Access Control Policy

POLICY # NIST-POL-0100	EFFECTIVE DATE January 1, 2026	APPROVED BY Insert Approver
VERSION # 1.0	LAST REVISED Insert Last Revised Date	REFERENCE NIST Control: AC

Purpose
To limit access to systems to authorized users who work on approved devices to process permitted transactions and functions.

Scope
This policy applies to all ORGANIZATION_NAME workforce members including, but not limited to, full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, authorized third parties, and anyone else granted access to sensitive information by ORGANIZATION_NAME.

Policy
Based on NIST SP 800-171r2 the following represents the requirements of the ORGANIZATION_NAME Access Control Policy:

Basic Security Requirements:

- Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems) (Access Control 3.1.1).
- Limit system access to the types of transactions and functions that authorized users are permitted to execute (Access Control 3.1.2).

Derived Security Requirements:

- Control the flow of CUI in accordance with approved authorizations (Access Control 3.1.3).
- Separate the duties of individuals to reduce the risk of malevolent activity without collusion (Access Control 3.1.4).
- Employ the principle of least privilege, including for specific security functions and privileged accounts (Access Control 3.1.5).
- Use non-privileged accounts or roles when accessing non-security functions (Access Control 3.1.6).
- Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs (Access Control 3.1.7).
- Limit unsuccessful logon attempts (Access Control 3.1.8).
- Provide privacy and security notices consistent with applicable CUI rules (Access Control 3.1.9).
- Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity (Access Control 3.1.10).
- Terminate (automatically) a user session after a defined condition (Access Control 3.1.11).

- Monitor and control remote access sessions (Access Control 3.1.12).
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions (Access Control 3.1.13).
- Route remote access via managed access control points (Access Control 3.1.14).
- Authorize remote execution of privileged commands and remote access to security-relevant information (Access Control 3.1.15).
- Authorize wireless access prior to allowing such connections (Access Control 3.1.16).
- Protect wireless access using authentication and encryption (Access Control 3.1.17).
- Control connection of mobile devices (Access Control 3.1.18).
- Encrypt CUI on mobile devices and mobile computing platforms (Access Control 3.1.19).
- Verify and control/limit connections to and use of external systems (Access Control 3.1.20).
- Limit use of portable storage devices on external systems (Access Control 3.1.21).
- Control CUI posted or processed on publicly accessible systems (Access Control 3.1.22).

Responsibilities
The Information Security Officer is responsible for ensuring compliance with this policy. Additionally, all individuals, groups, and organizations identified herein are responsible for compliance with NIST SP 800-171r2 policies.

The ORGANIZATION_NAME Information Security Officer, is responsible for:

- The development, implementation, and maintenance of ORGANIZATION_NAME security policies.
- Working with employees to develop procedures and plans in support of security policies.

The Information Security Officer is responsible for conducting at least an annual review of the Access Control Policy, making any appropriate changes and disseminating the updated policy to workforce members.

Retention
Every policy and procedure revision/replacement will be maintained for a minimum of six (6) years from the date of its creation or when it was last in effect, whichever is later. Other ORGANIZATION_NAME requirements may stipulate a longer retention. Log-in audit information and logs relevant to security incidents must be retained for six (6) years or a longer period, depending on the strictest regulatory mandate.

Compliance
Failure to comply with this or any other security policy results in disciplinary actions as outlined in the Personnel Sanctions Policy. Legal actions may also be taken for violations of applicable regulations and standards.

Related Form(s) and Evidence

- None

References

- NIST Special Publication 800-171r2
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- NIST Special Publication 800-53 Revision 5
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Contact

Insert Contact Person
Insert Full Address

E: Insert Email ID P: Insert Phone No. F: Insert Fax No.

Policy History

Initial effective date: January 1, 2026