I. Purpose

An audit is an independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. This policy is intended to establish the governance documentation for the auditing of County owned information systems.

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

Audit Logging Process Failure – When capabilities that collect and store logs are not operational, such as if the storage medium collecting the log data is full, or the server performing the logging fails due to a hardware or software issue.

Coordinated Universal Time (UTC) – the official, internationally agreed upon standard for world time.

Degraded Operational Mode – Continuing operations to maintain levels of service while capabilities supporting these services are reduced or unavailable for use.

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

IV. Policy

1. Supporting Audit and Accountability Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the audit and accountability policy. [AU-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 Audit and Accountability Policy and the associated controls;

b. Review and update the current audit and accountability 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. *[AU-1-T]*

2. Event Logging

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

a. Identify the types of events that the system is capable of logging in support of the audit function that are significant and relevant to the security of systems and the privacy of individuals;

b. Coordinate the event logging function with other County entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the event types for logging within the system along with the frequency and/or the situational requirements for logging each event type.

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging on annual basis and/or when the risk level to County operations justifies a change. [AU-2-T]

3. Content of Audit Records

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

a. Ensure that audit records contain information that establishes the following:
   I. What type of event occurred;
   II. When the event occurred;
   III. Where the event occurred;
   IV. Source of the event;
   V. Outcome of the event; and
   VI. Identity of any individuals, subjects, or objects/entities associated with the event. *[AU-3-T]*

b. Generate audit records containing the additional information based on system functionality to configure the audit record content. *[AU-3(1)-O]*

c. Limit personally identifiable information contained in audit records when such information is not needed for operational purposes which helps reduce the level of privacy risk created by a system. *[AU-3(3)-O]*

4. Audit Log Storage Capacity

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

a. Allocate audit log storage capacity to accommodate audit log processing requirements for every system. *[AU-4-T]*

b. Transfer audit logs based on the frequency and need defined by IS&T operations to a different system, system component, or media other than the system or system component conducting the logging. *[AU-4(1)-O]*

5. Response to Audit Logging Process Failures

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

a. Alert appropriate stakeholders upon notification in the event of an audit logging process failure; and

b. Take the necessary actions to:

i. Provide a warning to appropriate stakeholders upon notification when allocated audit log storage volume reaches defined thresholds of repository maximum audit log storage capacity. *[AU-5(1)-O]*

ii. Provide an alert immediately to appropriate stakeholders when audit failure events occur. *[AU-5(2)-O]*

iii. Invoke a degraded operational mode with limited mission or business functionality in the event of audit logging failures, unless an alternate audit logging capability exists. *[AU-5(4)-O]*

6. Audit Record Review, Analysis, and Reporting

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

a. Review and analyze system audit records on a consistent basis for indications of misuse, unusual, or malicious activity and the potential impact of such activity;

b. Report findings to all stakeholders as defined by IS&T operations; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. *[AU-6-T]*

d. Integrate audit record review, analysis, and reporting processes using automated mechanisms managed by IS&T operations. *[AU-6(1)-T]*

e. Analyze and correlate audit records across different repositories to gain County-wide situational awareness. *[AU-6(3)-T]*

f. Integrate analysis of audit records with analysis of system monitoring capabilities to further enhance the ability to identify inappropriate or unusual activity. *[AU-6(5)-O]*

g. Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. *[AU-6(6)-T]*

h. Specify the permitted actions for each system process, role and user associated with the review, analysis, and reporting of audit record information. *[AU-6(7)-O]*

i. Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis. *[AU-6(8)-O]*

7. Audit Record Reduction and Report Generation

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

a. Provide and implement an audit record reduction and report generation capability that:

I. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

II. Does not alter the original content or time ordering of audit records. *[AU-7-T]*

b. Provide and implement the capability to process, sort, and search audit records for events of interest based on the level of granularity defined by IS&T operations. *[AU-7(1)]*

8. Time Stamps

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

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet hundreds of milliseconds and that use Coordinated Universal Time (UCT), have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp. *[AU-8]*

9. Protection of Audit Information

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

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert appropriate stakeholders upon detection of unauthorized access, modification, or deletion of audit information. *[AU-9]*

c. Store audit records periodically in a repository that is part of a physically different system or system component than the system or component being audited. *[AU-9(2)-O]*

d. Authorize access to management of audit logging functionality to only those individuals that are authorized. *[AU-9(4)-T]*

e. Authorize read-only access to audit information to only those individuals that are authorized. *[AU-9(6)-T]*

f. Store audit information on a component running a different operating system than the system or component being audited. *[AU-9(7)-O]*

10. Non-repudiation

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

a. Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed a required action. *[AU-10-O]*

b. Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released. *[AU-10(3)-O]*.

11. Audit Record Retention

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

a. Retain audit records for period based on County-defined records retention policies to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. *[AU-11-T]*

b. Employ appropriate measures to ensure that long-term audit records generated by the system can be retrieved. *[AU-11(1)-O]*

12. Audit Record Generation

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

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2C. on specific systems;

b. Allow specific stakeholders or personnel to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2C that include the audit record content defined in AU-3. *[AU-12-O]*

d. Compile audit records from various system components into a system-wide (logical or physical) audit trail that is time-correlated to within tolerance levels defined by the County. *[AU-12(1)-O]*

e. Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format. *[AU-12(2)-O]*

f. Provide and implement the capability for specific stakeholders or assigned personnel to change the logging to be performed on specific system components based on defined criteria upon exceeding threshold. *[AU-12(3)-O]*

13. Cross-organizational Audit Logging

The Information Systems and Telecommunications (IS&T) division shall ensure that the information system(s):

a. Employ defined methods for coordinating defined audit information among external organizations when audit information is transmitted across organizational boundaries. *[AU-16-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

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	01.01.23	Initial Publication	IT/D. Russell