I. Purpose

This policy establishes the Personnel Security Policy, for managing risks to the controls implemented within systems and within the organization. The Personnel Security policy helps Indian River County implement security best practices and manage risk with employees and/or contractors to ensure that not only the physical environment is secure but also the logical environment.

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

Personnel Security – The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.

Personnel Screening – Personnel screening involves analyzing the background of company applicants to ensure that they are a creditable fit for the role in which they intend to work.

Personnel Termination – Termination of employment or separation of employment is an employee's departure from a job and the end of an employee's duration with an employer.

Personnel Sanctions – Consequences and the process for individuals failing to comply with established policies and procedures.

Risk Designation – The evaluation of each role within the County, Department and/or Business Unit and assigning a risk level to a position based on responsibility, level of data access and sensitivity of the data.

Roles and Responsibilities – Roles refer to one's position on a team. Responsibilities refer to the tasks and duties of their particular role or job description.

IV. Policy

1. Supporting Personnel Security Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the personnel security policy. [PS-1-T]

The Information Systems and Telecommunications (IS&T) Division and Human Resources Department 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 personnel security policy and the associated controls;

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

2. Position Risk Designation

The Human Resources Department shall:

a. Assign a risk designation to organizational positions as required or appropriate;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations annually. [PS-2-T]

3. Personnel Screening

The Human Resources Department shall:

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with County defined rescreening requirements and/or role specific rescreening requirements. [PS-3-T]

4. Personnel Termination

The Human Resources Department shall:

a. Conduct exit interviews that include a discussion of non-disclosure and confidentiality of County activities and operations;

b. Retrieve all security-related organizational system-related property; and

c. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and [PS-4-T]

d. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process. [PS-4(1)-O]

e. Use email communications as well as verbal communications to notify employee's manager and HR of individual termination actions; and to begin the process of disabling access to system resources. [PS-4(2)-T]

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

a. Upon termination of individual employment: Disable system access immediately for involuntary terminations while voluntary terminations will have system access disabled between 24 and 72 hours;

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Retain access to organizational information and systems formerly controlled by terminated individual. [PS-4-T]

5. Personal Transfer

Department Heads or Division Managers shall:

a. Initiate defined transfer or reassignment activities within five working days of notification of transfer/reassignment approval; and

b. Provide the Human Resources Department and the Information Systems & Telecommunication Division staff with transfer/reassignment details within five working days of receiving the approval for a transfer/reassignment. [PS-5-T]

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

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; and

b. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. *[PS-5-T]*

6. Access Agreements

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

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements annually or when roles change, transfer, or individual is reassigned; and

c. Verify that individuals requiring access to organizational information and systems:

I. Sign appropriate access agreements prior to being granted access; and

II. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or on an annual basis. *[PS-6-T]*

7. External Personnel Security

The Information Technology Department in conjunction with the Purchasing Division shall:

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify appropriate County assigned points of contact of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within 24-48 hours; and

e. Monitor provider compliance with personnel security requirements. [PS-7-T]

8. Personnel Descriptions

The Human Resources Department shall:

a. Incorporate security and privacy roles and responsibilities into organizational position descriptions. [PS-9-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

VII. References

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