|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Systems and Services Acquisition** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The Systems and Services Acquisition Policy aims to establish a framework for the secure acquisition of information systems, components, and services. This policy ensures that security considerations are integrated into the procurement process, safeguarding the organization’s information assets throughout their lifecycle. By defining clear guidelines and requirements for security functionality and documentation, this policy seeks to mitigate risks associated with the acquisition of technology and services.

Implementing the Systems and Services Acquisition Policy provides multiple benefits, including enhanced security posture and compliance with regulatory requirements. By ensuring that security requirements are incorporated into the acquisition process, the organization minimizes vulnerabilities that could be exploited by threats. Additionally, the policy promotes accountability and transparency in procurement activities, fostering a culture of security awareness among stakeholders. Overall, this proactive approach helps protect the confidentiality, integrity, and availability of sensitive information, thereby supporting the organization’s mission and business objectives.

# 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 Systems and Services Acquisition Policy outlines the necessary steps and considerations for acquiring information systems and services, applicable to all employees, contractors, and third-party vendors. Key components include the allocation of resources for security, adherence to security controls during the acquisition process, and documentation requirements for security-related information.

The policy mandates that all acquisitions comply with relevant laws and standards while ensuring that security roles and responsibilities are clearly defined throughout the system development lifecycle. By following these guidelines, the organization aims to safeguard its information systems from potential risks associated with external services and components. Non-compliance with this policy may lead to disciplinary action, reinforcing the importance of security in procurement practices.

* 1. Allocation of Resources

The [Owner] in direct guidance and association with the information system owner shall:

1. Determine information security requirements for the information system or information system service in mission/business process planning.
2. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.
3. Establish a discrete line item for information security in organizational programming and budgeting documentation.
   1. System Development Life Cycle

The [Owner] shall in direct guidance and association with the information system owner shall develop a contingency plan for the information system that:

1. Manages the information system using the system development life cycle to ensure incorporation information security considerations.
2. Defines and documents information security roles and responsibilities throughout the system development life cycle.
3. Identifies individuals having information security roles and responsibilities.
4. Integrates the information security risk management process into system development life cycle activities.
   1. Acquisition Process

The [Owner] shall ensure the acquisition process includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal, state, and local laws, Executive Orders, directives, policies, regulations, standards, guidelines, and mission and business needs:

1. Security functional requirements.
2. Security strength requirements.
3. Security assurance requirements.
4. Security-related documentation requirements.
5. Requirements for protecting security-related documentation.
6. Description of the information system development environment and environment in which the system is intended to operate.
7. Acceptance criteria.
   1. Security Controls

The [Owner] shall require the information system, system component, or information system service:

1. Describe the functional properties of the security controls to be employed; security-relevant external system interfaces; high-level design, low-level design, source code or hardware schematics that meet the business requirements.
2. Identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.
3. Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within information systems.
   1. Information System Documentation

The [Owner] shall:

1. Obtain administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service.
   2. Effective use and maintenance of security functions/mechanisms.
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
2. Obtain user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.
   3. User responsibilities in maintaining the security of the system, component, or service.
3. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [entity defined actions] in response.
4. Protect documentation as required, in accordance with the risk management strategy.
5. Distribute documentation to only authorized persons or entities.
   1. Security Engineering Principles

The [Owner] shall apply industry standard information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

* 1. External Information System Services

The [Owner] shall:

1. Require that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
2. Define and document government oversight and user roles and responsibilities with regard to external information system services.
3. Employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.
4. Require providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.
   1. Developer Configuration Management

The [Owner] shall ensure developers of the information system, system component, or information system service:

1. Perform configuration management during system, component, or service design; development, implementation, and/or operation.
2. Document, manage, and control the integrity of changes to configuration items under configuration management.
3. Implement only organization-approved changes to the system, component, or service.
4. Document approved changes to the system, component, or service and the potential security impacts of such changes.
5. Track security flaws and flaw resolution within the system, component, or service and report findings to authorized personnel and/or business units.
   1. Developer Configuration Requirements

The [Owner] shall:

1. Require the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.
2. Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.
3. Require the developer of the information system, system component, or information system service to enable integrity verification of hardware components.
4. Require the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous versions.
5. Require the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.
6. Require the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.
   1. Developer Security Testing and Evaluation

The [Owner] shall require the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan.
2. Perform unit; integration; system; regression testing/evaluation.
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
4. Implement a verifiable flaw remediation process.
5. Correct flaws identified during security testing/evaluation.
6. Employ static code analysis tools to identify common flaws and document the results of the analysis.
7. Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.
   1. Independent Verification of Assessment Plans and Evidence

The [Owner] shall:

1. Require an independent agent satisfying to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation.
2. Ensure that the independent agent either is provided with sufficient information to complete the verification process or has been granted the authority to obtain such information.
3. Perform a manual code review of defined processes, procedures, and/or techniques.
4. Perform penetration testing.
5. Verify that the scope of security testing/evaluation provides complete coverage of required security controls.
6. Employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

# 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 SP 800-35 – Guide to Information Technology Security Services](https://csrc.nist.gov/pubs/sp/800/35/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-37 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](https://csrc.nist.gov/pubs/sp/800/37/r2/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-70 – National Checklist Program for IT Products: Guidelines for Checklist Users and Developers](https://csrc.nist.gov/pubs/sp/800/70/r4/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-128 – Guide for Security-Focused Configuration Management of Information Systems](https://csrc.nist.gov/pubs/sp/800/128/upd1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-137 – Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/137/final)