|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **Configuration Management Policy** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 1.0 Purpose and Benefits

# To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with IT security policies, standards, and procedures.

# 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 [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

Needed

### Identification and Authentication

The [Owner] shall:

* 1. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of [Organization Name] users.
  2. Ensure that information systems implement multifactor authentication for network access to privileged accounts.
  3. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.
  4. Ensure that information systems implement multifactor authentication for local access to privileged accounts.
  5. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.
  6. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.
  7. Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials.

### Device Identification and Authentication

The [Owner] shall:

1. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

### Identifier Management

The [Owner] shall:

1. Ensure that the [entity] manages information system identifiers by receiving authorization from [entity defined personnel or roles] to assign an individual, group, role, or device identifier.

# 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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

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

# 10.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publications (SP):   
NIST SP 800-53a – Contingency Planning (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84; NIST Federal Information Processing Standards (FIPS) 199

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Configuration Management (CM)

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116;

Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140