I. Purpose

Configuration management consists of activities focused on establishing and maintaining the integrity of information technology products and systems used within County operations through the control of a set of processes to manage and monitor system and product configurations throughout its lifecycle. Configuration management consists of determining and documenting the appropriate specific settings for a system, conducting security impact analyses, and managing changes through a change team

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.

Change Advisory Board (CAB) – Group of stakeholders responsible for the advisement, assessment, and prioritization of changes.

Change Owner – Individual identifying the need and submission of a change

Changer Manager – individual who is responsible for planning, developing, delivering, and tracking change management deliverables

Change Implementer – Individual responsible to implement the required changes as outlined in the change requests.

Change Approver – Individual responsible to approve the need and accept the risk of implementation

Change Sponsor – Individual or group who has the power to authorize or legitimize change.

Firmware - Permanent software programmed into a read-only memory.

IV. Policy

1. Supporting Identification and Authentication Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the configuration management policy. *[CM-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 configuration management policy and the associated configuration management controls;

b. Review and update the current configuration management 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. *[CM-1-T]*

2. Baseline Configuration

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

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:
   i. On a annual or as needed basis;
   ii. When required due to changes in security and/or privacy control requirements or from changes with system or architecture requirements; and
   iii. When system components are installed or upgraded. *[CM-2-T]*

c. Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using the following tools and capabilities supported by County operations and within the IS&T division:
   - Configuration management
   - Network management
   - Hardware, software, and firmware tools *[CM-2(2)-T]*

d. Retain a sufficient number of previous versions of baseline configurations, as defined by system or application custodian, to support a successful rollback. *[CM-2(3)-T]*

e. Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration. *[CM-2(6)-O]*

3. Configuration Change Control

The Change Owner, Change Manager, Change Implementer or Change Advisory Board (CAB) shall:

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with a system or environment;

d. Implement approved configuration-controlled changes to a system or environment;

e. Retain records of configuration-controlled changes to the system based on the County's record retention policy and/or based on historical data and reporting;

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through the County's Change Advisory Group (CAG); when system or general environment changes have the potential to impact system or service availability throughout the County's operating environment. *[CM-3-T]*

h. Use County's change management capabilities to:

I. Document proposed changes to the system;
II. Notify Change Approver or Change Sponsor of proposed changes to the system and request change approval;
III. Highlight proposed changes to the system that have not been approved or disapproved within 10 business days;
IV. Prohibit changes to the system until designated approvals are received;
V. Document all changes to the system; and

VI. Notify Change Owner or Change Sponsor when approved changes to the system are completed. *[CM-3(1)-T]*

i. Test, validate, and document changes to the system before finalizing the implementation of the changes. *[CM-3(2)-T]*

j. Implement changes to the current system baseline and deploy the updated baseline across the installed base using configuration management, network management, or hardware, software, and firmware tools. *[CM-3(3)-T]*

k. Require the Director of Information Technology, the Risk Officer and/or the designated representatives to be members of the County's Change Advisory Group (CAG). *[CM-3(4)-T]*

l. Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner:

- Issue appropriate alerting and notification to key personnel upon detection of an unauthorized change and/or
- Take appropriate action to ensure unauthorized configurations do not impact service integrity or availability. *[CM-3(5)-T]*

m. Ensure that cryptographic mechanisms used to provide the following controls are under configuration management:
    - System certificates. *[CM-3(6)-T]*

n. Review changes continuously and periodically or when suspicious behavior and/or problems are identified to determine whether unauthorized changes have occurred. *[CM-3(7)-T]*

o. Prevent or restrict changes to the configuration of the system under the following circumstances:

- When any proposed change(s) does not follow the guidelines and procedures defined by the Change Manager and/or Change Advisory Group (CAG)
- When any proposed change(s) violate the County's governance policies, and
- When explicitly denied by the Change Advisory Group (CAG) based on the risk to stability and availability of the County's operating environment. *[CM-3(8)-T]*

4. Impact Analyses

The Change Owner, Change Manager, Change Implementer or Change Advisory Group (CAG) shall:

a. Analyze changes to the system to determine potential security and privacy impacts prior to change implementation. *[CM-4-T]*

b. Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice. *[CM-4(1)-T]*

c. After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system. *[CM-4(2)-T]*

5. Access Restrictions for Change

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

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system. *[CM-5-T]*

b. Enforce access restrictions using system authentication and authorization capabilities for every change implementer; and automatically generate audit records of the enforcement actions. *[CM-5(1)-T]*

c. Limit privileges to change system components and system-related information within a production or operational environment; and review and reevaluate privileges on an annual basis. *[CM-5(5)-T]*

6. Configuration Settings

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

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using the Security Technical Implementation Guides (STIGs) and the County's Information Security Policy (ISP) *[CM-6-T]*;

b. Implement the configuration settings *[CM-6-T]*;

c. Identify, document, and approve any deviations from established configuration settings of any County-owned or sanctioned hardware, software, or firmware components based on the operational requirements defined by the IS&T division *[CM-6-T]*; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures. *[CM-6-T]*

e. Manage, apply, and verify configuration settings for any County-owned or sanctioned hardware, software, or firmware components using the tools and capabilities operated and maintained by the IS&T division. *[CM-6(1)-T]*

f. Take the following actions in response to unauthorized changes to any County-owned or sanctioned hardware, software, or firmware components:

- Alert and notify key personnel of the violation
- Restore County established and approved configurations and/or
- Shutdown identified system or components to ensure operational integrity and availability to the County's computing environment. *[CM-6(2)-O]*

7. Least Functionality

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

a. Configure the system to provide only the minimum necessary resources and operational usage in order facilitate the service functionality and consumption of use for County operations; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:
   i. Administrative rights on endpoint devices
   ii. URL filtering outbound of the County's perimeter infrastructure to inspect and block objectionable, offensive, or illegal content
   iii. Personally owned software and hardware components
   iv. Certain peripheral devices *[CM-7-T]*

c. Review the system periodically to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

d. Disable or remove any functionality, software, or service that is deemed unnecessary and/or creates a vulnerability on a system or across the County's operating environment. *[CM-7(1)-T]*

e. Prevent program execution in accordance with the County's Acceptable Use Policy or which violates and exposes the County to license and copyright laws for a specific software or application *[CM-7(2)-T]*

f. Ensure compliance with the County's software or hardware request and authorization process; *[CM-7(3)-T]*

g. Identify all the software and applications that are approved and authorized for use within County operations *[CM-7(5)-T]*;

h. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system *[CM-7(5)-O];* and

i. Review and update the list of authorized software programs on an annual basis or when software or applications have been approved and authorized for use. *[CM-7(5)-T]*

j. Require that user-installed software execute in a confined physical or virtual machine environment with limited privileges; *[CM-7(6)-T]*

k. Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code. *[CM-7(8)-T];* and

l. Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official; *[CM-7(8)-T]*

m. Identify all the hardware and components that are approved and authorized for use within County operations;

n. Prohibit the use or connection of unauthorized hardware components;

o. Review and update the list of authorized hardware components an annual basis or when hardware or components have been approved and authorized for use. *[CM-7(9)-T]*

8. System Component Inventory

The Information Systems and Telecommunications (IS&T) division shall ensure that the information system(s):

a. Develop and document an inventory of system components that:
   I. Accurately reflects the system;
   II. Includes all components within the system;

III. Does not include duplicate accounting of components or components assigned to any other system;
IV. Is at the level of granularity deemed necessary for tracking and reporting; and
V. Includes the following information, at a minimum, to achieve system component accountability:
   - system name
   - system operating system/build version
   - software owners
   - software version numbers
   - hardware inventory specifications
   - software license information
   - machine names and network addresses (for network connected devices and components); and

b. Review and update the system component inventory continuously based on the platform capabilities. *[CM-8-T]*

c. Update the inventory of system components as part of component installations, removals, and system updates. *[CM-8(1)-T]*

d. Maintain the currency, completeness, accuracy, and availability of the inventory of system components using the configuration and inventory management system operated and maintained by IS&T operations. *[CM-8(2)-T]*

e. Detect the presence of unauthorized hardware, software, and firmware components within the system using configuration and inventory management system operated and maintained by IS&T operations on a continuous basis *[CM-8(3)-O]*; and

f. Take the following actions when unauthorized components are detected:
   - Disable the functionality for access to the County's network infrastructure
   - Further isolate the components as deemed necessary to minimize risk to County operations; and
   - Notify key personnel responsible to facilitate notification, awareness, or communication for proper action. *[CM-8(3)-T]*

g. Include in the system component inventory information, a means for identifying by role, individuals responsible and accountable for administering those components. *[CM-8(4)-T]*

h. Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory. *[CM-8(6)-T]*

i. Provide a centralized repository for the inventory of system components. *[CM-8(7)-T]*

j. Assign system components to a system; and

k. Receive an acknowledgement from the subject matter expert (SME) of this assignment. *[CM-8(9)-O]*

9. Configuration Management Plan

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

a. Develop, document, and implement a configuration management plan for the system that:
   i. Addresses roles, responsibilities, and configuration management processes and procedures;
   ii. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the items requiring changes;
   iii. Defines the configuration items for the system and places the configuration items under change management;
   iv. Is reviewed and approved by Director of Information Technology; and
   v. Protects the configuration management plan from unauthorized disclosure and modification. *[CM-9-T]*

b. Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development. *[CM-9(1)-T]*

10. Software Usage Restrictions

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

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. *[CM-10-T]*

d. Establish the following restrictions on the use of open-source software:
   - Reviewed and authorized for use by the IS&T division
   - Packages are provided by authorized sources
   - Packages are validated for integrity and authenticity. *[CM-10(1)-T]*

11. User-installed Software

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

a. Establish and deploy endpoint policies governing the installation of software by users;

b. Enforce software installation policies through approved methods;

c. Monitor policy compliance continuously. *[CM-11-T]*

d. Allow user installation of software only with explicit privileged status. *[CM-11(2)-T]*

e. Enforce and monitor compliance with software installation policies using the tools and capabilities operated and managed by IS&T operations. *[CM-11(3)-T]*

12. Information Location

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

a. Identify and document the location of information as outlined in the County's Data Classification Policy and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored. *[CM-12-T]*

d. Use automated tools to ensure controls are in place to protect the County's information and individual privacy. *[CM-12(1)-T]*

13. Signed Components

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

a. Prevent the installation of any software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. *[CM-14-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

NIST Security and Privacy Controls for Information Systems and Organizations (800.53 Rev.5)

Guide to Industrial Control Systems (ISC) Security (800.82 Rev.2)

VII. Responsibility

Information Technology Department

VIII. Authority Approval and Signature

Approved:

_____

Michael Zito

Interim County Administrator

VIII. History

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