# Communications Security 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 security is a key consideration in network management and in the transfer of information in and out of the organization.

# 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 Communications Security 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.13.1, A.13.2 |
| NIST SP 800-53 v4 | XX-1 controls, SA-5, CM-2~CM-9, AC-5, SA-9, SA-10, AU-4, AU-5, CP-2, SA-2, SC-5, CA-2, CA-6, SA-4, SA-11, AC-19, AT-2, AT-3, IR-2, IR-8, MA-3, MP-7, SC-42, SI-1, SI-3, SI-5, SI-7, SA-8, SC-2, SC-3, SC-7, SC-18, CP-9, AC-3, AC-17, AC-18, AC-20, SC-8, SC-15, CA-3, MP-5, AU-10, IA-2, IA-8, SC-7, SC-8, SC-13, AC-3, AC-22, SI-4, SI-7, SI-10, AU-2, AU-3, AU-8, AU-11, AU-12, AU-14, AU-6, AU-7, AU-12, CM-6, CM-11, PE-6, PE-8, SC-7, SI-4, SI-6, SI-7, |

# 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.

**Network Security Management:**

* + Network segregation must be implemented. Groups of information services, users, and information systems must be separated from one another.
  + [Insert Company’s name] should implement limitation and controls of network ports, protocols, and services.
  + Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered:
    - Responsibilities and procedures for the management of networking equipment should be established.
    - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks.
    - Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security.
    - Management activities should be closely coordinated both to optimize the service to [insert Company’s name] and to ensure that controls are consistently applied across the information processing infrastructure.
  + The following will be identified and listed within network services’ agreements – both in-house and outsourced agreements:
    - Security mechanisms.
    - Service levels.
    - Management requirements.

**Information Transfer:**

* + Appropriate policies, procedures, and controls must be established around the protection of information being transferred through various types of facilities.
  + External parties must agree to the secure transfer of business data with [insert Company’s name].
  + All information transferred in electronic messaging must be properly protected.
  + Any confidentiality or non-disclosure agreements of the organization must be acknowledged, reviewed often, and documented.

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