Policy #:	Title:	Effective Date:
x.xx	Security Assessment and Authorization Policy	MM/DD/YYYY

PURPOSE

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.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Security Assessment and Authorization (CA), NIST SP 800-12, NIST SP 800-37, NIST SP 800-39, NIST SP 800-47, NIST SP 800-100, NIST SP 800-115, NIST SP 800-137; NIST Federal Information Processing Standards (FIPS) 199

POLICY

This policy is applicable to all departments and users of IT resources and assets. Every department that maintains or collects informational assets must be compliant with this policy.

1. SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
   The [entity] shall:

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

      i. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

      ii. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.

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

2. SECURITY ASSESSMENTS
   The [entity] shall:

   a. Develop a security assessment plan that describes the scope of the assessment including:

i. Security controls and control enhancements under assessment.

ii. Assessment procedures to be used to determine security control effectiveness.

iii. Assessment environment, assessment team, and assessment roles and responsibilities.

b. 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.

c. Produce a security assessment report that documents the results of the assessment.

d. Provide the results of the security control assessment to [entity defined individuals or roles].

3. SYSTEM INTERCONNECTIONS
IT Department shall:

a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.

b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

c. Review and update Interconnection Security Agreements [entity defined frequency].

d. 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.

4. PLAN OF ACTION AND MILESTONES
The [entity] shall:

a. 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.

b. 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.

5. SECURITY AUTHORIZATION
The [entity] shall:

a. Assign a senior-level executive or manager as the authorizing official for the information system.

b. Ensure that the authorizing official authorizes the information system for processing before commencing operations.

c. Update the security authorization [entity defined frequency].

6. CONTINUOUS MONITORING
IT Department shall:

a. Develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

i. Establishment of [entity defined metrics] to be monitored.

ii. Establishment of [entity defined frequencies] for monitoring and [entity defined frequencies] for assessments supporting such monitoring.

iii. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

iv. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

v. Correlation and analysis of security-related information generated by assessments and monitoring.

vi. Response actions to address results of the analysis of security-related information.

vii. Reporting the security status of organization and the information system to [entity defined personnel or roles] [entity defined frequency].

7. INTERNAL SYSTEM CONNECTIONS
IT Department shall:

a. Authorize internal connections of [entity defined information system components or classes of components] to the information system.

b. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY