I. Purpose

This policy establishes the Personally Identifiable Information Processing and Transparency Policy, for managing risks to the controls implemented within systems and within the organization. The Personally Identifiable Information Processing and Transparency policy helps Indian River County implement security best practices with regards to enterprise systems, data from any potential tampering and unauthorized changes from either internal or external threat actors.

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.

Personally Identifiable Information (PII) – Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Per Florida Statute 501.171 personal information means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
   - A social security number;

- A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
- A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Privacy Act – A law that protects the records of individuals such as name, social security number or other identifying details

IV. Policy

1. Supporting Personally Identifiable Information Processing and Transparency Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the Personally Identifiable Information Processing and Transparency policy. *[PT-1-T]*

The Information Systems and Telecommunications (IS&T) Division and County Attorney's Office 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 Personally Identifiable Information Processing and Transparency policy and the associated controls;

b. Review and update the current Personally Identifiable Information Processing and Transparency procedures annually as well as 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. *[PT-1-T]*

2. Authority to Process Personally Identifiable Information

The Senior Officer for Privacy and the County Attorney's Office shall:

a. Determine and document the legal authority that permits the County departments and/or divisions the ability to process personally identifiable information; and

b. Restrict the processing of personally identifiable information to only those business departments and/or divisions authorized to do so as required to perform the assigned job duties. [PT-2-T]

3. Personally Identifiable Information Processing Purposes

The Senior Officer for Privacy shall:

a. Identify and document the County defined and established purpose and justification for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the processing of personally identifiable information to only that which is compatible with the identified purpose(s); and

d. Provide County-defined mechanisms to enable individuals to have access to elements of data that is classified as sensitive, confidential and/or Personally Identifiable Information. [AC-3(14)-T]

The Information Systems and Telecommunications (IS&T) Division and County Attorney's Office shall:

a. Monitor changes in processing personally identifiable information and implement County approved change control capabilities and procedures to ensure that any changes are made in accordance with County approved and defined change management processes and procedures. [PT-3-T]

4. Consent

Any Department and/or Division that handles, processes, or stores personally identifiable information shall:

a. Implement a capability and process for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitates individuals' informed decision-making as well as use within the County's operations. [PT-4-T]

5. Security Alerts, Advisories, and Directives

Any Department and/or Division that handles, processes, or stores personally identifiable information shall:

a. Provide notice to individuals about the processing of personally identifiable information that is available to individuals upon first interacting with an organization, and subsequently annually;

b. Provide clear and easy-to-understand documentation or informational guides that provide details about personally identifiable information processing in plain language;

c. Identify the authority that authorizes the processing of personally identifiable information;

d. Identify the purposes for which personally identifiable information is to be processed; and

e. Include details of the use of personally identifiable information for County operations. [PT-5-T]

f. Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records or provide Privacy Act statements on separate forms that can be retained by individuals. [PT-5(2)-T]

6. Specific Categories of Personally Identifiable Information

Any Department and/or Division that handles, processes, or stores personally identifiable information shall:

a. Apply security controls and restrictive conditions for specific categories of personally identifiable information collected by the County. [PT-7-T]

b. When a system processes Social Security numbers:

i. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

ii. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

iii. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it. *[PT-7(1)-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