I. Purpose

This policy establishes the Supply Chain Risk Management Policy, for managing risks to the controls implemented within systems and within the organization. The Supply Chain Risk Management policy helps Indian River County implement security best practices with regards to any risk to the supply chain that supports the County 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

Acquisition - Includes all stages of the process of acquiring product or service, beginning with the process for determining the need for the product or service and ending with contract completion and closeout.

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

Operations Security (OPSEC) - OPSEC is a security and risk management process and strategy that classifies information, oversees protection requirements for said information and preventing either accidental or intentional disclosure of the information to those without a need-to-know.

Supply Chain Risk Management (SCRM) - The implementation of processes, tools or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other

vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

IV. Policy

1. Supporting Supply Chain Risk Management Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the Supply Chain Risk Management policy. [SR-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 Supply Chain Risk Management policy and the associated controls;

b. Review and update the current supply chain risk management 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. *[SR-1-T]*

2. Supply Chain Risk Management Plan

The Information Systems and Telecommunications (IS&T) Division in conjunction with the Purchasing Division shall:

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of all County owned systems, system components or system services;

b. Review and update the supply chain risk management plan annually or as required, to address threat, organizational, or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification. [SR-2-T]

d. Establish a supply chain risk management team to lead and support Supply Chain Risk Management activities: [SR-2(1)-T]

3. Supply Chain Controls and Processes

The Information Systems and Telecommunications (IS&T) Division in conjunction with Purchasing Division shall:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the County's supply chain elements and processes;

b. Employ protective controls, as defined by the County, to protect against supply chain risks to the systems, system components, and/or system services and to limit the harm or consequences from supply chain-related events; and

c. Document the selected and implemented supply chain processes and controls within the supply chain risk management plan. [SR-3-T]

d. Employ a diverse set of sources for the critically identified system components and services. [SR-3(1)-T]

e. Employ protective controls, as defined by the County, to limit harm from potential adversaries identifying and targeting the organizational supply chain. [SR-3(2)-T]

4. Acquisition Strategies, Tools, and Methods

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

a. Employ County approved and defined acquisition strategies, contract tools, and procurement methods defined by IS&T and the Purchasing Division to protect against, identify, and mitigate supply chain risks. [SR-5-T]

b. Employ continuous availability controls, as defined by the County, to ensure an adequate supply of County defined critical systems, system components, and/or system services. [SR-5(1)-T]

5. Supplier Assessments and Reviews

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

a. Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide annually. *[SR-6-T]*

6. Notification Agreements

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

a. Establish agreements and procedures with all entities involved in the supply chain for the systems, system components, and/or system services being delivered to the County for the notification of supply chain compromises and/or results of assessments or audits. *[SR-8-T]*

7. Inspection of Systems or Components

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

a. Inspect critical systems and/or system components at random and all County systems and/or system components at least annually or upon County defined indications for inspection in order to detect tampering or any indications of compromise. *[SR-10-T]*

8. Component Disposal

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

a. Dispose of County owned and defined data, documentation, tools, systems and/or system components using County approved techniques and methods and/or suppliers. *[SR-12-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