I. Purpose

This policy is the Maintenance Policy for managing risks from information asset maintenance and repairs through the establishment of an effective System Maintenance program. The system maintenance program helps Indian River County implement security best practices with regards to enterprise system maintenance and repairs.

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

Business Continuity Planning (BCP) – The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Disaster Recovery Plan (DR) - A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Controlled Maintenance - Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers.

Field Maintenance - Field maintenance is the type of maintenance conducted on a system or system component after the system or component has been deployed to a specific site. In

certain instances, field maintenance (i.e., local maintenance at the site) may not be executed with the same degree of rigor or with the same quality control checks as depot maintenance.

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

Maintenance (MA) – Any act that either prevents the failure or malfunction of equipment or restores its operating capability.

Maintenance Personnel - Maintenance personnel are individuals who perform hardware or software maintenance on organizational systems. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website.

Maintenance Tools – potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website.

Non-local Maintenance – Non-local maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements.

Recovery Time Objective (RTO) - The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.

Recovery Point Objective (RPO) - Defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization.

IV. Policy

1. Supporting Maintenance Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the County's maintenance policy. *[MA-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 enterprise maintenance policy and the associated controls;

b. Review and update the maintenance 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. *[MA-1-T]*

2. Controlled Maintenance

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

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or County requirements as well as with any County approved automated mechanisms; and

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; and

c. Require that assigned IT staff for supporting end user computing devices explicitly approve the removal of the system or system components from County facilities for off-site maintenance, repair, or replacement; and

d. Sanitize equipment to remove all information from associated media prior to removal from County facilities for off-site maintenance, repair, or replacement, except for the information which is required to operate the asset/device (i.e. Operating System, firmware, etc.); and

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in County information technology maintenance records: Computing Asset Details. *[MA-2 -T]*

g. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using approved automated mechanisms implemented within the County's digital

footprint; and

h. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed on all County owned information technology assets. *[MA-2 (2) -T]*

3. Maintenance Tools

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

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools at minimum on a yearly basis or when determined that current capabilities are not addressing current County IT maintenance needs; and *[MA-3 -T]*

c. Inspect the maintenance tools used by the County's maintenance personnel for improper or unauthorized modifications; *[MA-3 (1) -O]*

d. Check media containing diagnostic and test programs for malicious code before the media are used within the County's information technology systems; *[MA-3 (2) -T]*

e. Prevent the removal of maintenance equipment containing the County's information by:
(1) Verifying that there is no organizational information contained on the equipment;
(2) Sanitizing or destroying the equipment;
(3) Retaining the equipment within County Facilities; or
(4) Obtaining an exemption from the County's Director of Information Technology explicitly authorizing removal of the equipment from the facility. *[MA-3 (3) -T]*

f. Restrict the use of maintenance tools to authorized personnel only; *[MA-3 (4) -T]*

g. Monitor the use of maintenance tools that require system privileged user access rights or permissions; *[MA-3 (5) -O]*

h. Inspect maintenance tools to ensure the latest software updates and patches are installed. *[MA-3 (6) -T]*

4. Nonlocal Maintenance

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

a. Approve and monitor non-local maintenance and diagnostic activities;

b. Allow the use of non-local maintenance and diagnostic tools only as consistent with the County's policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of non-local maintenance and diagnostic sessions;

d. Maintain records for non-local maintenance and diagnostic activities; and

c. Terminate session and network connections when non-local maintenance is completed. *[MA- 4 -T]*

f. Log any required maintenance data for non-local maintenance and diagnostic sessions; and

g. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior. *[MA- 4 (1) -O]*

h. Require the approval of each non-local maintenance session by the Director of Information Technology; and

i. Notify the following personnel or roles of the date and time of planned non-local maintenance, to include end users, support staff, stakeholders, and any other affected parties. *[MA- 4 (5) -T]*

j. Implement cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications. *[MA- 4 (6) -T]*

k. Verify session and network connection termination after the completion of non-local maintenance and diagnostic sessions. *[MA- 4 (7) -T]*

5. Maintenance Personnel

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

a. Establish a process for maintenance personnel authorization and maintain a list of authorized County maintenance or personnel;

b. Verify that suppliers and/or contractors performing maintenance on systems possess the required access authorizations; and

c. Designate appropriate County personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. *[MA- 5 - T]*

6. Timely Maintenance

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

a. Obtain maintenance support and/or spare parts for the organization's computing assets within the established RTO/RPO timelines when activation of the BCP/DR plan during a time of failure. *[MA- 6 - T]*

b. Perform preventive maintenance on County systems at regularly scheduled intervals. *[MA- 6(1) - T]*

c. Perform predictive maintenance on organization systems at regularly scheduled and defined timelines. *[MA- 6(2) - T]*

d. Transfer predictive maintenance data to a maintenance management system using County defined and approved automated capabilities. *[MA- 6(3) - O]*

7. Field Maintenance

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

a. Restrict or prohibit field maintenance on County owned and identified assets to organization approved maintenance facilities. *[MA- 7 - 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)

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