|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Security Assessment and Authorization** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

Information Technology (IT) and the various business units (information owners) will ensure security controls in information systems, and the environments in which those systems operate, as part of initial and ongoing security authorizations, annual assessments, continuous monitoring and system development life cycle activities.

# 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

This policy ensures that a structured and repeatable process is followed to assess and authorize the security posture of the organization's information systems. By defining clear roles and responsibilities, it establishes a framework for conducting comprehensive security assessments and authorizing system use based on the results. The policy ensures that security controls are regularly tested for effectiveness, system interconnections are managed securely, and continuous monitoring is implemented to detect emerging threats. These measures reduce vulnerabilities and support informed decision-making, contributing to the overall protection of the organization’s IT assets and data.

* 1. Security Assessment and Authorization Policy and Procedures

The [Organization Name] shall:

1. Develop, document, and disseminate to designated personnel such as IT staff, security teams, and management:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.
2. Review and update the current security assessment and authorization policy and procedures annually or bi-annually.
   1. Security Assessments

The [Organization Name] shall:

1. Develop a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment.
   2. Assessment procedures to be used to determine security control effectiveness.
   3. Assessment environment, assessment team, and assessment roles and responsibilities.
2. Assess the security controls in the information system and its environment of operation quarterly or semi-annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.
3. Produce a security assessment report that documents the results of the assessment.
4. Provide the results of the security control assessment to [Authority].
   1. System Interconnections

The [Organization Name] shall:

1. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.
2. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.
3. Review and update Interconnection Security Agreements annually or as necessary. Entities must establish processes for the establishment, operation and, as appropriate, integration of log management systems.
4. Employ an allow-all, deny-by-exception, deny-all, permit-by-exception, policy for allowing critical and sensitive information systems to connect to external information systems.
   1. Plan of Action and Milestones

The [Organization Name] shall:

1. Develop a plan of action and milestones for the information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
2. Update existing plan of action and milestones quarterly or after each significant assessment based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
   1. Security Authorization

The [Organization Name] shall:

1. Assign a senior-level executive or manager as the authorizing official for the information system.
2. Ensure that the authorizing official authorizes the information system for processing before commencing operations.
3. Update the security authorization annually or whenever there are significant changes to the system.
   1. Continuous Monitoring

The [Owner] shall develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

1. Establishment of entity-defined key performance indicators (KPIs) and security metrics to be monitored.
2. Establishment of monthly monitoring frequencies and semi-annual assessment frequencies supporting such monitoring.
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.
5. Correlation and analysis of security-related information generated by assessments and monitoring.
6. Response actions to address results of the analysis of security-related information.
7. Reporting the security status of organization and the information system to the [Authority] senior management team or Board of Directors quarterly.
   1. Internal System Connections

The [Owner] shall:

1. Authorize internal connections of specific system components such as servers, databases, and applications to the information system.
2. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

# 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) SP 800-30, Guide for Conducting Risk Assessments](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final" \t "_blank)

[National Institute of Standards and Technology (NIST) SP 800-39, Managing Information Security Risk](https://csrc.nist.gov/publications/detail/sp/800-39/final#:~:text=The%20purpose%20of%20Special%20Publication,the%20Nation%20resulting%20from%20the)

[National Institute of Standards and Technology (NIST) SP 800-92, Guide to Computer Security Log Management](https://csrc.nist.gov/pubs/sp/800/92/final)

[National Institute of Standards and Technology (NIST) SP 800-53a, Assessing Security and Privacy Controls in Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/53/a/r5/final)

[National Institute of Standards and Technology (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) SP 800-47 Rev. 1. Managing the Security of Information Exchanges](https://csrc.nist.gov/pubs/sp/800/47/r1/final)

[National Institute of Standards and Technology (NIST) SP 800-115, Technical Guide to Information Security Testing and Assessment](https://csrc.nist.gov/pubs/sp/800/115/final)

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