I. Purpose

Incident Response is the capability for the County to handle various threat events, including but not limited to malicious software, coordinated attacks from adversaries, and other system disrupted activities, that can disrupt or bring down County system operations. The Incident Response policy ensures that responsibilities and stakeholders are defined and outlines the procedures and steps required for incident identification, response and triage activities, and recovery capabilities. Incident response and the supporting evidence for incident handling are closely related to the contingency planning of the County in order to quickly and efficiently react to disruptions, such as an incident, and restore operations to a normal state. Therefore, it is necessary that Incident Response Plans (IRP) are coordinated and aligned with the County's Continuity of Operations Plans (COOP).

The purpose of this policy is to ensure proper governance and guidance of the County's incident response plan(s) in order to maintain system and service availability due to degradation or outages suffered from natural or unnatural incidents and disasters. 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 Systems and Telecommunications (IS&T).

Human Resources Department – Responsible for the formulation and administration of personnel policies that create a fair, safe and lawful working environment conducive to productivity for all directly hired County personnel and contractors.

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

Incident Response Team (IRT) – A cross-section of County personnel, representing County divisions, who are authorized and responsible to coordinate all associated activities with incidents that affect system integrity and availability of the County's operating environment.

Incident Response Plan – A formalized document that outlines the County's responsibilities, phases, and procedures to properly identify, respond and triage incident occurrences against the County's systems and operating environment.

IV. Policy

1. Incident Response Training

The Director of Information Technology shall manage the development, documentation, and dissemination of the incident response policy. *[IR-1-T]*

The Information Systems & Telecommunications (IS&T) Division in conjunction with the Human Resources Department, shall:

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
   i. Within the specified timeframes below of assuming a position and subsequent role of the County:
      - Within 30 days of account provisioning for an employee or contractor with privileged access to – County owned information systems and/or network operating environment
      - Within 30 days of assuming an incident response role or similar technical role to support incident response and recovery activities;
   ii. When required by system or procedural changes; and
   iii. On an annual or continuous basis thereafter

b. Review and update incident response training content on annual basis or when the threat or risk environment has changed, from the general threat landscape or from past events/incidents that occurred within the County's systems and general operating environment. *[IR-2-T]*

c. Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations. *[IR-2(1)-O]*

d. Provide an incident response training environment using mechanisms that simulate realistic incidents through various scenarios and stress testing the response capabilities. *[IR-2(2)-O]*

e. Provide incident response training on how to identify and respond to a breach, including the County's process for reporting a breach. *[IR-2(3)-O]*

2. Incident Response Testing

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

a. Test the effectiveness of the incident response capability for the system on a annual basis using one or more the following tests:
   - Checklist
   - Walk-through
   - Tabletop
   - Various levels of simulation (entire response team, incident coordinators, and/or executive leadership) *[IR-3-T]*

b. Test the incident response capability using realistic test scenarios reflective of the current operating environment to properly stress test the response capabilities. *[IR-3(1)-T]*

c. Coordinate incident response testing with the various elements of the County that are responsible for executing the incident response plan(s).

d. Update incident response procedures and ensure all responsible parties have sufficient training to respond during tests as well as a plan activation. *[IR-3(2)-T]*

e. Use qualitative and quantitative data from testing to:
   i. Determine the effectiveness of incident response processes;
   ii. Continuously improve incident response processes; and
   iii. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format. *[IR-3(3)-O]*

3. Incident Handling

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

a. Implement an incident handling capability for incidents that is consistent with the Incident Response Plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities as outlined in the County's Continuity of Operations Plans (COOP);

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting outcomes accordingly;

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the County; *[IR-4-T]*

e. Support the incident handling process using the following tools and output:
   - Host and application logs,
   - Network infrastructure logs including router, switch and firewall,
   - Host and network packet captures, and
   - Logs and forensics from host detection and response agent *[IR-4(1)-T]*

f. Include the following types of dynamic reconfiguration for core infrastructure components including switch, router, and firewalls as part of the incident response capability:
   - Deployment of dynamic access control lists to aggregate endpoints of switches and perimeter routers and firewalls. *[IR-4(2)-O]*

g. Identify the various classes of incidents caused by design and implementation issues to targeted and untargeted attacks against the County's infrastructure and take the following actions in response to those incidents to ensure continuation of the County's mission and business functions**:**
   - Orderly degradation of systems and services, and
   - System(s) shutdown to retain minimal service operations *[IR-4(3)-T]*

h. Correlate incident information and individual incident responses to achieve a County-Wide perspective on incident awareness and response; *[IR-4(4)-T]*

i. Implement a configurable capability to disable an information system if data or system integrity has been compromised by malware, data exfiltration activities, or from a severe software vulnerability or bug detection; *[IR-4(5)-O]*

j. Coordinate with the various stakeholders and teams as defined in the COOP to correlate and share incident response capabilities, activities and lessons learned to achieve a cross-county perspective on incident awareness and more effective incident responses; *[IR-4(8)-T]*

k. Establish and maintain an integrated incident response team (IRT) that can be deployed to any location identified by the County within the time for key personnel to perform proper triage and commute to the location point; [*IR-4(11)-T]*

l. Establish and maintain a security operations center; *[IR-4(14)-T]*

The County Administrator and Communications Manager shall:

a. Manage public relations associated with an incident

b. Employ measures to repair the reputation of the County's various districts, departments, and offices. *[IR-4(15)-T]*

4. Incident Monitoring

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

a. Track and document incidents. *[IR-5-T]*

b. Collect and analyze incident information using the specified tools and mechanisms as defined in the Incident Response Plan.

5. Incident Reporting

All County personnel shall:

a. Be required to report suspected incidents to the County's Information Systems & Telecommunications (IS&T) Division immediately upon observation;

b. Report incident information to the County's incident response hotline CIRT@ircgov.com or (772) 226-4357**;** *[IR-6-T]*

c. Report incidents using automated means of the County's Help Desk or service portal**;** *[IR-6(1)-T]*

d. Report system vulnerabilities associated with reported incidents to the personnel and teams as outlined in the Incident Response Plan. *[IR-6(2)-T]*

6. Incident Response Assistance

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

a. Provide an incident response support resource, integral to the County's incident response capability, that offers advice and assistance to users of County systems for the handling and reporting of incidents; *[IR-7-T]*

b. Increase the availability of incident response information and support using the County's Help Desk; *[IR-7(1)-T]*

c. Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and

d. Identify the County's Incident Response Team members to the external providers. *[IR-7(2)-T]*

7. Incident Response Plan

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

a. Develop an Incident Response Plan that:
   i. Provides the County with a roadmap for implementing its incident response capability;

   ii. Describes the structure and organization of the incident response capability;

   iii. Provides a high-level approach for how the incident response capability fits into the overall operations of the County;

   iv. Meets the unique requirements of the County, which relate to its mission, size, structure, and functions;

   v. Defines reportable incidents;

   vi. Provides metrics for measuring the incident response capability within the County;

   vii. Defines the resources and management support needed to effectively maintain and mature and fully capable incident response capability;

viii. Addresses the sharing of incident information;

ix. Is reviewed and approved by Information Technology Department Director and supporting senior officials on an annual basis or when significant changes are required; and

x. Explicitly designates responsibility for incident response to Information Systems and Telecommunications (IS&T) Division

b. Distribute copies of the Incident Response Plan to all stakeholders and to other supporting departments, divisions and offices as deemed necessary.

c. Update the Incident Response Plan to address system and County-Wide changes or problems encountered during plan implementation, execution, or testing;

d. Communicate Incident Response Plan changes to all stakeholders responsible for the COOP of the County.

e. Protect the Incident Response Plan from unauthorized disclosure and modification. *[IR-8-T]*

f. Include the following in the Incident Response Plan for breaches involving personally identifiable information (PII):

i. A process to determine if notice to individuals or other organizations or entities, including oversight organizations or governing bodies, is needed including the security of confidential personal information as defined by section 501.171, Florida Statutes;
ii. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
iii. Identification of applicable privacy requirements. *[IR-8(1)-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

Continuity of Operations Plan (COOP)

Incident Response Plan (IRP)

Florida Statue 501.171 – Security of confidential personal information

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. History

VERSION	DATE	CHANGES	DEPT/INDIVIDUAL
1.0	01.01.2023	Initial Publication	IT/D. Russell