Policy #:	Title:	Effective Date:
x.xx	Planning Policy	MM/DD/YYYY

PURPOSE

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Security Planning (PL), NIST SP 800-12, SP NIST 800-18, NIST SP 800-100

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. SYSTEM SECURITY PLAN
   IT Department shall:

   a. Develop a security plan for each information system that:

      i. Is consistent with the [entity's] enterprise architecture.

      ii. Defines explicitly the authorization boundary for the system.

      iii. Describes the operational context of the information system in terms of missions and business processes.

      iv. Provides the security categorization of the information system including supporting rationale.

      v. Describes the operational environment for the information system and relationships with or connections to other information systems.

      vi. Provides an overview of the security requirements for the system.

      vii. Identifies any relevant overlays, if applicable.

      viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.

        ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

    b. Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel and/or business units.

    c. Review the security plan for the information system at least annually.

    d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

    e. Protect the security plan from unauthorized disclosure and modification.

2. RULES OF BEHAVIOR
   IT Department shall:

    a. 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.

    b. 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.

    c. Review and update the rules of behavior.

    d. 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.

3. INFORMATION SECURITY ARCHITECTURE
   IT Department shall:

    a. Develop information security architecture for the information system that will:

        i. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.

        ii. Describe how the information security architecture is integrated into and supports the enterprise architecture.

        iii. Describe any information security assumptions and dependencies on external services.

   b. Review and update the information security architecture no less than annually, to reflect updates in the enterprise architecture.

   c. Ensure that planned information security architecture changes are reflected in the security plan, the security operations and procurements/acquisitions.

4. DEFENSE-IN-DEPTH APPROACH
   IT Department shall:

   a. Design security architecture using a defense-in-depth approach that:

      i. Allocates security safeguards to [entity] defined locations and architectural layers.

      ii. Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

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 and Information System Owners

DATE ISSUED/DATE REVIEWED

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