I. Purpose

This policy establishes the Physical and Environmental Protection Policy, for managing risks that may affect either the environmental conditions of the County or physical location of the County's facilities. The physical and environmental protection program helps Indian River County implement security best practices with regards to the environmental and physical conditions of County locations and personnel.

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

Access Control - The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Datacenter – Dedicated space or building utilized to hold computer systems and associated components to support and organization(s).

Environmental Control – Controls that protect organizations from the loss of connectivity and availability.

Information Leakage – The intentional or unintentional release of information to an untrusted environment.

Physical Security – The capabilities to limit physical access to information systems, equipment, and any operating environments to authorized individuals.

RFID Data – Data transmitted via radio waves that can be utilized to access, track and manage hardware as well as allow or restrict people from accessing spaces.

IV. Policy

1. Supporting Physical and Environmental Protection Procedures

The Director of Information Technology in conjunction with the Public Works Director shall manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures. [PE-1 -T]

The Information Systems and Telecommunications (IS&T) Division in conjunction with the Facilities Management Division shall:

a. Develop, document, and disseminate to all staff, contractors, and consultants in their respective departments, within the scope of this policy, procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental security controls;

b. Review and update the current physical and environmental protection procedures annually 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. *[PE-1 -T]*

2. Physical Access Authorizations

The Facilities Management Division, through the Public Works Department shall:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals at least twice a year or when required due to employee termination; and

d. d. Remove individuals from the facility access list when access is no longer required. *[PE-2 -T]*

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

a. Authorize physical access to the facility where the system resides based on position or role. *[PE-2(1) -T]*

b. Require two forms of identification for visitor access to county owned facility spaces where the system(s) reside and require access to said systems.

c. Sanitize equipment to remove the any and all County owned information from associated media prior to removal from County facilities for off-site maintenance, repair, or replacement; *[PE-2(2) -T]*

d. Restrict unescorted access within the county owned facility spaces where the system(s) resides to personnel with formal access authorizations for all information contained within the system; and a need for access to all information contained within the system. [PE-2(3) -T]

3. Physical Access Control

The Facilities Management Division in conjunction with County Departments shall:

a. Enforce physical access authorizations at County facility entry and exit points for spaces that contain sensitive non-IT assets by:

I. Verifying individual access authorizations before granting access to those spaces; and

II. Controlling ingress and egress to those spaces using County approved physical access control systems or devices;

b. Control access to areas within the facility designated as publicly accessible by implementing badging controls and visitor access/entrances at all ingress/egress points of County facilities;

c. Ensure that visitors are escorted and control visitor activity when accessing restricted spaces and performing activities such as facility and/or system repair for non-IT related actives;

d. Secure keys, combinations, and other physical access devices;

e. Inventory County physical access devices every year; and

f. Change combinations every three years and keys every 5 years, if possible and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated. [PE-3 -T]

g. Enforce physical access authorizations to the system in addition to the physical access controls for the facility in restricted areas as well as where key systems are located (need to know requirement). [PE-3(1) -T]

h. Use lockable physical casings to protect all systems and restricted spaces/offices from unauthorized physical access. [PE-3(4) -O]

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

a. Maintain physical access audit logs for all County Ingress and Egress points within County datacenters;

b. Escort visitors and control visitor activity when accessing restricted spaces or performing activities such as facility and/or system repair for all IT related activities within County Datacenters; [PE-3 -T]

4. Access Control for Output Devices

The Facilities Management Division shall:

a. Control physical access to output from physical access logs and electronic RFID data to prevent unauthorized individuals from obtaining the output. *[PE-5 -T]*

b. Link individual identity to receipt of output from output devices. *[PE-5(2) -O]*

5. Monitoring Physical Access

The Information Systems and Telecommunications Division shall:

a. Monitor physical access to the portion of the facility where system(s) reside to detect and respond to physical security incidents;

b. Review physical access logs monthly; and

c. Coordinate results of reviews and investigations with the organizational incident response plan. [PE-6 -T]

d. Monitor physical access to the portion of the facility where the system(s) resides using surveillance capabilities. [PE-6(1) -O]

e. Recognize physical security intrusions and initiate appropriate actions to mitigate effects of physical intrusions. [PE-6(2) -O]

The Facilities Management Division shall:

a. Employ video surveillance of County facilities;

b. Review video recordings monthly; and

c. Retain video recordings in accordance with Florida Statutes. [PE-6(3)-O]

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

a. Monitor physical access to the system and locations with IT systems and applications. [PE-6(3)-T]

6. Visitor Access Records

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

a. Maintain visitor access records to the portion of the county owned facility where the system(s) resides.

b. Review visitor access records annually.

c. Report anomalies in visitor access records to County Facilities Management Division. [PE-8- T]

d. Maintain and review visitor access records using County approved mechanisms such as Excel, print/paper, etc. [PE-8 (1)- T]

e. Limit personally identifiable information contained in visitor access records to elements identified in the privacy risk assessment and/or any items that are identified as sensitive and/or critical to County operations. [PE-8 (3)- T]

7. Power Equipment and Cabling

The Facilities Management Division shall:

a. Protect power equipment and power cabling for the system from damage and destruction. [PE-9- T]

b. Employ redundant power cabling paths that are physically separated through the use of multiple providers or segmented utilities for each facility. [PE-9(1)- O]

c. Employ automatic voltage controls for systems that require set voltages/power conditioning within select County facilities/locations. [PE-9(2)- T]

8. Emergency Shutoff

The Facilities Management Division shall:

a. Provide the capability of shutting off power to County facilities/locations and various systems and applications in emergency situations;

b. Place emergency shutoff switches or devices in County facilities/locations and various systems and applications to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation. [PE-10- T]

9. Emergency Power

The Facilities Management Division shall:

a. Provide an uninterruptible power supply to facilitate an orderly shutdown of County applications and/or system and/or transition of County applications and/or systems to long-term alternate power in the event of a primary power source loss. [PE-11- T]

b. Provide an alternate power supply for the system that is activated either manually or automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source. [PE-11(1)- T]

c. Provide an alternate power supply for the system that is activated either manually or automatically and that is:

I. Self-contained;

II. Not reliant on external power generation; and

III. Capable of maintaining minimally required operational capabilities for the County in the event of an extended loss of the primary power source. *[PE-11(2)- T]*

10. Emergency Lighting

The Facilities Management Division shall:

a. Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. [PE-12- T]

b. Provide emergency lighting for all areas within the facility supporting essential mission and business functions. [PE-12(1)- T]

11. Fire Protection

The Facilities Management Division shall:

a. Employ and maintain fire detection and suppression systems that are supported by an independent energy source. [PE-13- T]

b. Employ fire detection systems that activate automatically, provide notification to emergency responders in the event of a fire. [PE-13(1)- T]

c. Employ fire suppression systems that activate automatically and notify emergency responders; and

d. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis. [PE-13(2)- T]

e. Ensure that the facility undergoes fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within an acceptable time period. [PE-13(4)- T]

12. Environmental Controls

The Facilities Management Division shall:

a. Maintain temperature; humidity; pressure; radiation; levels within the portion of the facility where the system(s) resides at acceptable levels; and

b. Provide emergency lighting for all areas within the facility supporting essential mission and business functions. [PE-14- T]

c. Employ the automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system]. [PE-14(1)- T]

d. Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to Facilities Management Personnel. [PE-14(2)- T]

13. Water Damage Protection

The Facilities Management Division shall:

a. Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. [PE-15- T]

b. Detect the presence of water near the system and alert Facilities Management Personnel automated mechanisms. [PE-15(1)- T]

14. Delivery and Removal

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

a. Authorize and control IT system and components entering and exiting the facility; and

b. Maintain records of the system components. [PE-16- T]

15. Alternate Work Site

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

a. Determine and document the organization approved alternate work sites allowed for use by employees as per the continuity plans;

b. Employ controls at alternate work sites that control physical security as well as logical security for employees, contractors and visitors at alternate work site(s);

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents. [PE-17- T]

16. Location of System Components

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

a. Position system components within the facility to minimize potential damage from various physical and environmental hazards that may impact said system components and to minimize the opportunity for unauthorized access. [PE-18- T]

17. Information Leakage

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

a. Protect the system from information leakage due to electromagnetic signal emanations. [PE-19-O]

b. Protect system components, associated data communications, and networks in accordance with national emissions security policies and procedures based on the security category or classification of the information. [PE-1(1)- O]

18. Facility Location

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

a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and

b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy. [PE-23- 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