I. Purpose

The purpose of this policy is to ensure proper governance and guidance of the County's contingency plan(s) in order to maintain system and service availability due to degradation or outages suffered from natural or unnatural incidents and disasters. Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

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, external agencies, 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 Information Technology service operations.

Indian River County BCC – The governing body of Indian River County.

Emergency Services Department – Responsible for development, coordination, and promotion of comprehensive emergency plans for all disaster events within Indian River County.

Business Impact Analysis – The process and documentation to evaluate and define the potential effects of an interruption to the County's critical information systems and services.

County COOP Coordinator – Individual with the overall responsibility for assuring that the COOP is reviewed and updated on an annual basis or when improvement areas are identified through drills, exercises, or actual events.

Information System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information for the various departments, officers and special dependent districts of Indian River County

Continuity of Operations Plan (COOP) – A formalized plan to ensure the County's ability to perform essential and critical functions under emergency circumstances.

IV. Policy

1. Contingency Plan

The Director of Information Technology shall manage the development, documentation, and dissemination of the contingency plan and procedures. *[CP-1-T]*

The Information Systems and Telecommunications (IT&S) Division shall:

a. Develop a contingency plan (COOP) for mission critical information that:
   I. Identifies essential mission and business functions and associated contingency requirements
   II. Provides recovery objectives, restoration priorities, and metrics;
   III. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   IV. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
   V. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   VI. Addresses the sharing of contingency information; and is shared with the Emergency Services Department.

b. Distribute copies of the contingency plan to secure locations within each County critical facility as defined in the plan;

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the systems within the departments, divisions and facilities on an annual basis;

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training [CP-1-T]

g. Protect the contingency plan from unauthorized disclosure and modification and ensure all pertinent information is handled in accordance with Florida Statutes; *[CP-2-T]*

h. Coordinate contingency plan development with organizational elements responsible for related plans. *[CP-2(1)-T]*

i. Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. *[CP-2(2)-T]*

j. Plan for the resumption of essential mission and business functions within the timeframe for each application and function as outlined in the Business Impact Analysis (BIA) of contingency plan activation. *[CP-2(3)-T]*

k. Plan for the continuance of essential mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites. *[CP-2(5)-T]*

l. Plan for the transfer of essential mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites. *[CP-2(6)-T]*

m. Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied. *[CP-2(7)-T]*

n. Identify critical system assets supporting essential mission and business functions. *[CP-2(8)-T]*

2. Contingency Training

The Information Systems and Telecommunications (IS&T) division in coordination with the other departments and divisions of the County shall:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:
   I. Within thirty- to sixty-days of assuming a contingency role or responsibility; or
   II. When required by system changes; and
   III. Coincident with plan updates and testing exercises thereafter

b. Review and update contingency training content when changes or errors have been identified and following plan updates or testing exercises. *[CP-3-T]*

c. Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations. *[CP-3(1)-O]*

3. Contingency Plan Testing

The Information Systems and Telecommunications (IS&T) division in coordination with other departments and divisions of the County shall:

a. Test the contingency plan for the system on annual basis using the following tests to determine the effectiveness of the plan and the readiness to execute the plan based on the following services:
   - Basic checklist
   - Walk-through
   - Table-top and or comprehensive simulations (parallel interruption).

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed. *[CP-4-T]*

d. Coordinate contingency plan testing with organizational elements responsible for related plans. *[CP-4(1)-O]*

e. Test the contingency plan at the alternate processing site:

   I. To familiarize contingency personnel with the facility and available resources; and
   II. To evaluate the capabilities of the alternate processing site to support contingency operations. *[CP-4(2)-T]*

f. Test the contingency plan using existing and new technological capabilities for simulating realistic test scenarios to understand the outcome of stress testing the systems and operating environment. *[CP-4(3)-O]*

g. Include a full recovery and reconstitution of the system to a previously established and working state as part of contingency plan testing. *[CP-4(4)-O]*

h. Employ mechanisms such as disablement of system components or bandwidth degradation techniques to disrupt system operations and functionality, to those components that service the essential systems and processes to disrupt and adversely affect the system or system component. *[CP-4(5)-O]*

4. Alternate Storage Site

The Information Systems and Telecommunications (IS&T) division coordination with other departments and divisions of the County shall:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site. *[CP-6-T]*

c. Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. *[CP-6(1)-T]*

d. Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. *[CP-6(2)-T]*

e. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. *[CP-6(2)-T]*

5. Alternate Processing Site

The Information Systems & Telecommunications Division (IS&T) in coordination with the Emergency Services Department and other departments and divisions of the County shall:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of applications, databases and supporting systems for essential mission and business functions defined by the objectives outlined in the Business Impact Analysis when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site. *[CP-7-T]*

d. Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats. *[CP-7(1)-T]*

e. Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. *[CP-7(2)-T]*

f. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives). *[CP-7(3)-T]*

g. Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions. *[CP-7(4)-T]*

h. Plan and prepare for circumstances that preclude returning to the primary processing site. *[CP-7(6)-T]*

6. Telecommunications Services

The Information Systems and Telecommunications (IS&T) Division, in alignment with the requirements outlined in the COOP, shall:

a. Establish alternate telecommunications services, including necessary agreements to permit the resumption of applications, databases and supporting systems for essential mission and business functions within 72 hours of when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. *[CP-8]*

b. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

c. Request Telecommunications Service Priority for all telecommunications services used for regional security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier. *[CP-8(1)-O]*

d. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services. *[CP-8(2)-T]*

e. Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats. *[CP-8(3)-O]*

f. Require primary and alternate telecommunications service providers to have contingency plans;

g. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

h. Obtain evidence of contingency testing and training by providers on an annual basis. *[CP-8(4)-O]*

i. Test alternate telecommunication services on annual basis. *[CP-8(5)-O]*

7. System Backup

The Information Systems and Telecommunications (IS&T) Division, in alignment with the requirements outlined in the COOP, shall:

a. Conduct backups of user-level information contained in applications, databases and supporting systems to meet the objectives defined in the Business Impact Analysis (BIA);

b. Conduct backups of system-level information contained in the systems and services to meet the objectives defined in the Business Impact Analysis (BIA);

c. Conduct backups of system documentation, including security- and privacy-related documentation to meet the objectives defined in the Business Impact Analysis (BIA); and

d. Protect the confidentiality, integrity, and availability of backup information. *[CP-9-T]*

e. Test backup information on a quarterly basis to verify media reliability and information integrity. *[CP-9(1)-T]*

f. Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing. *[CP-9(2)-T]*

g. Store backup copies of all media and software, required for restoration of services, in a separate facility or in a fire rated container that is not collocated with the operational system. *[CP-9(3)-O]*

h. Transfer system backup information to the alternate storage site that supports the expected recovery time and point objectives defined in the Business Impact Analysis (BIA). *[CP-9(5)-T]*

i. Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations. *[CP-9(6)-T]*

j. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all media including disk, tape and portable devices. *[CP-9(8)-T]*

8. System Recovery and Reconstitution

The Continuity of Operations team in coordination with the Emergency Services Department and other departments and divisions of the County shall:

a. Provide for the recovery and reconstitution of the system to a known state within expected recovery time and point objectives defined in the Business Impact Analysis (BIA) after a disruption, compromise, or failure. *[CP-10-T]*

b. Implement transaction recovery for systems that are transaction-based. *[CP-10(2)-T]*

c. Provide the capability to restore system components to meet expected recovery time and point objectives defined in the Business Impact Analysis (BIA) from configuration-controlled and integrity-protected information representing a known, operational state for the components. *[CP-10(4)-T]*

d. Protect system components used for recovery and reconstitution.

9. Alternative Security Mechanisms

The Information Systems and Telecommunications (IS&T) Division, in alignment with the requirements outlined in the COOP, shall:

a. Employ alternative security mechanisms for satisfying the minimal level of security requirements when the primary means of implementing the security function is unavailable or compromised. *[CP-13-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

Business Impact Analysis (BIA)

Continuity of Operations Plan (COOP)

Indian River County Comprehensive Emergency Management Plan

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)

VIII. Responsibility

Information Technology Department

IX. Authority Approval and Signature

Approved:

_____

Michael Zito

Interim County Administrator

X. Revision History

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