I. Purpose

This policy establishes the System and Services Acquisition Policy, for managing risks to the controls implemented within systems and within the organization. The System and Services Acquisition policy helps Indian River County implement security best practices with regards to capabilities, solutions, and systems procured from external partners and any impact that may result from these capabilities.

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

System Development Life Cycle - The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

Privacy Risk Management – The methodology for analyzing, assessing, and prioritizing privacy risks to determine how to respond and select appropriate solutions to accept, avoid, mitigate, and/or transfer the risk.

Pre-Production Environment - Pre-production environments are usually built before applications go into production. The two primary environments include:

Development environment: The development environment provides a layer on which software engineers can build and test their code. These tests are usually limited and focus mostly on unit-style tests.

Test environment: Test environments are usually where QA engineers will run a long list of test cases to make sure the code acts as expected.

Production Environment - A production environment, sometimes called deployment environment, is the set of computers where finished, user-ready software is deployed and executed.

IV. Policy

1. Supporting System and Services Acquisition Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the system and services acquisition policy. *[SA-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 system and services acquisition policy and the associated controls;

b. Review and update the current system and services acquisition procedures annually as well as 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. *[SA-1-T]*

2. Allocation of Resources

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

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation. [SA-2-T]

3. System Development Life Cycle

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

a. Acquire, develop, and manage the system using County approved and defined system development life cycle that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities. [SA-3-T]

e. Protect system pre-production environments commensurate with risk throughout the system development life cycle for the system, system component, or system service. [SA-3(2)-T]

f. Approve, document, and control the use of live data in pre-production environments for the system, system component, or system service; and

g. Protect pre-production environments for the system, system component, or system service at the same impact or classification level as any live data in use within the pre-production environments. [SA-3(2)-T]

h. Plan for and implement a technology refresh schedule for the system throughout the system development life cycle. [SA-3(3)-T]

4. Acquisition Process

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

a. Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language and/or County specific contract language in the

acquisition contract for the system, system component, or system service:

I. Security and privacy functional requirements;

II. Strength of mechanism requirements;

III. Security and privacy assurance requirements;

IV. Controls needed to satisfy the security and privacy requirements.

V. Security and privacy documentation requirements;

VI. Requirements for protecting security and privacy documentation;

VII. Description of the system development environment and environment in which the system is intended to operate;

VIII. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

IX. Acceptance criteria. [SA-4-T]

b. Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented. *[SA-4(1)-T]*

c. Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:

I. County approved systems engineering methods;

II. County approved systems security; privacy and engineering methods; and

III. County approved software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes. *[SA-4(3)-T]*

d. Require the developer of the system, system component, or system service to:

I. Deliver the system, component, or service with County approved and defined security configurations implemented; and

II. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade. *[SA-4(5)-T]*

e. Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use. *[SA-4(9)-T]*

f. Include organizational data ownership requirements in the acquisition contract; and

g. Require all data to be removed from the contractor's system and returned to the organization within 5 business days or the stipulated time as stated within the agreement between the County and the contracting organization. *[SA-4(12)-T]*

5. System Documentation

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

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

I. Secure configuration, installation, and operation of the system, component, or service;

II. Effective use and maintenance of security and privacy functions and mechanisms; and

III. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

I. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

II. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

III. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. When system, system component, or system service documentation is unavailable or nonexistent, take appropriate action to document and/or collect residual information; and

d. Distribute documentation to all appropriate staff, leadership and stakeholders. [SA-5-T]

6. Security and Privacy Engineering Principles

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

a. Apply County approved and defined industry best practices for systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components. *[SA-8-T]*

b. Implement the security design principle of least privilege in County identified systems and/or system components. *[SA-8(14)-T]*

c. Implement the privacy principle of minimization using County approved and defined minimization processes/procedures *[SA-8(33)-T]*

7. External System Services

All Departments and Divisions in conjunction with the Information Technology Department shall:

a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information systems or security services; and

b. Verify that the acquisition or outsourcing of dedicated information system or security services is approved by the Information Technology Department as well as the Purchasing Division. *[SA-9(1)-T]*

c. Require that providers of external system services comply with organizational security and privacy requirements and employ County approved and defined security and privacy controls;

d. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

e. Employ County approved processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis through County approved and defined processes, methods, and techniques. *[SA-9-T]*

f. Require providers of external system services to identify the functions, ports, protocols, and other services required for the use of external system services. *[SA-9(2)-T]*

g. Establish, document, and maintain trust relationships with external service providers based on properties, factors, and/or condition requirements as required by the County to ensure security and privacy requirements are being met. *[SA-9(3)-T]*

h. Take approved actions to verify that the interests of external service providers providing services to the County are consistent with and reflect County interests. *[SA-9(4)-T]*

i. Restrict the location of information processing; information and/or data; system services to County approved locations based on requirements to support availability. *[SA-9(5)-T]*

j. Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system. *[SA-9(6)-T]*

k. Provide the capability to check the integrity of information while it resides in the external system. *[SA-9(7)-T]*

l. Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States. *[SA-9(8)-T]*

8. Developer Configuration Management

All Departments and Divisions shall:

a. Require the developer of the system, system component, or system service to:

b. Perform configuration management during system, component, or service: design and/or development;

c. Document, manage, and control the integrity of changes to County hardware and software configuration items under configuration management functions;

d. Implement only organization-approved changes to the system, component, or service;

e. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

f. Track security flaws and flaw resolution within the system, component, or service and report findings to the Information Systems and Telecommunications division. [SA-10-T]

g. Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components. [SA-10(1)-T]

h. Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team. [SA-10(2)-T]

i. Require the developer of the system, system component, or system service to enable integrity verification of hardware components. [SA-10(3)-O]

j. Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies. [SA-10(6)-T]

k. Require the Information Technology Director to be included in the configuration change management and control process. [SA-10(7)-T]

9. Developer Testing and Evaluation

All Departments and Divisions shall:

a. Require the developer of a system, system component, or system service, at all post-design stages of the system development life cycle, to:

I. Develop and implement a plan for ongoing security and privacy control assessments;

II. Perform system testing/evaluation annually to ensure all source code and application/system functionality is working as intended;

III. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

IV. Implement a verifiable flaw remediation process; and

V. Correct flaws identified during testing and evaluation. [SA-11-T]

b. Require the developer of a system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis. [SA-11(1)-T]

c. Require the developer of a system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

I. Uses contextual County information concerning impact, environment of operations, known or assumed threats, and/or acceptable risk levels;

II. Employs County approved and defined tools and methods;

III. Conducts the modeling and analyses that ensures the integrity of privacy and security of developed applications/systems; and

IV. Produces evidence that meets the County application and/or system acceptance criteria. [SA-11(2)-O]

d. Require the developer of a system, system component, or system service to perform a manual code review of any code being utilized within the County's digital environment using the County approved and defined processes, procedures, and/or techniques. [SA-11(4)-O]

e. Require the developer of a system, system component, or system service to perform penetration testing:

I. To the County defined level of testing that ensures the privacy and security of said applications and/or systems; and

II. Under the constraints that an application, system, system component or system service is not in scope of penetration testing. [SA-11(5)-T]

f. Require the developer of a system, system component, or system service to perform attack surface reviews. [SA-11(6)-T]

g. Require the developer of a system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. [SA-11(8)-T]

h. Require the developer of a system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results. [SA-11(9)-T]

10. Development Process, Standards, and Tools

The Information Technology Department shall:

a. Require the developer of a system, system component, or system service to follow a documented development process that:

I. Explicitly addresses security and privacy requirements;

II. Identifies the standards and tools used in the development process;

III. Documents the specific tool options and tool configurations used in the development process; and

IV. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations at least annually to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy County accepted and defined security and privacy requirements. [SA-15-T]

11. Developer Screening

The Information Technology Department shall:

Require that the developer of any application and/or system utilized by the County:

a. Has appropriate access authorizations as determined by Information Technology Department; [SA-21-T]

12. Unsupported System Components

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide County approved options of alternative sources for continued support for unsupported components through either in-house support or support from external providers. [SA-22-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