# Asset Management 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 and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. ISO/IEC 27040: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-2:v1:en>
2. ISO 55000 Series: <https://theiam.org/knowledge-library/iso-55000/>
3. NIST SP 800-124: <https://csrc.nist.gov/pubs/sp/800/124/r2/final>
4. NIST SP 800-114: <https://www.nist.gov/privacy-framework/nist-sp-800-114>
5. NIST 800-88: <https://csrc.nist.gov/pubs/sp/800/88/r1/final>
6. ISO/IEC 27555: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27555:ed-1:v1:en>
7. ISO/IEC 27040: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-2:v1:en>
8. ISO/IEC 27001:2022: A.5.9, A.5.11, A.7.7, A.7.10, A.7.14, A.8.1, A.8.10
9. NIST 800-53 rev. 5: AC-11, AC-11(1), AC-19, AC-19(5), AC-20(2), CM-8, MA-3(2), MP-1, MP-3, MP-5, MP-6, MP-7, PE-5, PS-4, PS-5, SC-15, SR-12
10. AICPA SOC 2 TSC: C1.2, CC2.1, CC6.4, CC6.5, CC6.7, CC6.8
11. PCI DSS 4.0: 1.5.1, 5.3.3, 9.2.4, 9.4.6, 9.4.7, 9.5.1, 9.5.1.1, 12.5.1,
12. CIS v8: 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 2.4, 3.5, 3.9, 4.5, 4.6, 4.10, 4.11, 4.12, 10.3, 10.4

## 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

This asset Management Policy establishes a framework for effectively managing the organization's assets throughout their lifecycle. This includes acquiring, inventorying, tracking, maintaining, protecting, and disposing of assets. The policy aims to ensure organizational assets' integrity, confidentiality, and availability, protect against unauthorized access and use, and comply with relevant legal, regulatory, and contractual requirements.

## Scope

This policy applies to all employees, contractors, vendors, and third parties who interact with the organization's assets. It covers all categories of assets, including but not limited to:

* Devices and endpoints such as desktops, laptops, tablets, and smartphones
* Information, data, and records
* System and networking components including servers, switches, routers, and firewalls
* Wireless access points
* Cloud and virtual assets such as cloud services, virtual machines, and virtual networks
* Software and licenses
* Intellectual property, including patents, copyrights, trademarks, and trade secrets
* Spare components for critical systems
* IoT and embedded devices
* Peripheral devices such as printers, scanners, and copiers
* Removable media and portable storage devices

This policy mandates procedures and responsibilities for the inventory management, regular review, authorization, protection, and disposal of these assets to ensure they are used and maintained securely and effectively.

## 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. Asset: Any item of value owned by the organization, including hardware, software, data, and intellectual property.
	2. Critical Asset: An asset essential to the organization's operations, security, or compliance, whose compromise, loss, or failure could significantly impact the organization's functionality, information protection, or regulatory compliance.
	3. Device/Endpoint: Any computing device such as desktops, laptops, tablets, and smartphones used within the organization.
	4. Information: Data, documents, and records that are stored, processed, or transmitted by the organization.
	5. System and Networking Components: Hardware and software components that form part of the organization's IT infrastructure, including servers, switches, routers, and firewalls.
	6. Wireless Access Point: A device that provides wireless network connectivity to other devices.
	7. Cloud and Virtual Assets: Services, virtual machines, and virtual networks hosted in cloud environments.
	8. Software and Licenses: Applications and programs used by the organization, along with their associated usage rights.
	9. Intellectual Property: Legal rights associated with creations of the mind, such as patents, copyrights, trademarks, and trade secrets.
	10. Spare Components: Backup hardware components reserved for use in critical systems in the event of a failure.
	11. IoT (Internet of Things) Devices: Internet-connected devices that collect and exchange data.
	12. Embedded Devices: Specialized computing devices that perform dedicated functions within larger systems.
	13. Peripheral Devices: External devices connected to a computer, such as printers, scanners, and copiers.
	14. Inventory: A detailed list of assets owned by the organization.
	15. Patching: The process of applying updates to software to fix vulnerabilities or improve functionality.
	16. Encryption: The process of converting data into a coded format to prevent unauthorized access.
	17. Malicious Code: Software designed to disrupt, damage, or gain unauthorized access to computer systems.
	18. Mobile Device Policy: Guidelines that govern the use of mobile devices within the organization, including BYOD, CYOD, and COPE approaches.
	19. BYOD (Bring Your Own Device): A policy allowing employees to use their personal devices for work purposes.
	20. CYOD (Choose Your Own Device): A policy where employees choose from a list of approved devices provided by the organization.
	21. COPE (Corporate-Owned, Personally Enabled): A policy where the organization provides devices that can be used for both work and personal purposes.
	22. Removable Media: Portable storage devices such as USB drives, external hard drives, and CDs/DVDs.
	23. Tampering Detection: Measures implemented to identify unauthorized alterations to devices or components.
	24. Counterfeit Detection: Measures implemented to identify fake or unauthorized components.
	25. Wiping: The process of securely erasing data from storage devices to prevent data recovery.
	26. Degaussing: The process of using a magnetic field to erase data stored on magnetic media.

## Policy

#### Inventory Management

The [responsible party] shall:

* 1. Maintain a comprehensive inventory of all critical assets, which includes but is not limited to the following categories:
		+ 1. Devices/Endpoints: All computing devices, including desktops, laptops, tablets, and smartphones.
			2. Information: Business-critical data, documents, and records.
			3. System and Networking Components: Servers, switches, routers, firewalls, and other network infrastructure.
			4. Wireless Access Points: All devices providing wireless connectivity.
			5. Cloud and Virtual Assets: Cloud-based services, virtual machines, and virtual networks.
			6. Software and Licenses: All software applications and associated licenses.
			7. Intellectual Property: Patents, copyrights, trademarks, and trade secrets.
			8. Spare Components: Backup hardware components for critical systems.
			9. IoT and Embedded Devices: Internet of Things devices and embedded systems.
			10. Peripheral Devices: Printers, scanners, copiers, and other peripherals.
		1. Ensure that all assets are uniquely identified and tracked throughout their lifecycle.
		2. Conduct regular reviews of asset inventories to ensure accuracy and completeness.
		3. Update the inventories to reflect any changes, additions, or disposals of assets.
		4. Implement measures to detect tampering and counterfeit components within the organization's assets.

#### Software Licensing

* + 1. Ensure that all software in use is properly licensed.
		2. Maintain records of software licenses and ensure compliance with licensing agreements.
		3. Ensure that all software and components used in critical systems are properly authorized and approved before deployment.

#### Device Management

The [responsible party] shall:

* + 1. Implement full device encryption for all devices used for processing or storing protected data to ensure data confidentiality and integrity.
		2. Ensure timely application of patches and updates to all devices to protect against vulnerabilities.
		3. Deploy and maintain up-to-date anti-malware solutions on all devices to protect against malicious code.
		4. Ensure that all devices lock after a defined period of inactivity to prevent unauthorized access.
		5. Establish and enforce a mobile device policy that covers Bring Your Own Device (BYOD), Choose Your Own Device (CYOD), and Corporate-Owned, Personally Enabled (COPE) approaches based on risk assessments.
		6. Ensure the return of all organizational assets upon termination of employment, role change, or other qualifying events.

#### Peripheral and Removable Devices

The [responsible party] shall:

* + 1. Secure all peripheral devices to prevent unauthorized connections to the network.
		2. Implement controls to prevent the connection of unauthorized peripheral devices.
		3. Require scanning of removable devices for malicious code before use.
		4. Enforce policies to control the use of removable media within the organization.

#### Destruction of Assets

The [responsible party] shall:

* + 1. Implement procedures for properly destroying information assets to ensure data cannot be recovered.
		2. Ensure the proper destruction of physical devices by following the industry's best practices to prevent data leakage.
		3. Ensure that data and devices cannot be recovered after disposal

## 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** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |