I. Purpose

This policy establishes the System and Information Integrity Policy, for managing risks to the controls implemented within systems and within the organization. The System and Information Integrity Policy helps Indian River County implement security best practices with regards to enterprise systems, protecting 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.

Firmware – Permanent software that is installed on a device's read only memory.

Flaw – An imperfection or weakness that could expose the exploitation of a vulnerability either accidentally or intentionally.

Kernel Application Programming Interface –The kernel application programming interface allows application programs to access system resources and services.

Malicious Code – Malicious code is applications, unwanted files and/or programs that can cause harm to a computer and/or compromise any data stored on that device.

Operating System – Software that supports a computer's basic functionality and supports the execution of other applications, programs and connected peripherals.

Quarantine Code – Any application, unwanted files and/or programs that are deemed suspicious and isolated from being installed and or spreading across the digital network.

Remediation – The act of mitigating a vulnerability or threat that has been identified with the appropriate controls to an acceptable level of risk.

Software – Applications and/or programs that run on a computing asset to execute specific tasks.

System and Information Integrity – Ensuring that information technology resources and information systems have the appropriate capabilities to prevent the infiltration of malware, source code flaws and other vulnerabilities do not alter/change the configuration, and or any data that resides on said system(s).

IV. Policy

1. Supporting System and Information Integrity Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the system and information integrity policy. *[SI-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 information integrity policy and the associated controls.

b. Review and update the current system and information integrity procedures on a regularly established schedule or at least 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. *[SI-1-T]*

2. Flaw Remediation

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

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within 30 days of the release of the updates;

d. Incorporate flaw remediation into the County's Change and Configuration Management process. [SI-2-T]

e. Determine if system components have applicable security-relevant software and firmware updates installed using County approved update capabilities on a monthly basis. *[SI-2(2)-T]*

f. Measure the time between flaw identification and flaw remediation; and

g. Establish benchmarks for taking corrective actions focused on the time to remediate identified flaws. *[SI-2(3)-T]*

e. Employ automated patch management tools to facilitate flaw remediation to system components on all County information technology assets. *[SI-2(4)-T]*

f. Install security-relevant software and firmware updates identified and received for all applicable systems automatically on all County information technology assets. *[SI-2(5)-T]*

g. Remove previous versions of identified software and firmware updates automatically on all County information technology assets after updated versions have been installed. *[SI-2(6)-T]*

3. Malicious Code Protection

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

a. Implement signature based as well as non-signature based malicious code protection.

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.

c. Configure malicious code protection mechanisms to:

I. Perform periodic scans of the system at least weekly and real-time scans of files from external sources at County information technology endpoints, network entry and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and

II. Block malicious code and/or quarantine malicious code dependent on the severity; take appropriate remediation actions; and send alert to the security operations center in response to malicious code detection; and

III. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system. [SI-3-T]

e. Update malicious code protection mechanisms only when directed by a privileged user. *[SI-3(4)-T]*

f. Test malicious code protection mechanisms semiannually by introducing known benign code into a standalone network not connected to the County's operational network; and

g. Verify that the detection of the benign code and the associated incident reporting occurs. *[SI-3(6)-T]*

h. Detect unauthorized operating system commands through the kernel application programming interface on County information technology assets as well as unauthorized operating system commands on said assets as identified by the County's Information System and Telecommunications (IS&T) division; and

j. Either issue a warning; audit the command execution; or prevent the execution of the commands identified by the County's Information System and Telecommunications (IS&T) Division. *[SI-3(8)-T]*

k. I. Employ County approved and defined tools and techniques to analyze the characteristics and behavior of malicious code through County systems, system components and connected interfaces; and

II. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes. *[SI-3(10)-O]*

4. System Monitoring

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

a. Monitor the system to detect:

   I. Attacks and indicators of potential attacks in accordance with County established information technology asset monitoring objectives; and

   II. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through County approved techniques and methods;

c. Invoke internal monitoring capabilities or deploy monitoring devices:

   I. Strategically within the system to collect County determined essential information; and

   II. At ad hoc locations within the system to track specific types of transactions of interest to the County;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities on County owned systems; and

g. Provide County approved system monitoring information to IT staff members with delegated responsibility of system monitoring on a continuous basis or as needed for investigations. [SI-4-T]

h. Connect and configure individual intrusion detection tools into a system-wide intrusion detection system. [SI-4(1)-O]

i. Employ automated tools and mechanisms to support near real-time analysis of events. [SI-4(2)-O]

j. Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms. [SI-4(3)-O]

k. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

l. Monitor inbound and outbound communications traffic on a continuous basis for County defined unusual or unauthorized activities or conditions that go against policy and/or normal operating conditions. [SI-4(4)-T]

m. Alert County IT Staff members when the system-generated indications of compromise or potential compromise through alerting and/or user notifications occur as defined by the County as well as per policy. [SI-4(5)

I. Notify IT Director of detected suspicious events; and

II. Take the least disruptive actions upon detection to terminate suspicious events affecting the County: *[SI-4(7)-T]*

n. Test intrusion-monitoring tools and mechanisms at least annually. [SI-4(9)-O]

o. Make provisions so that County approved encrypted communications mechanisms are visible to County approved system monitoring tools and mechanisms. [SI-4(10)-O]

p. Analyze outbound communications traffic at the external interfaces and selected interior points within the County's digital footprint to discover anomalies. [SI-4(11)-T]

q. Alert IT Staff members using County approved automated monitoring mechanisms when indications of inappropriate or unusual activities with security or privacy implications/impacts occur. [SI-4(12)-T]

r. Analyze communications traffic and event patterns for the system;

s. Develop profiles representing common traffic and event patterns; and

t. Use the traffic and event profiles in tuning system-monitoring devices. [SI-4(13)-T]

u. Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system. [SI-4(14)-O]

v. Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wired networks. [SI-4(15)-O]

w. Correlate information from monitoring tools and mechanisms employed throughout the system. [SI-4(16)-O]

x. Correlate and share information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness. [SI-4(17)-O]

y. Analyze outbound communications traffic at external interfaces to the system and at identified interior points to detect covert exfiltration of information. [SI-4(18)-O]

z. Implement monitoring of privileged users with access to sensitive data and/or systems within the County's digital footprint. [SI-4(20)-T]

aa. Implement additional monitoring upon request of individuals during County established probationary periods of new hires or disciplinary actions. [SI-4(21)-O]

bb. Detect network services that have not been authorized or approved by the Director of IT;

cc. Audit or review County roles when abnormal activities, requests and network traffic are detected or occur. [SI-4(22)-T]

dd. Implement County approved host-based monitoring mechanisms on County Information Technology assets: [SI-4(23)-T]

ee. Discover, collect, and distribute to County IT staff, County employees and contractors, along with anyone who may access County IT assets, indicators of compromise. [SI-4(24)-T]

ff. Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices. [SI-4(25)-T]

5. Security Alerts, Advisories, and Directives

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

a. Receive system security alerts, advisories, and directives from external organizations approved by the County (US-CERT, FBI IC3, MS-ISAC and CISA etc.) on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to appropriate IT Staff members; for applicability and/or implementation if necessary to enhance the County's IT security posture; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance. *[SI-5-T]*

e. Broadcast security alert and advisory information throughout the organization using County approved communication mechanisms. *[SI-5(1)-T]*

6. Software, Firmware, and Information Integrity

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

a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information within the County's computing environment; and

b. Take actions to prevent unauthorized changes to software, firmware, and information within the County's digital footprint when they are detected. *[SI-7-T]*

c. Perform an integrity check of County purchased software, asset firmware, and information upon procurement; *[SI-7(1)-T]*

d. Employ automated tools that provide notification to IS&T staff members upon discovering discrepancies during integrity verification. *[SI-7(2)-T]*

e. Employ centrally managed integrity verification tools. *[SI-7(3)-T]*

f. Implement cryptographic mechanisms to authenticate County software or asset firmware components purchased through the approved procurement process prior to installation. *[SI-7(15)-O]*

7. Spam Protection

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

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. *[SI-8-T]*

c. Automatically update spam protection mechanisms on a weekly basis or when updates are provided by the County approved spam protection capability. *[SI-8(2)-T]*

d. Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic. *[SI-8(3)-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