# Secure System Design Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. NIST 800-160:<https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final>
2. NIST SP 800-207: <https://csrc.nist.gov/pubs/sp/800/207/final>
3. NIST SP 800-215: <https://csrc.nist.gov/pubs/sp/800/215/final>
4. ISO/IEC 27034:<https://www.iso.org/obp/ui/#iso:std:iso-iec:27034:-1:ed-1:v1:en>
5. ISO/IEC 27001:2022: A.8.21, A.8.22, A.8.25, A.8.26, A.8.27, A.8.31
6. NIST 800-53 rev. 5: CM-5(5), CM-8, CM-8(1), CM-8(3), PL-2, PL-8, SA-4, SA-8, SA-15, SA-15(3), SC-2, SC-39
7. CIS v8: 3.8, 12.2, 12.4, 13.4, 16.4, 16.8, 16.10, 16.11
8. PCI DSS 4.0: 1.1.1, 1.2.1, 1.2.3, 1.2.4, 1.4.1, 1.4.2, 1.4.4, 1.4.5, 6.1.1, 6.3.2, 6.5.3, 6.5.4
9. AICPA SOC 2 TSC: CC2.1, CC5.2, CC6.1, CC6.7, CC7.1, CC8.1, PI1.3

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this Secure System Design Policy is to establish a comprehensive framework for incorporating security principles and practices throughout the system development lifecycle. This policy aims to ensure that all systems are designed, developed, deployed, and maintained with robust security measures to protect organizational assets, data integrity, and user privacy. By adhering to industry best practices and regulatory requirements, this policy seeks to mitigate security risks, prevent unauthorized access, and ensure the continuous protection of critical information systems.

## Scope

This policy applies to all information systems developed, maintained, or operated by [Organization name], including but not limited to:

* Software applications
* Network infrastructure
* Hardware components
* Third-party services and integrations

This policy is mandatory for all employees, contractors, third-party vendors, and stakeholders involved in the development, deployment, or maintenance of [Organization name]'s information systems. Compliance with this policy is essential to ensuring the security and resilience of the organization's IT infrastructure and safeguarding sensitive data against threats and vulnerabilities.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators**  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. **Secure Engineering Principles:** A set of best practices and methodologies aimed at ensuring the security of systems throughout the development lifecycle by integrating security requirements from the outset.
	2. **Fail Secure:** A security mechanism that ensures systems default to a secure state in the event of a failure, preventing unauthorized access or data leakage.
	3. **Components:** Individual parts or elements that make up a system, including hardware, software, and third-party services, which are essential for the system's functionality.
	4. **Infrastructure:** The foundational physical and virtual resources (such as servers, networking equipment, and cloud services) required to operate and manage IT services and solutions.
	5. **Specifications:** Detailed, documented requirements and standards that define the security and privacy needs of a system, ensuring alignment with industry standards and regulatory obligations.
	6. **Network Separation:** The practice of dividing a network into distinct segments to enhance security and limit the spread of potential threats.
	7. **Zero Trust:** A security model that assumes no implicit trust and requires continuous verification of user identity, device health, and access rights before granting access to resources.
	8. **Development Environment:** An isolated environment where software development activities take place, including writing, testing, and debugging code.
	9. **Staging Environment:** A pre-production environment that closely mirrors the production environment, used for final testing and validation of changes before deployment.
	10. **Production Environment:** The live environment where the final version of software or services is deployed and accessible to end users.
	11. **Testing Environment:** An optional isolated environment used specifically for extensive testing, including functional, performance, and security testing, to ensure system stability and security.
	12. **Network Diagrams:** Visual representations of a network's components and their interconnections, used to illustrate and document the architecture of the network.
	13. **Data Flows:** Diagrams or descriptions showing how data moves through a system, including sources, destinations, and transformations along the way.
	14. **Capacity Planning:** The process of forecasting and managing the resources required (such as storage and processing power) to meet current and future demand for IT services.
	15. **Software Bill of Materials (SBOM):** A comprehensive inventory of all software components, including versions and dependencies, used in an application or system, essential for managing and mitigating security vulnerabilities.

## Policy

#### Secure Engineering Principles

The [responsible party] shall implement secure engineering principles to ensure the robustness and resilience of all systems.

* + 1. Incorporate security requirements early in the system development lifecycle.
		2. Conduct regular threat modeling and risk assessments.
		3. Utilize secure coding practices and static code analysis tools.
		4. Perform regular security reviews and audits throughout the development process.

#### Fail Secure

The [responsible party] is required to ensure that control systems fail securely to prevent unauthorized access or data leakage.

* + 1. Implement mechanisms to ensure systems default to a secure state in the event of a failure.
		2. Regularly test fail-secure mechanisms to verify their effectiveness.
		3. Document and address any identified weaknesses in the fail-secure mechanisms.

#### Secure Use of Components and Infrastructure

The [responsible party] shall ensure the secure use of components and infrastructure.

* + 1. Use only approved and validated components in the system architecture.
		2. Regularly update and patch all components to protect against vulnerabilities.
		3. Conduct security assessments on third-party components and services.

#### Specifications for Defining Requirements for Security and Privacy

The [responsible party] is required to use specifications for defining security and privacy requirements.

* + 1. Develop comprehensive security and privacy requirements documentation.
		2. Ensure alignment with industry standards and regulatory requirements.
		3. Conduct periodic reviews and updates to the security and privacy specifications.

#### Network Separation and Zero Trust

The [responsible party] shall implement network separation and zero trust principles.

* + 1. Segment networks to isolate critical systems and data.
		2. Implement strict access controls and authentication mechanisms.
		3. Regularly review and update network segmentation and access policies.

#### Separate Environments for Development, Staging, and Production

The [responsible party] is required to maintain separate environments for development, staging, and production.

* + 1. Establish isolated environments to prevent cross-contamination of data and code.
		2. Implement stringent access controls for each environment.
		3. Optionally, create an additional environment for testing purposes.

#### Creation of Network Diagrams and Data Flows

The [responsible party] shall create and maintain up-to-date network diagrams and data flow documentation.

* + 1. Document all network components, connections, and data flows.
		2. Regularly review and update diagrams to reflect any changes in the infrastructure.
		3. Ensure diagrams are accessible to relevant stakeholders.

#### Capacity Planning for Storage and Processing

The [responsible party] is required to perform capacity planning for storage and processing.

* + 1. Analyze current and projected storage and processing needs.
		2. Implement scalable solutions to accommodate growth and demand.
		3. Regularly review and adjust capacity plans based on usage patterns and trends.

#### Maintain of a Software Bill of Materials (SBOM)

The [responsible party] shall maintain a comprehensive Software Bill of Materials (SBOM).

* + 1. Document all software components, including versions and dependencies.
		2. Update the SBOM with each new release or update.
		3. Use the SBOM to track and manage vulnerabilities in software components.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |