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

# 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 [Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to users of any system’s information or physical infrastructure regardless of its form or format, created or used to support the organization. It is the user’s responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organization’s Information Security Policy and its associated standards.

# 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.

### Security Assessment and Authorization Policy and Procedures

The [Organization Name] shall:

* 1. Develop, document, and disseminate to [entity defined personnel or roles]:

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.
   1. Review and update the current security assessment and authorization policy and procedures [entity defined frequency].

### Security Assessments

The [Organization Name] shall:

1. Develop a security assessment plan that describes the scope of the assessment including:
2. Security controls and control enhancements under assessment.
3. Assessment procedures to be used to determine security control effectiveness.
4. Assessment environment, assessment team, and assessment roles and responsibilities.
5. Assess the security controls in the information system and its environment of operation [entity defined frequency] 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.
6. Produce a security assessment report that documents the results of the assessment.
7. Provide the results of the security control assessment to [Authority].

### System Interconnections

The [Owner] 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 [entity defined frequency]. 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 [entity defined information systems] to connect to external information systems.

### 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 [entity defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

### 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 [entity defined frequency].

### 4.6 Continuous Monitoring

The [Owner] shall:

1. Develop a continuous monitoring strategy and implement a continuous monitoring program that includes:
2. Establishment of [entity defined metrics] to be monitored.
3. Establishment of [entity defined frequencies] for monitoring and [entity defined frequencies] for assessments supporting such monitoring.
4. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.
5. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.
6. Correlation and analysis of security-related information generated by assessments and monitoring.
7. Response actions to address results of the analysis of security-related information.
8. Reporting the security status of organization and the information system to [Authority] [entity defined frequency].

### 4.7 Continuous Monitoring

The [Owner] shall:

1. Authorize internal connections of [entity defined information system components or classes of components] 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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 8.0 Revision History

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

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

# 10.0 Related Documents

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

[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)

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

[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)

[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)

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

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

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