**Template Instructions**

Systems and Services Acquisition Policy

Follow the instructions below to complete this policy template for use within your own organization.

1. Click each bracketed field below to input basic policy information:

* **Organization Name *(e.g. ACME Co)*:**

[Organization Name]

* **Organization Address *(e.g. 123 Elm St. City, ST. 12345)*:**

[Organization Address]

* **Policy Authority *(e.g. CEO, CIO, or CISO)*:**

[Policy Authority]

* **Policy Owner *(e.g. IT Department)*:**

[Policy Owner]

* **Owner Contact Info *(e.g.*** [***jon.smith@acme.com***](mailto:jon.smith@acme.com)***)*:**

[Owner Contact Info]

* **Policy Number *(e.g. POL-INFOSEC-01)*:**

[Policy Number]

1. Thoroughly review all 10 Policy Sections to ensure accuracy and alignment with existing organizational policies, procedures, and standards.
2. Input key term definitions that require clarification into Section 7.
3. Review related documents in Section 10.
4. Save the document and print the necessary pages to a PDF or printer.
5. Visit [docs.policytemplates.online](https://docs.policytemplates.online/) for further policy/standard creation and implementation resources.

|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Systems and Services Acquisition** | **Updated:** 11/1/2024 |
| **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. System Security Plan

The [Policy Owner] shall:

1. Develop a security plan for each information system that:
   1. Is consistent with [Organization Name]’s enterprise architecture.
   2. Defines explicitly the authorization boundary for the system.
   3. Describes the operational context of the information system in terms of missions and business processes.
   4. Provides the security categorization of the information system including supporting rationale.
   5. Describes the operational environment for the information system and relationships with or connections to other information systems.
   6. Provides an overview of the security requirements for the system.
   7. Identifies any relevant overlays, if applicable.
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
2. Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel and/or business units.
3. Review the security plan for the information system at least annually.
4. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
5. Protect the security plan from unauthorized disclosure and modification.
   1. Rules of Behavior

The [Policy Owner] shall:

1. Establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.
2. Receive a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
3. Review and update the rules of behavior.
4. Require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised and updated.
   1. Information Security Architecture

The [Policy Owner] shall:

1. Develop information security architecture for the information system that will:
   1. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.
   2. Describe how the information security architecture is integrated into and supports the enterprise architecture.
   3. Describe any information security assumptions and dependencies on external services.
2. Review and update the information security architecture no less than annually, to reflect updates in the enterprise architecture.
3. Ensure that planned information security architecture changes are reflected in the security plan, the security operations and procurements/acquisitions.
   1. Defense in Depth Approach

The [Policy Owner] shall design security architecture using a defense-in-depth approach that:

1. Allocates security safeguards to [Organization Name] defined locations and architectural layers.
2. Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

# 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 [Policy 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 [Policy 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]

[Owner 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)