ADMINISTRATIVE POLICY MANUAL	**SECTION** Information Technology	**NUMBER** AM-1200-5	**EFFECTIVE DATE** 01/31/2023
	SUBJECT Planning		PAGE Page 1 of 7

I. Purpose

Systems that support operations contribute to the strategic goals and objectives of the county. Therefore, proper planning is required to ensure systems provide a security level commensurate with the risk associated with the operation of the system, improve productivity and performance, and enable new capabilities over time. Planning is essential in the development and implementation of the county's information security goals. System security plans (SSPs) are the fundamental methods to communicate the security requirements of the system and document how the security controls and controls meet those security requirements. Through planning, the County must develop, document, and disseminate how controls are implemented, rules that describe the responsibility of users, and how the county operates the system from a perspective of information security.

Control requirements, and hence policy statements, are based on the adoption strategy defined by the Information Technology Department which are denoted by either threshold (T) or objective (O) based on current and future capabilities of the security program.

II. Scope

This policy applies to all staff, contractors, and consultants that are employed or contracted with the divisions of the Indian River Board of County Commissioners, including its officers, departments, and special dependent districts. This includes the information technology governance of system operations for divisions including Human Resources, Budget, Information Technology, Community Development, Parks and Recreation, Emergency Services, Public Works, Utility Services, County Attorney's Office, the Emergency Services District, the Solid Waste Disposal District and General Services.

III. Definitions

Information Systems and Telecommunications (IS&T) – The division of Indian River County that supports the various departments with technology solutions and IT service operations.

Concept of operations (CONOP) - A security-focused description of a system, its operational policies, classes of users, interactions between the system and its users, and the system's contribution to the operational mission.

Authorizing Official – An individual responsible for operating an information system at an acceptable level of risk to County operations.

Designated Representative – An individual acting on behalf of the authorizing official in carrying out and coordinating some or all activities associated with security authorization of County systems

IV. Policy

1. Supporting Planning Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the information system security planning policy. [PL-1-T]

The Information Systems and Telecommunications (IS&T) division shall:

a. Develop, document, and disseminate to all staff, contractors, and consultants in their respective divisions as outlined in the scope of this policy, procedures to facilitate the implementation of the planning policy and the associated planning controls

b. Review and update the current planning procedures annually and following advisements or recommendations from assessments and audits, the threat level to County operations based on recent security incidents, breaches, or changes in applicable laws, regulations, and policies. [PL-1-T]

2. System Security and Privacy Plans

The Information Systems and Telecommunications (IS&T) division shall:

a. Develop security and privacy plans for the system that:

i. Are consistent with the County’s enterprise architecture;
ii. Explicitly define the constituent system components;
iii. Describe the operational context of the system in terms of mission and business processes;
iv. Identify the individuals that fulfill system roles and responsibilities;
v. Identify the information types processed, stored, and transmitted by the system;
vi. Provide the security categorization of the system, including supporting rationale;
vii. Describe any specific threats to the system that are of concern to the County;

viii. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
ix. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
x. Provide an overview of the security and privacy requirements for the system;
xi. Identify any relevant control baselines or overlays, if applicable;
xii. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
xiii. Include risk determinations for security and privacy architecture and design decisions;
xiv. Include security and privacy-related activities affecting the system that require planning and coordination with key personnel within County operations that include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing; and
xv. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to key personnel that are responsible for security and privacy planning within County operations;

c. Review the plans annually;

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification. *[PL-2-T]*

3. Rules of Behavior

The Information Systems and Telecommunications (IS&T) division shall:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented 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 system;

c. Review and update the rules of behavior annually; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge through literacy training and awareness and role-based training programs conducted by the County. *[PL-4-T]*

e. Include in the rules of behavior, restrictions on:
   i. Use of social media, social networking sites, and external sites/applications;
   ii. Posting County information on public websites; and
   iii. Use of County-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications. *[PL-4(1)-T]*

4. Concept of Operations

The Information Systems and Telecommunications (IS&T) division shall:

a. Develop a Concept of Operations (CONOPS) for the system describing how the County intends to operate the system from the perspective of information security and privacy; and

b. Review and update the CONOPS annually. *[PL-7-O]*

5. Security and Privacy Architectures

The Information Systems and Telecommunications (IS&T) division shall:

a. Develop security and privacy architectures for the system that:

   i. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of County information;
   ii. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
   iii. Describe how the architectures are integrated into and support the enterprise architecture; and
   iv. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures annually or when security and privacy-related requirements change to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, County procedures, and procurements and acquisitions. *[PL-8-T]*

d. Design the security and privacy architectures for the system using a defense-in-depth approach that:

   i. Allocates various controls deployed and managed by IS&T operational staff to the various architectural layers that include internal and external (DMZ, Extranet, and perimeter) network segments, host-based solutions, and separation methods for system and user functionality; and

   ii. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner. *[PL-8(1)-T]*

e. Require that various controls deployed and managed by IS&T operational staff allocated to the various architectural layers that include internal and external (DMZ, Extranet, and perimeter) network segments, host-based solutions, and separation methods for system and user functionality are obtained from different suppliers. *[PL-8(2)-O]*

6. Central Management

The Information Systems and Telecommunications (IS&T) division shall:

a. Centrally manage:
   - Remote access
   - Identity Access Management (IAM)
   - Wireless access
   - Perimeter defense (firewall)
   - Mobile Device Management (MDM)
   - Information flow enforcement
   - Event logging and correlation
   - Endpoint Detections and Response (EDR) *[PL-9-T]*

7. Baseline Selection

The Information Systems and Telecommunications (IS&T) division shall ensure that the information system(s):

a. Select a control baseline for the system. *[PL-10-T]*

8. Baseline Tailoring

The Information Systems and Telecommunications (IS&T) division shall:

a. Tailor the selected control baseline by applying specified tailoring actions. *[PL-11-T]*

VI. Disciplinary Action

All employees found to have violated any of the policy statements defined within this policy will be subject to discipline up to and including dismissal in accordance with County policy.

VII. Procedures, Guidelines, Forms and Other Related Resources

VIII. References

NIST Security and Privacy Controls for Information Systems and Organizations (800.53 Rev.5)

Guide to Industrial Control Systems (ISC) Security (800.82 Rev.2)

IX. Responsibility

Information Technology Department

X. Authority Approval and Signature

Approved:

____

Michael Zito

Interim County Administrator

XI. History

VERSION	DATE	CHANGES	DEPT/INDIVIDUAL
1.0	01.01.23	Initial Publication	IT/D. Russell