# Access Control 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 users have the appropriate access levels specifically authorized to them to access information on systems and applications.

# 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 Access Control 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** |
| ISO/IEC 27001:2013 | A.9 (A.9.1, A.9.2, A.9.3, A.9.4) |
| NIST SP 800-53 v4 | AC-1~AC-25 |

# 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.

**Business Requirements of Access Control:**

* + This access control policy must be developed and reviewed regularly (i.e. annually) based on [Insert Company’s Name] security requirements.
    - [Insert Company’s Name] will employ a role-based access method.
  + Users will only receive access to networks and network systems specifically authorized to them.
    - [Insert Company’s Name] will follow the principle of least privilege.

**User Access Management:**

* + A formal user registration and de-registration process must be developed and initiated to allow assignment of rights.
    - [Insert Company’s Name] will employ use of automated mechanisms to enhance this process.
  + A formal user provisioning process must be in place. This process will allow for the assignment or revocation of access rights for all users to all systems and services.
  + Privileged access rights will be allocated in a highly controlled and restricted process. Their usage will also be controlled.
    - Inactivity logout will be enabled after a pre-determined time period.
  + Secret authentication information allocation will be managed through a formal process.
  + Asset owners must conduct regular reviews of users’ access rights and use of accounts.
  + Upon termination of employment, an employee’s or external party’s user access rights will be revoked.
    - If there is a change to a contract or agreement, then the access will be adjusted appropriately.
    - [Insert Company’s Name] will employ automated processes here to remove temporary and emergency accounts after a determined amount of time. A similar automated process will exist for disabling inactive accounts.
      * [Insert Company’s Name] will also terminate any accounts of high-risk users.

**User Responsibilities:**

* Users must follow [Insert Company’s Name]’s procedures surrounding secret authentication information usage.

**System and Application Access Control:**

* User access to all information and application systems will be restricted based on [Insert Company’s Name]’s access control standards.
  + According to the access control policy, access to systems and applications will be restricted with a secure log-on process.
    - A limit of successive incorrect logons (e.g. six times) will be enforced and an automatic account lock will be enabled.
    - Time and date of logons and account changes will be appropriately recorded and monitored.
  + Network and information systems sessions should remain locked for a predetermined time or until the user reestablishes access through an established authentication procedure.
  + [Insert Company’s Name] will establish appropriate restrictions around remote access, wireless access, and mobile devices.
* Password management systems will be interactive and mandate strong passwords.
* Any use of utility programs capable of overriding system and application controls will be highly controlled and restricted, if necessary.
* Any access to program source code will be strictly prohibited.
* [Insert Company’s Name] will control the flow of information between interconnected systems to ensure secure transfers through measures like encrypted tunnels.
  + When an automated flow control decision is not possible or available, [Insert Company’s Name] will initiate a human review.
* The [Insert Company’s Name] will enact separation of duties to decrease abuse of privileges.
* Access by external information systems will be regulated.
* [Insert Company’s Name] will ensure information sharing process follows appropriate access levels of sharing partners.
  + [Insert Company’s Name] will designate individuals allowed to post information on publicly available systems.
* [Insert Company’s Name] will implement appropriate data mining prevention controls.

**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.