I. Purpose

This policy establishes the System and Communications Protection Policy for managing risks to the controls implemented within systems and within the organization. The System and Communications Protection 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

Child Zone- A separate, functioning zone which is the subdomain of another zone. Please refer to RFC-1034: Domain Names for additional information.

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

National Institute of Standards and Technology (NIST) – a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce.

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.

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 Communications Protection Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the system and communications protection policy. *[SC-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 communication protection procedures 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. *[SC-1-T]*

2. Separation of System and User Functionality

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

a. Separate user functionality, including user interface services from system management functionality. *[SC-2-T]*

3. Denial-of-Service Protection

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

a. Protect against the effects of denial-of-service events that affect the County directly, as well as constituent facing systems.

b. Employ County approved and defined controls to achieve the denial-of-service objective.

c. Restrict the ability of individuals to launch denial-of-service attacks against other systems through IP blacklisting, DoS Protection and other technological and administrative capabilities. *[SC-5(1)-T]*

c. Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks. *[SC-5(2)-O]*

d. Employ monitoring tools to detect indicators of denial-of-service attacks against or launched from the system; and

e. Monitor denial-of-service mitigation system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks. *[SC-5(3)-T]*

4. Resource Availability

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

a. Protect the availability of resources by allocating critical systems with a priority as well as a resource quota. *[SC-6-T]*

5. Boundary Protection

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

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; and

b. Implement subnetworks for publicly accessible system components that are either physically and/or logically separated from internal County networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture; and *[SC-7-T]*

d. Implement a managed interface for each external telecommunication service; and

e. Establish a traffic flow policy for each managed interface; and

f. Protect the confidentiality and integrity of the information being transmitted across each interface; and

g. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need; and

h. Review exceptions to the traffic flow policy as they are submitted through a centralized review committee and remove exceptions that are no longer supported by an explicit mission or business need; and

i. Prevent unauthorized exchange of control plane traffic with external networks; and

j. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

k. Filter unauthorized control plane traffic from external networks and *[SC-7(4)-T]*

l. Deny network communications traffic by default and allow network communications traffic by exception through the approved and managed interfaces for County systems that fall within the scope; and *[SC-7(5)-T]*

m. Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using County approved safeguards and secure mechanisms; and *[SC-7(7)-T]*

n. Route internal communications traffic to County approved external networks through authenticated proxy servers at approved managed interfaces; and *[SC-7(8)-T]*

o. Detect and deny outgoing communications traffic posing a threat to external systems; and

p. Audit the identity of internal users associated with denied communications; and *[SC-7(9)-T]*

q. Prevent the exfiltration of information; and

r. Conduct exfiltration tests annually; and *[SC-7(10)-O]*

s. Only allow incoming communications from County authorized sources and systems to be routed to pre-approved and authorized destinations; and *[SC-7(11)-T]*

t. Implement host-based boundary protection capabilities on all end points that allow and manage external network traffic into the County's digital footprint; and *[SC-7(12)-T]*

u. Isolate County approved information security tools, mechanisms, and support components from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system through either logical and/or physical separation; and *[SC-7(13)-T]*

v. Protect against unauthorized physical connections at all County owned technological assets unless authorized/approved; and *[SC-7(14)-T]*

w. Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing; and *[SC-7(15)-O]*

x. Prevent the discovery of specific system components that represent a managed interface; and *[SC-7(16)-O]*

y. Enforce adherence to protocol formats; and *[SC-7(17)-T]*

z. Employ boundary protection mechanisms to isolate specific County owned IT assets and/or systems supporting dedicated and specific business functions or critical County activities; and *[SC-7(21)-T]*

aa. Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device; and *[SC-7(18)-T]*

ab. Block inbound and outbound communications traffic between specific County owned IT assets and/or systems that are independently configured by end users and external service providers; and *[SC-7(19)-T]*

ac. Provide the capability to dynamically isolate specific County owned IT assets and/or systems from other system components; and *[SC-7(20)-T]*

ad. Implement separate network addresses to connect to systems in different security domains; and *[SC-7(22)-T]*

ae. Disable feedback to senders on protocol format validation failure; and *[SC-7(23)-T]*

af. For systems that process personally identifiable information:

I. Apply processing rules to data elements of personally identifiable information on all systems that process personally identifiable information (PII);
II. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;

III. Document each processing exception; and
IV. Review and remove exceptions that are no longer supported. *[SC-7(24)-T]*

ag. Prohibit the direct connection of defined County systems to any public network; and *[SC-7(28)-T]*

ah. Implement a combination of physically and logically separate subnetworks to isolate critical system components and functions defined by the County. *[SC-7(29)-T]*

6. Transmission Confidentiality and Integrity

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

a. Protect the confidentiality and/or integrity of transmitted information on the County's network as well as when it leaves the County's network. *[SC-8-T]*

b. Implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission. *[SC-8(1)-T]*

c. Implement cryptographic mechanisms to protect message externals unless otherwise protected by County approved and defined compensating controls. *[SC-8(3)-T]*

7. Network Disconnect

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

a. Terminate the network connection associated with a communications session at the end of the session or after 15 minutes of inactivity. *[SC-10-T]*
b.

8. Cryptographic Protection

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

a. Determine the cryptographic use cases for the County; and

b. Implement County approved types of cryptography for each specific cryptographic use case. [SC-13-T]

9. Cryptographic Key Establishment and Management

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

a. Establish and manage cryptographic keys (key generation, distribution, storage, access, and destruction) when cryptography is employed within the system in accordance with County key management requirements. *[SC-12-T]*

b. Maintain availability of information in the event of the loss of cryptographic keys by users. *[SC-12(1)-T]*

c. Produce, control, and distribute symmetric cryptographic keys using NIST FIPS-validated and/or NSA-approved key management technology and processes. *[SC-12(2)-O]*

d. Produce, control, and distribute asymmetric cryptographic keys using either NSA-approved key management technology and processes and/or DoD-approved or DoD-issued Medium Assurance PKI certificates, DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key, and certificates issued in accordance with County approved and defined requirements. *[SC-12(3)-O]*

e. Maintain physical control of cryptographic keys when stored information is encrypted by external service providers. *[SC-12(6)-O]*

10. Collaborative Computing Devices and Applications

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

a. Prohibit remote activation of collaborative computing devices and applications except when remote activation is to be allowed and these exceptions are documented and approved by appropriate County leadership; and

b. Provide an explicit indication of use to users physically present at the devices; and [SC-15-T]

c. Provide either a physical or logical capability to disconnect collaborative computing devices in a manner that supports ease of use; and [SC-15(1)-T]

d. Disable or remove collaborative computing devices and applications from County networks and connected network assets in defined secure/sensitive work areas; and [SC-15(3)-O]

e. Provide an explicit indication of current participants in sensitive County online meetings and/or teleconferences for restricted County leadership. [SC-15(4)-T]

11. Transmission of Security and Privacy Attributes

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

a. Associate all County security and privacy capabilities and their attributes with information exchanged between systems and between system components. [SC-16-O]

12. Public Key Infrastructure Certificates

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

a. Issue public key certificates under a County defined and established certificate policy or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization. [SC-17-T]

13. Mobile Code

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

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system; and [SC-18-T]

c. Identify any unacceptable mobile code and take the actions of preventing code execution and begin isolating and removing code from the County's digital footprint; and [SC-18(1)-T]

d. Prevent the download and execution of County defined unacceptable mobile code; and [SC-18(3)-T]

e. Prevent the automatic execution of mobile code in all County software applications and enforce dynamic mobile code scanning prior to executing the code. [SC-18(4)-T]

14. Secure Name/address Resolution Service (authoritative Source)

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

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child zone supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. [SC-20-T]

15. Secure Name/address Resolution Service (recursive or Caching Resolver)

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

a. Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. [SC-21-T]

16. Architecture and Provisioning for Name/address Resolution Service

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

a. Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation. [SC-22-T]

17. Session Authenticity

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

a. Protect the authenticity of communications sessions. [SC-23-T]

b. Only allow the use of County approved certificate authorities for verification of the establishment of protected sessions. [SC-23-T]

18. Decoys

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

a. Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks. [SC-26-O]

19. Protection of Information at Rest

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

a. Protect the confidentiality and integrity of all County information at rest. [SC-28-T]

b. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest on County defined system components and/or media. [SC-28(1)-T]

c. Remove information from online storage and store offline in a secure location as approved and defined by the County. [SC-28(2)-T]

d. Provide a combination of protected storage for cryptographic keys through County defined logical safeguards and hardware-protected key store. [SC-28(3)-T]

20. System Partitioning

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

a. Partition the system into approved segments residing in either separate physical and/or logical domains or environments based on County defined requirements of segmentation. [SC-32-O]

21. Distributed Processing and Storage

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

b. Distribute processing and storage components across either physical locations and/or logical domains for identified processing and storage components. [SC-36-O]

22. Out-of-band Channels

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

a. Employ out-of-band channels for the physical delivery or electronic transmission of County defined information, system components, and/or devices to approved individuals and/or systems via County approved and defined out-of-band channels. [SC-37-O]

23. Operations Security

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

a. Employ operations security controls to protect key organizational information throughout the system development life cycle. [SC-38-T]

24. Process Isolation

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

a. Maintain a separate execution domain for each executing system process. [SC-39-O]

25. Wireless Link Protection

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

a. Protect external and internal wireless links from signal parameter attacks. [SC-40-T]

b. Implement cryptographic mechanisms to reduce the detection potential of wireless links to an acceptable level defined by the County. [SC-40(2)-O]

26. Port and I/O Device Access

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

a. Physically and/or logically disable or remove connection ports or input/output devices on the systems or system components identified by the County and/or the IS&T division. [SC-41-T]

27. System Time Synchronization

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

a. Include synchronized system clocks within and between systems and system components. [SC-45-T]

b. Compare the internal system clocks annually with the NIST atomic clock; and

c. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 2 minutes. [SC-45(1)-T]

d. Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and

e. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable. [SC-45(2)-T]

28. Alternate Communications Paths

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

a. Establish a County approved and defined communication paths for system operations organizational command and control. [SC-47-O]

29. Software-enforced Separation and Policy Enforcement

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

a. Implement software-enforced separation and policy enforcement mechanisms between established security domains. [SC-50-O]

VI. 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.

VII. Procedures, Guidelines, Forms and Other Related Resources

VIII. 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)

IX. Responsibility

Information Technology Department

X. Authority Approval and Signature

Approved:

_____

Michael Zito

Interim County Administrator

XI. History

VERSION	DATE	CHANGES	DEPT/INDIVIDUAL
1.0	01.01.23	Initial Publication	IT/D. Russell