# Operations 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 the secure operations of information processing facilities within and related to [insert Company’s name].

# 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 Operations 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 & 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.12 – Operational Security (A.12.1, A.12.1.1, A.12.1.2., A.12.2.1, A.12.3.1, A.12.4., A.12.5, A.12.6., A.12.7) |
| NIST SP 800-53 v4 | SC-38 |

# 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.

**Operational Procedures and Responsibilities:**

* + A standardized configuration, or baseline, will be established and maintained for all information systems. These baselines will indicate the specifications of information system components (hardware, firmware, and software), their relationship, and their ownership.
    - Changes to an information system must be fully documented and authorized, and must be performed in a controlled manner.
  + Operational procedures will be made available to all applicable users.
  + A change management request should be created for all information system maintenance.
  + Capacity management to ensure appropriate usage of resources will be implemented.
  + Any testing environments will be made separate from the main operational network and facilities.

**Protection from Malware:**

* + Protection against malware should be based on malware detection and repair software, information security awareness, and appropriate system access and change management controls.
  + Anti-virus software should be deployed on all systems commonly affected by malicious software (particularly, personal computers and servers).
  + Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
  + Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy and unauthorized mobile code shall be prevented from executing.

**Backup:**

* + A backup policy must be agreed upon to collect backup copies of necessary data, software, etc. and test them in a timely manner.

**Logging and Monitoring:**

* + Information systems should be configured to record all critical systems activities such as login/logout and administrative changes into a log file.
  + Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed.
  + In addition, the information systems should be configured to notify administrative staff via a Security Information Event Management (SIEM) solution in the event that inappropriate, unusual, and/or suspicious activity is noted.
  + These logging processes and facilities will be protected accordingly.
  + All clocks of the logging and information processing systems will be appropriately synchronized.

**Control of Operational Software:**

* [Insert Company’s name] will implement controls for the implementation of software and to prevent or detect the use of unauthorized software (e.g. application whitelisting)

**Mobile Devices and Teleworking:**

* + Security measures will be developed and adhered to in order to manage risks introduced by the use of mobile devices.
  + Security measures will be implemented to protected information accessed, processed, or stored at teleworking/remote sites.

**Technical Vulnerability Management:**

* + [Insert Company’s name] will implement controls and processes to properly scan and address vulnerabilities in information systems at least [insert frequency – suggested annually], and when new vulnerabilities appear.
  + Appropriate measures should be taken to address associated risks.

**Information Systems Audit Considerations:**

* + Security audits will be conducted [insert frequency – suggested annually] to ensure information system security controls have been implemented correctly, are operating effectively, and are producing the desired level of security.

**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.