I. Purpose

The assessment, authorization, and monitoring policy governs the security control assessment process of the County and establishes the appropriate level of monitoring activities to ensure controls are efficient and effective. Control assessments include the testing and evaluation of the various controls on a system or throughout an environment to determine the extent to which those controls are implemented, operating as intended, and producing the desired outcome based on meeting the security requirements of the County. The assessment of security controls is a continuous process which supports the County's efforts to demonstrate an ever-evolving security posture based on system or environment changes and the internal and external threat landscape.

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

Authorizations – The official management decision by senior official(s) to authorize operation of systems, authorize the use of common controls (for inheritance by County systems), and explicitly accept the risk (to County operations and assets, individuals, and other external entities).

Authorizing official – Individual(s) that provide budgetary oversight for County systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls.

Control Inheritance- Typically occurs when an application and/or system receives control protection from entities other than those typically responsible for that specific application

and/or system. An example of this would be a web application hosted within a government data center. The data center has several physical security controls and therefore the web application will inherit those physical security controls.

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

Information exchange – Access to or the transfer of data outside of the County's authorization boundary in order to conduct business.

Security control assessment – The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

Specialized assessments – A specific type of assessment that improves the readiness by exercising the County's capabilities and indicating gauging current levels of performance as means to improve security program.

IV. Policy

1. Supporting Assessment, Authorization and Monitoring Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the assessment, authorization and monitoring procedures. *[CA-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 assessment, authorization, and monitoring policy and the associated controls

b. Review and update the current assessment, authorization and monitoring 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. *[CA-1-T]*

2. Control Assessments

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

a. Develop a control assessment plan that describes the scope of the assessment including:

   i. Security controls and control enhancements under assessment.

   ii. Assessment procedures to be used to determine security control effectiveness.

   iii. Assessment environment, assessment team, and assessment roles and responsibilities.

b. Assess the security controls in the information system and its environment of operation on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

c. Select the appropriate assessor or assessment team for the type of assessment to be conducted.

d. Ensure the control assessment plan is reviewed and approved by the Director of Information Technology prior to conducting the assessment.

e. Produce a security assessment report that documents the results of the assessment.

f. Provide the results of the security control assessment to key stakeholders as determined by the Director of Information Technology**.** *[CA-2-T]*

g. Employ independent assessors or assessment teams to conduct control assessments*. [CA-2(1)-O]*

h. Include specialized assessments:

   i. Performed on an as-needed basis,
   ii. Announced or unannounced based on the type of assessment, and
   iii. Based on the following: in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; and data leakage or data loss assessment. *[CA-2(2)-T]*

i. Leverage the results of control assessments performed by the designated assessor of the target environment or system when the assessment meets the defined requirements established by the key stakeholders. *[CA-2(3)-T]*

3. Information Exchange

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

a. Approve and manage the exchange of information between the system and other systems using the following agreements:
    i. interconnection security agreements;
    ii. information exchange security agreements;
    iii. memoranda of understanding or agreement;
    iv. service level agreements;
    v. user agreements; or
    vi. nondisclosure agreements;

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update, if required, the agreements annually. *[CA-3-T]*

d. Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data. *[CA-3(6)-O]*

4. Plan of Action and Milestones

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

a. Develop a plan of action and milestones for a system, environment, or program to document the planned remediation actions of the County to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones periodically based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities. *[CA-5-T]*

c. Ensure the accuracy, currency, and availability of the plan of action and milestones for the system, environment, or program using automated mechanisms deployed and managed by the Information Systems and Telecommunications (IS&T) division. *[CA-5(1)-O]*

5. Authorization

The County Administrator shall:

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by County systems;

The Information Technology Department shall:

a. Ensure that the authorizing official for the system, before commencing operations:
   i. Accepts the use of common controls inherited by the system; and
   ii. Authorizes the system to operate;

b. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by County systems;

c. Update the authorizations continuously. *[CA-6-T]*

6. Continuous Monitoring

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

a. Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the County-level continuous monitoring strategy that includes:
   i. Establishing system-level metrics to be monitored;
   ii. Establishing defined frequency for monitoring and assessment of control effectiveness;
   iii. Ongoing control assessments in accordance with the continuous monitoring strategy;
   iv. Ongoing monitoring of system and County-defined metrics in accordance with the continuous monitoring strategy;
   v. Correlation and analysis of information generated by control assessments and monitoring;

vi. Response actions to address results of the analysis of control assessment and monitoring information; and
vii. Reporting the security and privacy status of the system to defined personnel within the County on continuous basis. [CA-7-T]

b. Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis. [CA-7(1)-O]

c. Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data. [CA-7(3)-O]

d. Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
   i. Effectiveness monitoring;
   ii. Compliance monitoring; and
   iii. Change monitoring. *[CA-7(4)-O]*

e. Ensure the accuracy, currency, and availability of monitoring results for the system using automated mechanisms deployed and managed by the Information Systems and Telecommunications (IS&T) division. *[CA-7(6)-O]*

7. Penetration Testing

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

a. Conduct penetration testing annually on designated systems or environments. *[CA-8-T]*

b. Employ an independent penetration testing agent or team to perform penetration testing on the system or system components. *[CA-8(1)-O]*

c. Employ the following red-team exercises to simulate attempts by adversaries to compromise County systems in accordance with applicable rules of engagement:

   i. Social-engineering attacks, and
   ii. Technological-based attacks. *[CA-8(2)-O]*

d. Employ a penetration testing process that includes annual unannounced attempts to bypass or circumvent controls associated with physical access points to the County owned facilities. *[CA-8(3)-O]*

8. Internal System Connections

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

a. Authorize internal connections of system components or class of components to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections when connections are no longer required; and

d. Review continuously the need for each internal connection. *[CA-9-T]*

e. Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection. *[CA-9(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

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. Authority and Responsibility

Information Systems and Telecommunications (IS&T) Division

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