Heimdal®

Information Security Policy Template

[Entity] **Information Security Policy**	**No:**
IT Policy: **Information Security**	**Updated:** **Issued By:** **Owner:**

1.0 Purpose and Objectives

This policy establishes the essential minimum standards for information security that must be met by the specified entity.

It permits entities to enhance these security measures based on their unique business requirements and the specific legal and federal guidelines applicable to them, but mandates that they at least meet the security benchmarks outlined herein.

Serving as a foundational document, this policy provides direction for all other security policies and related standards. It outlines the obligation to:

1. Safeguard and uphold the confidentiality, integrity, and availability of information and its supporting infrastructure;

2. Effectively manage the risks associated with security breaches or vulnerabilities;
3. Ensure a secure and reliable information technology (IT) framework;
4. Detect and act upon incidents involving the misuse, loss, or unauthorized access of information assets;
5. Supervise systems for irregularities that may suggest security compromises; and
6. Enhance and promote awareness of information security practices.

Inadequate security measures leading to compromised confidentiality, integrity, and availability of information assets can severely disrupt critical infrastructure operations, financial and business activities, and crucial governmental functions; endanger data; and result in legal and regulatory penalties.

This policy offers advantages to entities by creating a structured approach to ensure protective measures are adequately implemented to guard the confidentiality, integrity, and availability of information. It also ensures that employees and affiliates are aware of their responsibilities, possess sufficient understanding of security policies, procedures, and practices, and are informed on how to safeguard information.

2.0 Authority

Document Owner: [Owner's Name]
Approval Authority: [Authority Name]
Last Reviewed: [Date]
Next Review Date: [Date]
Change History: [Record of changes]

3.0 Scope

This information security policy template applies to all systems, both automated and manual, over which the entity has administrative control. This includes systems that are managed or hosted by third-party services on the entity's behalf. It covers all types of information, in any form or format, that are produced or utilized in the course of conducting business activities.

4.0 Statement on Information Security

4.1 Organizational Security Management

a. Effective information security necessitates the establishment of both an information risk management function and an information technology security function. The configuration of the organization will determine whether these roles are combined and undertaken by either an individual or a group, or if separate individuals or groups are allocated for each function. It is advised that a senior executive or a team involving senior executives undertake these responsibilities.

Organizations must appoint either an individual or a team to oversee risk management, ensuring that:

i. The approach to risk for both information assets and specific information systems, including decisions on authorization, is integrated and aligned with the broader strategic aims and foundational activities of the organization;

ii. The oversight of information assets and the management of risks related to information systems are uniform, mirror the organization's risk appetite, and are evaluated alongside other risk types to guarantee the success of the organization's mission and business operations.
Each organization is required to nominate an individual or a team to handle the technical aspects of information security. For the sake of clarity, this policy will refer to this role as the Information Security Officer (ISO) or the designated security representative. This role entails assessing and providing advice on information security risks.

b. Decisions regarding information security risk must involve consultations with the functional areas mentioned in section a.

c. While the technical aspect of information security may be outsourced, the ultimate responsibility for the security of its information remains with the organization.

4.2 Functional Responsibilities

Executive management is tasked with:

1. Evaluating and accepting entity risks.

2. Defining information security objectives and integrating them into processes.

3. Ensuring the consistent application of security policies and standards.

4. Demonstrating support for security through guidance and resource allocation.

5. Raising security awareness via regular distribution of ISO materials.

6. Managing information classification and protection based on best practices and legal requirements.

7. Overseeing information asset management, including their use and disposal, according to classification.

8. Assigning information owners while retaining overall responsibility for data protection.

9. Engaging in security incident responses.

10. Following breach notification protocols.

11. Complying with legal and regulatory information security obligations.

12. Informing the ISO about legal and regulatory demands.

13. Communicating policy and standards requirements, including non-compliance consequences, to employees and third parties, ensuring third party contract compliance.

IT management is tasked with:

1. Guiding and integrating security measures into the data processing and network infrastructure to aid information owners.
2. Allocating resources to uphold information security as per this policy.
3. Establishing and applying security processes, policies, and controls as specified by business needs and this policy.
4. Applying appropriate controls for information based on its classification.
5. Training relevant technical personnel in secure practices.
6. Encouraging the involvement of security and technical staff in safeguarding information assets and selecting efficient security measures.
7. Executing business continuity and disaster recovery plans.

The CISO is tasked with:

1. Offering internal security consultation;
2. Formulating and implementing the security strategy and its effectiveness measures;
3. Creating and upholding the organization's security policy and standards;
4. Verifying adherence to these policies and standards;
5. Recommending secure system development practices;
6. Managing incident response and providing expertise;
7. Observing network irregularities;
8. Keeping track of potential external threats like data breaches;
9. Staying connected with security communities and authorities;
10. Alerting to imminent threats and weaknesses;
11. Supplying training materials and conducting awareness programs.

4.3 Duties Separation

1. Implement separation of duties to lower misuse risks. If infeasible, apply alternative controls like activity monitoring and management oversight.
2. Security control audit and approval must stay separate from their implementation.

4.4 Risk Management

1. Systems supporting business must manage information risks and have annual risk assessments within a secure development lifecycle.

2. New projects and major changes require security risk assessments.
3. Entities choose their risk assessment method according to their needs and relevant regulations.
4. Document assessment outcomes and related decisions.

4.5 IT Asset Management

1. Assign all IT hardware and software to a specific business unit or person.
2. Keep a detailed automated inventory of all hardware and software assets, noting key details like network address, machine name, and software version.
3. Use regular scanning to detect unauthorized hardware/software and alert relevant personnel.

4.6 Cyber Incident Management

1. Organizations must establish an incident response plan with consistent standards for effective security incident response.
2. Any detected or suspected security incidents or vulnerabilities must be promptly reported to the relevant management and the ISO/security representative. Employees concerned about unaddressed cyber security issues can confidentially reach out to the Security Operations Center.
3. The Security Operations Center should be alerted to any cyber incidents with potential significant operational or security impacts, or those requiring digital forensics, to ensure appropriate response coordination and oversight.

4.7 Account Management & Access Control

1. Each account needs a designated individual or group for its management, potentially involving both the business unit and IT.
2. Access requires unique user-IDs, unless specified otherwise in the Account Management/Access Control Standard.

3. User-IDs must have an authentication method (e.g., password, biometric) for verifying identity.
4. Systems must lock after inactivity, displaying neutral information (e.g., screen saver), and require re-authentication.
5. Sessions must end automatically under defined conditions as per the standard.
6. Authentication tokens should be confidential and securely protected.
7. Tokens must be securely stored, if at all, with approved methods (e.g., password vault).
8. Information owners decide on access and privileges for their resources.
9. Access is based on job needs, adhering to the principle of least privilege.
10. Privileged account users must have a separate account for general business activities.
11. Systems should display a logon banner stating policy compliance and monitoring.
12. Remote access requires prior approval, risk assessment, and documented controls.
13. Remote connections should occur through managed entry points as per ISO/security guidance.
14. Remote work needs management authorization and secure data handling training.

4.8 Vulnerability Management:

1. Systems must undergo vulnerability scans before production deployment and regularly after.
2. Regular penetration testing is mandatory for all systems.
3. Critical systems require periodic penetration testing.
4. Outsourced system vulnerability scans and penetration tests must be coordinated.
5. Contracts with third parties must include scan/test and mitigation obligations.
6. Scan/test results are to be promptly reviewed by the system owner and shared with the security representative for risk assessment.
7. Discovered vulnerabilities must be promptly addressed through actions like patching, with a documented action and milestones plan for mitigation.

8. Only authorized individuals can conduct scans/tests, with prior notification to the CISO. Unauthorized attempts are prohibited.
9. Authorized testers must adhere to a formal, tested process to avoid disruption.

4.9 Compliance

This policy becomes active immediately upon publication. All members are required to adhere to the established enterprise policies and standards. These policies and standards are subject to change at any time, and adherence to any revised policies and standards is also required.

Should adherence to this standard be impractical or technically unattainable, or if a departure from this policy is required to facilitate a business function, entities must seek approval for an exception via the Chief Information Security Officer's exception procedure.

5.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Entity Address]

6.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Change Description	Reviewer