I. Purpose

This policy establishes the Media Protection Policy, for protecting electronic and/or physical media used by the County on a day-by-day basis to support business operations. The media protection efforts will help Indian River County implement security best practices with regards to media protection throughout its use within the County's digital footprint.

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

Digital Media – A form of electronic media where data is stored in digital (as opposed to analog) form.

Electronic Media - General term that refers to media on which data are recorded via an electrically based process.

Non-Digital Media – A form of media stored as a hard copy or physical representation of information, including, but not limited to: paper copies, printer ribbons, drums, microfilm, platens, and other forms of preserved or preservable information.

Media Sanitization - The general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

Purge/Wipe - A method of Sanitization by applying physical or logical techniques that renders Target Data recovery infeasible using state of the art laboratory techniques.

IV. Policy

1. Supporting Media Protection Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the media protection policy. *[MP-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, within the scope of this policy, procedures to facilitate the implementation of the media protection policy and the associated controls;

b. Review and update the current media protection 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. *[MP-1 -T]*

2. Media Access

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

a. Restrict access to County assets to those approved to access data with a need-to-know requirement. *[MP-2 -T]*

3. Media Storage

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

a. Provide and publish guidance on physical control and on securely storing County owned digital media within approved areas, offices, cabinets, and safes; non-digital media will be controlled and overseen by the Florida statue of retention and exclusion of public release; and

b. Protect system media types defined in Section III until the media is destroyed or sanitized using approved equipment, techniques, and procedures. *[MP-4 -T]*

c. Restrict access to media storage areas and log access attempts and access granted using County approved credentials and access rights. *[MP-4(2) -T]*

4. Media Transport

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

a. Protect and control all County system media during transport outside of controlled areas using approved mechanisms for securely transporting media such as locked cases, passwords, etc.;

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel. *[MP-5 -O]*

5. Media Sanitization

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

a. Sanitize County owned media and media storage devices prior to disposal, release out of organizational control, or release for reuse using approved sanitization/destruction processes/techniques; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. *[MP-6 -T]*

c. Review, approve, track, document, and verify media sanitization and disposal actions. *[MP-6(1) -T]*

d. Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the circumstances such as hard drive re-use, County flash drive use, etc. *[MP-6(3) -T]*

e. Provide the capability to purge or wipe information from any and all County information systems either remotely or in person under the conditions of refresh/reuse or extreme cases of cyber intrusion after appropriate forensics have been performed. *[MP-6(8) -T]*

6. Media Use

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

a. Have the ability to both prohibit and restrict the use of any type of digital media on all County owned digital assets using endpoint tools to block USB's, Data Loss Prevention (DLP), when required due to data classification and/or business need, as well as policy enforcement; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner. *[MP-7 -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