I. Purpose

This policy establishes the Risk Assessment Policy, the overall methodology for how Indian River County will manage risks to the controls implemented within systems and within the organization. The Risk Assessment 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

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Impact - The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Likelihood - A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Threshold - Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.

Risk Acceptance - the level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific IT system.

Risk Transference - the level of Residual Risk of potential loss/disruption for a specific IT system that that has been shifted from one party to another.

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Avoidance - Risk avoidance is a risk management strategy that seeks to eliminate the possibility of risk by avoiding engaging in activities that create exposure to risk.
Policy

1. Supporting Risk Assessment Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the risk assessment policy. *[RA-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 risk assessment policy and the associated controls;

b. Review and update the current risk assessment 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. *[RA-1-T]*

2. Security Categorization

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

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision. [RA-2-T]

d. Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels. [RA-2(1)-O]

3. Risk Assessment

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

a. Conduct a risk assessment, including:

I. Identifying threats to and vulnerabilities in the system;

II. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

III. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in a risk assessment report;

d. Review risk assessment results annually;

e. Disseminate risk assessment results with the Information Technology Department and County leadership; and

f. Update the risk assessment methodology every three to five years or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system. [RA-3-T]

g. Assess supply chain risks associated with County approved systems, system components, and system services; and

h. Update the supply chain risk assessment every three to five years, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply

chain. [RA-3(1)-T]

i. Determine the current cyber threat environment on an ongoing basis through active threat identification. [RA-3(3)-T]

j. Employ advanced automation and analytics capabilities to predict and identify risks to County owned systems and/or system components. [RA-3(4)-O]

4. Vulnerability Monitoring and Scanning

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

a. Monitor and scan for vulnerabilities in the system and hosted applications regularly as a part of standard operations or randomly and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

   I. Enumerating platforms, software flaws, and improper configurations;

   II. Formatting checklists and test procedures; and

   III. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities within defined Service Level Agreements (SLA) in accordance with the County defined assessment of risk and its equivalent remediation timeline;

e. Share information obtained from the vulnerability monitoring process and control assessments with appropriate County, and State representatives to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned across the County's technology footprint. [RA-5-T]

g. Update the system vulnerabilities to be scanned prior to a new scan dependent on the criticality of the vulnerability and/or when new vulnerabilities are identified and reported. [RA-5(2)-*T]*

h. Define the breadth and depth of vulnerability scanning coverage. [RA-5(3)-T]

i. Determine information about the system that is discoverable and take corrective action to reduce the impact of the vulnerability. [RA-5(4)-T]

j. Implement privileged access authorization to critical County systems for vulnerability scanning activities that may cause a disruption and/or an outage to services for the County. [RA-5(5)-T]

k. Use automated mechanisms to analyze multiple vulnerability scans over time to determine trends in system vulnerabilities and identify patterns of attack. [RA-5(6)-O]

l. Review historic audit logs to determine if a vulnerability identified in a County information system has been previously exploited within the past three years. [RA-5(8)-O]

m. Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors. [RA-5(10)-O]

5. Risk Response

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

a. Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance. [RA-7-T]

6. Privacy Impact Assessments

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

a. Conduct privacy impact assessments for systems, programs, or other activities before developing or procuring information technology that processes personally identifiable

information; or

b. Initiating a new collection of personally identifiable information when a new service offering that the County is delivering:

I. Will be processed using information technology; and

II. Includes personally identifiable information.

7. Criticality Analysis

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

a. Identify critical system components and functions by performing a criticality analysis for all County owned systems, system components, and/or system services at the initiation step in the system development life cycle. [RA-9-T]

8. Threat Hunting

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

a. Establish and maintain a cyber threat hunting capability to:

I. Search for indicators of compromise in organizational systems; and

II. Detect, track, and disrupt threats that evade existing controls; and

b. Employ the threat hunting capabilities across the County system components that operate monthly. [RA-10-O]

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)
c. FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems

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