I. Purpose

Awareness and Training are the methods through education to enhance the general security knowledge of all users on the County's systems and network infrastructure. The outcome of these methods includes elevated awareness for the need and requirement to protect the County's systems and resources, develop the skills and knowledge for staff to perform their duties securely, and promote risk-aware decisions throughout every process and within every throughout the County.

The purpose of this policy is to ensure proper governance and guidance of the County's information systems security awareness and training program. Control requirements, and hence policy statements, are based on the adoption strategy defined by the Information Systems and Telecommunications (IS&T) division 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, external agencies, 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

Advanced Persistent Threat (APT) – An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the County's operating environment for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of the County's mission, program, or general operations.

Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.

Human Resources – Responsible for the formulation and administration of personnel policies that create a fair, safe and lawful working environment conducive to productivity for all County personnel.

Incident – An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, and/or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies defined by the County.

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

Event – Any observable occurrence in a network or information system within or against the County's digital footprint of technological capabilities.

Personally Identifiable Information (PII) – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Social engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Social mining – The process of obtaining information from various sources and means to formulate patterns, form conclusions, and act upon the information to construct various attacks

Threat - Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service

IV. Policy

1. Literacy Training and Awareness

The Director of Information Technology shall manage the development, documentation, and dissemination of the awareness and training policy. *[AT-1-T]*

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

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

   I. As part of initial training for new users and on an annual cadence thereafter; and
   II. Upon initiating a contract with a consultant or other contracting agency.

III. When required by significant system changes or following:
- a credible threat against the County
- a past breach or incident against the County's systems or operating environment, or
- the overall change within the threat landscape at either the County, State or Nation level.

b. Employ the following techniques to increase the security and privacy awareness of system users through:
- periodic email communications to users
- posters and pamphlets and
- periodic awareness discussions with County staff, contractors and consultants to reinforce security and privacy awareness training.

c. Update training and awareness content on a periodic basis and following:

- advisements or recommendations from assessments and audits
- threat level updates due to any recent security incidents or breaches affecting similar organizations, entities and/or types of data.
- changes in applicable laws, regulations, and policies.

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques. *[AT-2-T]*

e. Provide practical exercises in literacy training that simulate events and incidents. *[AT-2(1)-T]*

f. Provide literacy training on recognizing and reporting potential indicators of insider threat. *[AT-2(2)-T]*

g. Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining. *[AT-2(3)-T]*

h. Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using various tools and techniques that lead to or are the result of:

- Unknown applications within the system
- Unauthorized setting changes on endpoints
- Unusual activity from administrator or privileged accounts
- Unusual or high levels of inbound and outbound network traffic *[AT-2(4)-T]*

i. Provide literacy training on the Advanced Persistent threat (APT). *[AT-2(5)-T]*

j. Provide literacy training on the cyber threat environment and reflect current cyber threat information in system operations. *[AT-2(6)-T]*

2. Role-Based Training

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

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities which include senior managers, system owners, information owners, and security administrators:

   I. Before authorizing access to the system, information, or performing assigned duties, and on annual basis thereafter; and

   II. When required by system or network changes;

b. Update role-based training content on a periodic basis and following:
   - advisements or recommendations from assessments and audits
   - threat level updates due to any a recent security incidents or breaches affecting similar organizations, entities and/or types of data.
   - changes in applicable laws, regulations, and policies; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training. *[AT-3-T]*

d. Provide selected or qualified staff with initial and annual training in the employment and operation of environmental controls. *[AT-3(1)-O]*

e. Provide selected or qualified staff with initial and annual training in the employment and operation of physical security controls. *[AT-3(2)-O]*

f. Provide practical exercises in security and privacy training that reinforce training objectives. *[AT-3(3)-O]*

g. Provide all applicable staff with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls. *[AT-3(5)-T]*

3. Training Records

The Information Systems and Telecommunications (IS&T) division, in coordination with the Human Resources Department, shall:

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for proper reporting and trend analysis purposes. *[AT-4-T]*

4. Training Feedback

The Information Systems and Telecommunications (IS&T) division, in coordination with Human Resources department, shall:

a. Provide feedback on organizational training results to the following personnel on frequent basis:
   - Managers of direct county staff, contractors and/or consultants
   - Senior management and
   - Various audiences based on need or insight. *[AT-6-T]*

V. 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.

VI. Procedures, Guidelines, Forms and Other Related Resources

None

VII. 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)

VIII. Responsibility

Information Technology Department

IX. Authority Approval and Signature

Approved:

_____

Michael Zito

Interim County Administrator

X. History

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