COMPANY policy template instructions

This COMPANY policy template represents a complete, compliance-ready policy with placeholders for company specific text. Each policy section represents a policy-specific topic that you should consider and/or modify to match your company’s practices.

For each policy section

* Consider if this section and its corresponding risks applies to you. If it does not, remove it and/or replace it with your organization’s corresponding practices.
* Replace any highlighted text in angled brackets < > with your own language
* Rewrite the policy language such that it reflects the practices of your organization

Policy completion checklist

1. Use Find to make sure that all text in angled brackets is replaced
2. Proofread your policy for spelling and grammar mistakes
3. Confirm that the policy’s content reflects your organizations practices
4. Add any company-specific letterhead, branding, and formatting
5. Remove this instructions page
6. Export this document as PDF — File > Save As > Change “File Format” to PDF
7. Upload the PDF to COMPANY at https://app.COMPANY.com/policies

More questions?

A good rule-of-thumb is to keep your language high enough level such that it stays representative for at least a year. If you have more questions about how to use this template, please reach out to support@COMPANY.com or your auditor for additional guidance.

Asset Management Policy

Policy Owner: <Policy owner>

Effective Date: <Effective date>

# Purpose

To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

# Scope

This policy applies to all <Company Name> owned or managed information systems.

# Policy

## Inventory of Assets

Assets associated with information and information processing facilities that store, process, or transmit classified information shall be identified and an inventory of these assets shall be created and maintained.

## Ownership of Assets

Assets maintained in the inventory shall be owned by a specific individual or group within <Company Name>.

## Acceptable Use of Assets

Rules for the acceptable use of information, assets, and information processing facilities shall be identified and documented in the Information Security Policy.

## Loss or Theft of Assets

All <company> personnel must immediately report the loss of any information systems, including portable or laptop computers, smartphones, PDAs, authentication tokens (keyfobs, one-time-password generators, or personally owned smartphones or devices with a <Company Name> software authentication token installed) or other devices that can store and process or help grant access to <Company Name> data.

## Return of Assets

All employees and third-party users of <Company Name> equipment shall return all of the organizational assets within their possession upon termination of their employment, contract, or agreement.

## Handling of Assets

Employees and users who are issued or handle <Company Name> equipment are expected to use reasonable judgment and exercise due care in protecting and maintaining the equipment.

Employees are responsible for ensuring that company equipment is secured and properly attended to whenever it is transported or stored outside of company facilities.

All mobile devices shall be handled in accordance with the Information Security Policy.

Excepting employee-issued devices, no company computer equipment or devices may be moved or taken off-site without appropriate authorization from management.

## Asset Disposal & Re-Use

Company devices and media that stored or processed confidential data shall be securely disposed of when no longer needed. Data must be erased prior to disposal or re-use, using an approved technology in order to ensure that data is not recoverable. Or a Certificate of Destruction (COD) must be obtained for devices destroyed by a third-party service.

Please refer to NIST Special Publication 800-88 Revision 1 “Guidelines for Media Sanitization” in order to select which methods are appropriate.

## Customer Asset Return

Any physical assets owned by customers shall be promptly returned to the customer following service termination in accordance with the terms of contract or service agreement.

# Exceptions

Requests for an exception to this policy must be submitted to the <approver of requests for an exception to this policy, e.g., IT Manager> for approval.

# Violations & Enforcement

Any known violations of this policy should be reported to the <recipient of reports of violations of this policy, e.g., IT Manager>. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** | **Approved by** |
| <1.0> | <29-Apr-2020> | <First Version> | <OWNER> | <APPROVER> |
|  |  |  |  |  |