|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **System and Communication Protection** | **Updated:** 10/29/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the System and Communication Protection Policy is to establish guidelines for safeguarding the organization’s information systems and communication channels against unauthorized access, data breaches, and other security threats. By implementing effective controls and best practices, the policy aims to ensure the confidentiality, integrity, and availability of sensitive information across all platforms and formats.

This policy enhances the organization's cybersecurity posture by providing a structured approach to protecting information assets and communication processes. It promotes the secure management of user and device access, reduces the risk of data leaks through shared resources, and safeguards against denial of service attacks. By adhering to this policy, the organization can foster trust among employees and stakeholders while ensuring compliance with relevant regulations and standards.

# 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 System and Communication Protection Policy applies to all employees, contractors, and third-party vendors who access the organization’s information systems, whether onsite or remotely. It encompasses all forms of communication and information storage, including electronic, paper-based, and verbal formats. All users must adhere to the established security measures to protect sensitive information, with non-compliance potentially resulting in disciplinary action. Key controls include application partitioning, boundary protection, cryptographic management, and session authenticity, all designed to ensure robust security and data protection across the organization.

* 1. Application Partitioning

The [Owner] shall:

1. Separate user functionality from information system management functionality either logically or physically.
2. Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.
   1. Information in Shared Resources

The [Owner] shall:

1. Prevent unauthorized and unintended information transfer via shared system resources.
2. This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.
   1. Denial of Service Protection

The [Owner] shall:

1. Ensure that the information system protects against or limit the effects of the following types of denial of service attacks: [entity defined types of denial of service attacks] by employing [entity defined security safeguards].
2. The information system restricts the ability of individuals to launch [entity defined denial of service attacks] against other information systems.
   1. Boundary Protection

The [Owner] shall:

1. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.
2. Implement sub-networks for publicly accessible system components that are [physically; logically] separated from internal organizational networks, and connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
3. Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.
   1. Transmission Confidentiality and Integrity

The [Owner] shall:

1. Deploy information systems that protect the [confidentiality; integrity] of transmitted information.
2. This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).
   1. Network Disconnect

The [Owner] shall:

1. Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after [entity defined time period] of inactivity; this control applies to both internal and external networks.
2. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.
   1. Cryptographic Key Establishment and Management

The [Owner] shall establish and manage cryptographic keys for required cryptography employed within the information system in accordance with [entity defined requirements for key generation, distribution, storage, access, and destruction].

* 1. Cryptographic Protection

The [Owner] shall:

1. Implement [entity defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal and state laws, directives, policies, regulations, and standards.
2. Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.
   1. Collaborative Computing Devices

The [Owner] shall:

1. Prohibit remote activation of collaborative computing devices with the following exceptions: [entity defined exceptions where remote activation is to be allowed].
2. Provide an explicit indication of use to users physically present at the devices.
3. Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.
   1. Public Key Infrastructure Certificates

The [Owner] shall:

1. Issue public key certificates under a [defined certificate policy] or obtain public key certificates from an approved service provider.
2. Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.
   1. Mobile Code

The [Owner] shall:

1. Define acceptable and unacceptable mobile code and mobile code technologies.
2. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.
3. Authorize, monitor, and control the use of mobile code within the information system.
4. Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.
   1. Voice Over Internet Protocol

The [Owner] shall:

1. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.
2. Authorize, monitor, and control the use of VoIP within the information system.
   1. Secure Name/Address Resolution Service (Authoritative Source)

The [Owner] shall:

1. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
2. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
3. This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.
   1. Secure Name/Address Resolution Service (Recursive or Cashing Resolver)

The [Owner] shall:

1. Ensure information systems that requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
2. Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.
   1. Architecture and Provisioning for Name/Address Resolution Service

The [Owner] shall:

1. the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
2. Employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server, to eliminate single points of failure and to enhance redundancy.
3. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.
   1. Session Authenticity

The [Owner] shall:

1. Ensure the information system protects the authenticity of communications sessions.
2. This control addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.
   1. Protection of Information at Rest

The [Owner] shall:

1. Ensure the information system protects the [confidentiality; integrity] of [entity defined information at rest].
2. This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.
   1. Process Isolation

The [Owner] shall:

1. Ensure the information system maintains a separate execution domain for each executing process.
2. Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

# 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 Publications (SP): NIST SP800-28 - Guidelines on Active Content and Mobile Code](https://csrc.nist.gov/pubs/sp/800/28/ver2/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-41 - Guidelines on Firewalls and Firewall Policy](https://csrc.nist.gov/pubs/sp/800/41/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-52 - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations](https://csrc.nist.gov/pubs/sp/800/52/r2/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-56 - Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography](https://csrc.nist.gov/pubs/sp/800/56/a/r3/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-57 - Recommendation for Key Management: Part 1 – General](https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-58 - Security Considerations for Voice Over IP Systems](https://csrc.nist.gov/pubs/sp/800/58/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-77 - Guide to IPsec VPNs](https://csrc.nist.gov/pubs/sp/800/77/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-81 - Secure Domain Name System (DNS) Deployment Guide](https://csrc.nist.gov/pubs/sp/800/81/2/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-95 - Guide to Secure Web Services](https://csrc.nist.gov/pubs/sp/800/95/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-111 - Guide to Storage Encryption Technologies for End User Devices](https://csrc.nist.gov/pubs/sp/800/111/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-113 - Guide to SSL VPNs](https://csrc.nist.gov/pubs/sp/800/113/final)