|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Access Control** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Access Control Policy is to establish a comprehensive framework for managing access to organizational information systems and data. By defining roles, responsibilities, and procedures for account management, access enforcement, and monitoring, the policy aims to protect sensitive information from unauthorized access and potential breaches. It ensures that only authorized users can access specific resources based on their roles and responsibilities, thereby supporting the organization's overall security posture. Additionally, the policy mandates regular reviews and audits to ensure compliance with internal and external regulations, ultimately safeguarding the integrity and confidentiality of the organization's information assets.

The Access Control Policy provides numerous benefits that enhance the security and efficiency of the organization. By implementing strict access controls, the policy minimizes the risk of data breaches and unauthorized access, protecting sensitive information from potential threats. It fosters a culture of accountability by clearly defining user roles and responsibilities, which helps in monitoring and managing user activities effectively. The policy also facilitates compliance with regulatory requirements, thereby reducing legal and financial risks. Furthermore, it streamlines access processes, ensuring that employees can efficiently obtain the access they need while maintaining robust security measures. Overall, the policy enhances operational efficiency and builds trust among stakeholders by demonstrating a commitment to information security.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The IT Access Control Policy establishes guidelines to secure organizational information systems by managing user accounts and access privileges effectively. Key components include account management, access enforcement, separation of duties, and the principle of least privilege, ensuring that access is limited to necessary users only. The policy mandates session management practices, specifies security measures for remote and wireless access, and outlines conditions for using external information systems. Additionally, it promotes responsible information sharing while safeguarding nonpublic data and ensures that publicly accessible content is reviewed for compliance. Overall, the policy aims to mitigate risks and protect sensitive information while adhering to relevant laws and regulations.

* 1. Account Management

The [Owner] shall:

1. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.
2. Assign account managers for information system accounts.
3. Establish conditions for group and role membership.
4. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
5. Require approvals by system owners for requests to create information system accounts.
6. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.
7. Monitor the use of information system accounts.
8. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.
9. Authorize access to the information system based on a valid access authorization or intended system usage.
10. Review accounts for compliance with account management requirements quarterly.
11. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
12. Employ automated mechanisms to support the management of information system accounts.
13. Ensure that the information system automatically disables temporary and emergency accounts after usage.
14. Ensure that the information system automatically disables inactive accounts after 90 days.
15. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.
    1. Access Enforcement

The [Owner] shall ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

* 1. Information Flow Enforcement

The [Owner] shall ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

* 1. Separation of Duties

The [Owner] shall:

1. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
2. Document the separation of duties of individuals.
3. Define information system access authorizations to support separation of duties.
   1. Least Privilege

The [Owner] shall:

1. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
2. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.
3. Require that users of information system accounts, or roles, with access to security configuration settings, audit logs, and privileged system administration functions, use non-privileged accounts or roles, when accessing non-security functions.
4. Restrict privileged accounts on the information system to system administrators and designated security personnel.
5. Ensure that the information system audits the execution of privileged functions.
6. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
   1. Unsuccessful Logon Attempts

The [Owner] shall ensure that the information system:

1. Enforces a limit of consecutive invalid logon attempts by a user during a 10-minute period.
2. Locks the account/node automatically for 15 minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
   1. System Notification

The [Owner] shall ensure that the information system:

1. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:
   1. Users are accessing a [Organization Name] information system.
   2. Information system usage may be monitored, recorded, and subject to audit.
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
   4. Use of the information system indicates consent to monitoring and recording.
   5. There are not rights to privacy.
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
3. For publicly accessible systems, the IT Department shall ensure that the information system:
   1. Displays system use information at each logon attempt, before granting further access.
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
   3. Includes a description of the authorized uses of the system.
   4. Session Lock

The [Owner] shall ensure that the information system:

1. Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.
2. Retain the session lock until the user reestablishes access using established identification and authentication procedures.
3. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.
   1. Session Termination

The [Owner] shall ensure that the information system automatically terminates a user session after 60 minutes of inactivity.

* 1. Permitted Actions Without Identification or Authentication

The [Owner] shall:

1. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.
2. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.
   1. Remote Access

The [Owner] shall:

1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
2. Authorize remote access to the information system prior to allowing such connections.
3. Ensure that the information system monitors and controls remote access methods.
4. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
5. Ensure that the information system routes all remote accesses through two managed network access control points to reduce the risk for external attacks.
6. Authorize the execution of privileged commands and access to security-relevant information via remote access only for approved system administrators and security personnel.
7. Document the rationale for such access in the security plan for the information system.
   1. Wireless Access

The [Owner] shall:

1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
2. Authorize wireless access to the information system prior to allowing such connections.
3. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.
   1. Access Control for Mobile Devices

The [Owner] shall:

1. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.
2. Authorize the connection of mobile devices to organizational information systems.
3. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.
   1. Use of External Information Systems

The [Owner] shall:

1. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
   1. Access the information system from external information systems.
   2. Process, store, or transmit organization-controlled information using external information systems.
2. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
   1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan.
   2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
   3. Information Sharing

The [Owner] shall:

1. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for cross-departmental projects or external collaborations.
2. Employ automated mechanisms to assist users in making information sharing/collaboration decisions.
   1. Publicly Accessible Content

The [Owner] shall:

1. Designate individuals authorized to post information onto a publicly accessible information system.
2. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
3. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.
4. Review the content on the publicly accessible information system for nonpublic information annually and removes such information, if discovered.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publication 800-92, Guide to Computer Security Log Management](https://csrc.nist.gov/pubs/sp/800/92/final)

[National Institute of Standards and Technology (NIST) Access Control Policy and Implementation Guides](https://csrc.nist.gov/projects/access-control-policy-and-implementation-guides)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)