I. Purpose

The County's systems and the associated information within them are critical to the County's ability to perform its missions and deliver critical services to the residents of Indian River County. The senior officials view system security as a management issue and seek to protect their County's information technology resources as any other valuable asset. To do this effectively requires the development of a comprehensive management approach through program establishment and execution.

The purpose of this policy is to ensure proper management and oversight of the County's security program through the establishment of security requirements that define program management controls. Program management controls may be implemented for the entirety of the County or it can be specifically defined for the mission or business process being performed/delivered. These controls are essential for managing the County's information security program. Control requirements, and hence policy statements, are based on the adoption strategy defined by the Information Systems and Telecommunications (IS&T) Division 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 IT service operations.

IV. Policy

1. Information Security Program Plan

The Director of Information Technology shall manage the development, documentation, and dissemination of the county-wide information security program plan. *[PM-1-T]*

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

a. Develop and disseminate a county-wide information security program plan that:

   i. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
   ii. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among county entities, and compliance;
   iii. Reflects the coordination among county entities responsible for information security; and
   iv. Is approved by the County Administrator, who is responsible and accountable for the risk being incurred to county operations (including mission, functions, image, and reputation), county assets, individuals, other counties, and the state;
   v. Review and update the county-wide information security program plan annually and following county administrative changes, problems identified during plan implementation, or changes with control requirements.
   vi. Protect the information security program plan from unauthorized disclosure and modification. *[PM-1-T]*

2. Information Security Program Leadership Role

The Information Technology Department Director shall:

a. Appoint an information security officer (ISO) or similar position in rank and authority with the mission and resources to coordinate, develop, implement, and maintain a County-wide information security program. *[PM-2-T]*

3. Information Security and Privacy Resources

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

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources. *[PM-3-T]*

4. Plan of Action and Milestones Process

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

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated county systems:
   i. Are developed and maintained;
   ii. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to county operations and assets, individuals, other counties, and the state; and
   iii. Are reported in accordance with established reporting requirements of the division.

b. Review plans of action and milestones for consistency with the County's risk management strategy and county-wide priorities for risk response actions. *[PM-4-T]*

5. System Inventory

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

a. Develop and update continuously an inventory of County information systems. *[PM-5-T]*

b. Establish, maintain, and update continuously an inventory of all systems, applications, and projects that process personally identifiable information. *[PM-5(1)-T]*

6. Measures of Performance

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

a. Develop, monitor, and report on the results of information security and privacy measures of performance. *[PM-6-T]*

7. Enterprise Architecture

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

a. Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to county operations and assets, individuals, other counties, and the state. *[PM-7-T]*

b. Offload endpoint protection and response capabilities to other systems, system components, or an external provider. *[PM-7(1)-T]*

8. Critical Infrastructure Plan

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

a. Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. *[PM-8-T]*

9. Risk Management Strategy

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

a. Develop a comprehensive strategy to manage:
   i. Security risk to county operations and assets, individuals, other counties, and the state associated with the operation and use of county information systems; and
   ii. Privacy risk to individuals resulting from the authorized processing of personally identifiable information (PII);

b. Implement the risk management strategy consistently across the county; and

c. Review and update the risk management strategy on annual basis or as required, to address changes or direction from the Board of County Commissioners. *[PM-9-T]*

10. Authorization Process

The Information Technology Department Director shall:

a. Manage the security and privacy state of county systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the County's risk management process; and

c. Integrate the authorization processes into a county-wide risk management program. *[PM-10-T]*

11. Mission and Business Process Definition

The Information Systems and Telecommunications (IS&T) Division in conjunction with business process owners shall:

a. Define the County's mission and business processes with consideration for information security and privacy and the resulting risk to county operations, county assets, individuals, other counties, and the state; and

b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes on an annual basis or to address changes or direction from the Board of County Commissioners. *[PM-11-T]*

12. Security and Privacy Workforce

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

a. Establish a security and privacy workforce development and improvement program. *[PM-13-T]*

13. Testing, Training, and Monitoring

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

a. Implement a process for ensuring that the County plans for conducting security and privacy testing, training, and monitoring activities associated with County systems:
   i. Are developed and maintained; and
   ii. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the county's risk management strategy and county-wide priorities for risk response actions. *[PM-14-T]*

14. Security and Privacy Groups and Associations

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

a. Establish and institutionalize contact with selected groups and associations within the security and privacy communities:
   I. To facilitate ongoing security and privacy education and training for county personnel;
   II. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
   III. To share current security and privacy information, including threats, vulnerabilities, and incidents. *[PM-15-T]*

15. Threat Awareness Program

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

a. Implement a threat awareness program that includes a cross-county information-sharing capability for threat intelligence. *[PM-16-T]*

b. Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information. *[PM-16(1)-T]*

16. Privacy Program Plan

The Risk Management Division shall:

a. Develop and disseminate a County-wide privacy program plan that provides an overview of the program, and:
   I. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
   II. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
   III. Includes the role of the senior officer for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
   IV. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
   V. Reflects coordination among County departments and divisions responsible for the different aspects of privacy; and

VI. Is approved by a senior officer with responsibility and accountability for the privacy risk being incurred to county operations (including mission, functions, image, and reputation), county assets, individuals, other counties, and the state; and

b. Update the plan on annual basis and to address changes in federal, state or local privacy laws and policy and county changes and problems identified during plan implementation or privacy control assessments. *[PM-18-T]*

17. Privacy Program Plan

The County Administrator shall:

a. Appoint a senior officer for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the county-wide privacy program. *[PM-19-O]*

18. Dissemination of Privacy Program Information

The Risk Management Division shall:

a. Maintain a central resource webpage on the County's principal public website that serves as a central source of information about the County's privacy program and that:

I. Ensures that the public has access to information about county privacy activities and can communicate with its senior officer for privacy;
II. Ensures that County privacy practices and reports are publicly available; and
III. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices or designated individuals regarding privacy practices. *[PM-20-T]*

b. Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

I. Are written in plain language and organized in a way that is easy to understand and navigate;
II. Provide information needed by the public to make an informed decision about whether and how to interact with the county; and

III. Are updated whenever the County makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes. *[PM-20(1)-T]*

19. Accounting of Disclosures

The Risk Management Division shall:

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:
   I. Date, nature, and purpose of each disclosure; and
   II. Name and address, or other contact information of the individual, organization or entity to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or six years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request. *[PM-21-T]*

20. Personally Identifiable Information Quality Management

The Senior Privacy Officer in conjunction with the County Attorney shall:

a. Develop and document County-wide policies and procedures for:

   I. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
   II. Correcting or deleting inaccurate or outdated personally identifiable information;
   III. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and
   IV. Appeals of adverse decisions on correction or deletion requests. *[PM-22-T]*

21. Privacy Data Governance

The Senior Privacy Officer in conjunction with the County Attorney shall:

a. Develop and implement guidelines that support the de-identification needs of personally identifiable information across the information life cycle

b. Review and approve applications to release privacy data outside of the county that does not meet the qualification of public record
c. Archive the applications and the released data and perform post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid. [PM-23-T]

22. Minimization of Personally Identifiable Information Used in Testing, Training, and Research

The Senior Privacy Officer shall:

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures on an annual basis. *[PM-25-T]*

23. Complaint Management

The Senior Privacy Officer shall:

a. Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the County's security and privacy practices that includes:

I. Mechanisms that are easy to use and readily accessible by the public;
II. All information necessary for successfully filing complaints;
III. Tracking mechanisms to ensure all complaints received are reviewed and addressed within seven days;
IV. Acknowledgement of receipt of complaints, concerns, or questions from individuals within fourteen days; and
V. Response to complaints, concerns, or questions from individuals within thirty-sixty days. *[PM-26-T]*

24. Privacy Reporting

All County departments that handle personally identifiable information shall:

a. Develop reporting to demonstrate accountability with statutory, regulatory, and policy privacy mandates and disseminate to:

   I. The County Administrator, the County Attorney, designated senior officers and other personnel with responsibility for monitoring privacy program compliance

b. Review and update privacy reports on an annual basis. *[PM-27 -T]*

25. Risk Framing

The County Administrator shall:

a. Identify and document:
   I. The County's risk tolerance;

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

a. Identify and document:
   II. Assumptions affecting risk assessments, risk responses, and risk monitoring;
   III. Constraints affecting risk assessments, risk responses, and risk monitoring; and
   IV. Priorities and trade-offs considered by the county for managing risk;

b. Distribute the results of risk framing activities across county departments, divisions, and key personnel; and

c. Review and update risk framing considerations on an annual basis or when the risk profile changes. *[PM-28-T]*

26. Risk Management Program Leadership Roles

The County Administrator shall:

a. Appoint a Senior Officer accountable for risk management to align the County's information security and privacy management processes with strategic, operational, and budgetary planning processes; and

b. Establish a Risk Executive (function) to view and analyze risk from a County-wide perspective and ensure management of risk is consistent across all areas under the Board of County Commissioners. *[PM-29-T]*

27. Supply Chain Risk Management Strategy

The information Technology Director in conjunction with the Purchasing Division shall:

a. Develop a County-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of information systems, system components, and system services;

I. Implement the supply chain risk management strategy consistently across the County; and
II. Review and update the supply chain risk management strategy on an annual basis or as required, to address changes or direction from the Board of County Commissioners. *[PM-30-T]*

b. Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services. *[PM-30(1)-T]*

28. Purposing

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

a. Analyze the systems and infrastructure supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose. *[PM-32-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

Information Security Program Plan

Critical Infrastructure 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. History

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