relevant to SFM.
Confidentiality	The principle of restricting access to information to authorized individuals to protect sensitive data from unauthorized disclosure.
Containment	Steps taken to limit the extent of damage or spread of a cybersecurity incident.
Cybersecurity Incident	An event that impacts the confidentiality, integrity, or availability of information assets and requires a response.
Data Breach Notification	A legal requirement to inform individuals and authorities about unauthorized access to confidential data.
Data Integrity	The accuracy and consistency of data over its lifecycle, ensuring it remains unaltered from unauthorized or accidental changes.
Debriefing	A structured review process conducted after an incident to analyze the response and identify lessons learned.
Disaster Recovery	The strategies and plans for recovering from large-scale, disruptive events, focusing on restoring IT infrastructure and operations.
Encryption	The process of converting data into a code to prevent unauthorized access.
Forensic Analysis	The process of collecting, preserving, analyzing, and presenting digital evidence related to a cybersecurity incident.
Incident Response Plan	A predefined set of instructions and procedures for detecting, responding to, and limiting the impact of a cybersecurity incident.
Information Systems	An integrated set of components for collecting, storing, and processing data, including both technology and people.
Lessons Learned	Insights gained from the review of incident response and recovery processes, used to improve future performance.
Mitigation Strategies	Actions taken to reduce the severity or impact of a cybersecurity incident.
Network Segmentation	Dividing a computer network into subnetworks to improve performance and security.
Patch Management	The process of managing updates of software and technologies, including the deployment and installation of patches.
Public Relations	Management of communication between an organization and its publics to influence perception and maintain a positive reputation.
Recovery Plan	A set of strategies and actions to restore normal operations and services following a cybersecurity incident.
Reputation Management	The practice of influencing and controlling an organization's reputation following an incident.
Risk Assessment	The process of identifying, analyzing, and evaluating risks associated with cybersecurity threats.
Risk Tolerance	The acceptable level of risk an organization is willing to assume to achieve its objectives.
Social Engineering	The psychological manipulation of individuals to perform actions or divulge confidential information.

Stakeholder Engagement	The process of involving stakeholders in the planning, development, and implementation of policies and decisions.
Stakeholders	Individuals or groups who have an interest in the outcome of a process or project, including employees, customers, partners, and regulatory bodies.
Threat Landscape	The evolving set of threatening actions and actors, security vulnerabilities, and the potential impact of these threats.
Two-Factor Authentication	A security process that requires two different forms of identification to access something.
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.
Vulnerability Assessment	The process of identifying, quantifying, and prioritizing vulnerabilities in information systems.
Zero-Day Exploit	A cyber-attack targeting a software vulnerability that is unknown to the software vendor or to antivirus vendors.