# Cryptography 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 correct use of cryptography to protect the confidentiality, authenticity, and integrity of the organization’s information.

# 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 Cryptography 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 & 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.10 (A.10.1) |
| NIST SP 800-53 v4 | SC-12, SC-13, SC-17 |
| NIST SP 800-21 | 2.1, 3.6 |

# 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.

**Cryptographic Controls:**

* + [Insert Company’s name] will develop a policy surrounding the proper procedures needed around the use of cryptographic controls. The following items should be considered:
		- Based on a risk assessment, the required level of protection should be identified taking into account the type, strength, and quality of the encryption algorithm required.
		- The use of encryption for protection of information transported by mobile or removable media devices or across communication lines.
		- The standards to be adopted for effective implementation throughout the organization.
		- The impact of using encrypted information on controls that rely upon content inspection.

**Key Management:**

* + Cryptographic keys should be protected through their whole lifecycle.
	+ Cryptographic algorithms, key lengths, and usage practices should be selected according to best practice.
	+ All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure.
	+ Equipment used to generate, store, and archive keys should be physically protected.
	+ A key management system should be based on an agreed set of standards, procedures, and secure methods for:
		- Generating keys for different cryptographic systems and different applications.
		- Issuing and obtaining public key certificates.
		- Distributing keys to intended entities, including how keys should be activated when received.
		- Storing keys, including how authorized users obtain access to keys.
		- Changing or updating keys, including rules on when keys should be changed and how this will be done.
		- Dealing with compromised keys.
		- Revoking keys, including how keys should be withdrawn or deactivated.
		- Recovering keys that are lost or corrupted.
		- Backing up or archiving keys.
		- Destroying keys.
		- Logging and auditing of key management related activities.

**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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |