# Asset Management Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to ensure assets are identified appropriately and the proper protection controls for those assets are in place.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Asset Management Policy applies to all business processes and data, information systems and components, personnel, and physical areas of [Insert Company’s Name].

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws, Regulations, and Standards

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
| ISO27001:2013 | A.8 (A.8.1., A.8.2., A.8.3.) |
| NIST SP 800-53 v4 | AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16 |

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

**Responsibility for Assets:**

* + Information or information processing facility assets must be inventoried and documented and that record must be kept up to date.
		- Inventory categorization must be approved by the appropriate parties or authorizing authority.
		- Organization will employ use of automated mechanisms to identify unauthorized systems including hardware or software.
		- Inventory must also include information system updates or removals.
	+ This process must be assigned to an owner to maintain the process.
		- Individuals requiring access to the information systems must follow proper procedure to receive such access, such as signed acknowledgement of standards and consequences.
	+ The following assets should be considered in the inventory process:
		- Authorized assets
		- Unauthorized assets
		- Software
		- Databases
		- Information stores
		- Physical assets
		- Services
		- People
		- Tangibles
	+ Processes around configuration management will be established as well.
	+ All assets must be returned upon termination of employment or contract.

**Information Classification:**

* + All assets must be classified in terms of legal requirements, value to the organization, their criticality to the organization, and sensitivity if they were to be disclosed by an unauthorized party.
	+ [Insert Company’s Name] data shall be classified into one of the following categories:
		- Top Secret: Critical information whose existence or content is only known to a small group of individuals. Disclosure of this information would harm the company or impede ability to achieve corporate objectives.
		- Sensitive: Sensitive information requires an elevated level of protection (e.g. encryption) to satisfy regulatory requirements or prevent its unintended disclosure. Information is disclosed only to authorized individuals on a need-to-know basis.
		- Business Confidential: Business confidential information / data is used to conduct normal business operations of [Insert Company’s Name]. Normal levels of confidentiality (per the Employee Code of Conduct) are applied. The intention is to minimize the impact upon business operations.
		- Internal Use: Internal use data / information is used to support the business operations of a department. The information is intended for internal use only.
		- Public: Public information is such that [Insert Company’s Name] has published for general or public consumption, or publicly known information that [Insert Company’s Name] has received from other organizations.
	+ Assets will be labeled and handled based on appropriate information classification procedures used by the organization.

**Media Handling:**

* Removable media must also be managed by the same asset classification procedure used by the organization.
* Removable media must be protected against unauthorized access and misuse while in use and in transit, and must be disposed of securely, using appropriate procedures.
* Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation.

**Acceptable Use:**

* Standards or guidelines for the acceptable usage of assets should be documented to indicate what information system users are and are not allowed to do.
* The following items should be covered in acceptable usage guidelines:
	+ Computer and information system usage
	+ Software and data usage
	+ Internet and email usage
	+ Telephone usage
	+ Office equipment & materials usage
* As a requirement of information system access, and as a component of security awareness training, all information system users, whether employees or third parties, will be required to provide signed acceptance of the acceptable usage guidelines.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |