I. Purpose

Access control is the process of granting and denying requests to either consume data from information systems for viewing and processing purposes or to enter general or specific areas of County facilities. The access controls used to enter information systems and supporting resources are described as logical access controls. Logical access controls prescribe an individual or process that requires access to a system resource and the explicit permissions and rights granted for that access. Controls may be internal or native to a system – operating system, database system, etc. – or external (Citizens of Indian River County, privately owned organizations, etc.) to facilitate the authorization and management of access.

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

Account Manager – The individual responsible for requesting, creating, issuing, modifying, and disabling user accounts.

Application Owner – An individual and/or a group with the responsibility that the program and/or programs under their privy accomplish the objective and/or requirements established for that application(s).

Covered Subject – An entity who's PII is being collected, processed and/or utilized.

Data Owners – Individual having operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

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 System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information for the various departments of Indian River County

Object – Any type of medium or system that supports and/or collects Personally Identifiable Information.

Privileged User Account – An account with access rights higher than a average user, permitted to typically perform administrative functions with authorized permissions or job duties.

Role Based Access Schema – A set standard of user profiles that are defined based on job role, responsibilities to ensure that access rights are limited to those minimally necessary to perform one's job.

System Owner – Individual having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system.

System Session – The total time spent on an activity or job purpose. This begins when a user logs in to when they log out.

IV. Policy

1. Supporting Access Control Procedures

The Director of Information Technology shall manage the development, documentation, and dissemination of the access control policy. [AC-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 access control policy and the associated controls.

b. Review and update the current access control 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. [AC-2-T]

2. Account Management

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

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require proper authorization and approval for group and role membership;

d. Specify:
   i. Authorized users of the system;
   ii. Group and role membership; and
   iii. Access authorizations (i.e. privileges) and other attributes as deemed by account type for each account;

e. Require approvals by the data owners or system owners for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with the Identity Access Request Process and supporting policies and procedures of the County;

g. Monitor the use of accounts;

h. Authorize access to the system based on:
   i. A valid access authorization;
   ii. Intended system usage; and
   iii. Other attributes as deemed by the account type;

i. Review accounts for compliance with account management requirements annually;

j. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

k. Align account management processes with personnel termination and transfer processes. [AC-2-T]

l. Support the management of system accounts using the automated process and notification capabilities of the Identity Access Request Process. [AC-2(1)-T]

m. Automatically disable temporary and emergency accounts upon notification and/or based on the termination date specified in the Identity Access Request Process. [AC-2(2)-T]

n. Disable accounts immediately or within one business day when the accounts: *[AC-2(3)-T]*
   i. Have expired;
   ii. Are no longer associated with a user or individual;
   iii. Are in violation of organizational policy; or
   iv. Have been inactive for over a three-month period.

o. Automatically audit account creation, modification, enabling, disabling, and removal actions. *[AC-2(4)-T]*

p. Require that users log out when he/she is done performing their duties or activities for a system session. *[AC-2(5)-T]*

q. Establish and administer privileged user accounts in accordance with a role-based access schema established by County operations;

r. Monitor privileged role or attribute assignments;

s. Monitor changes to roles or attributes; and

t. Revoke access when privileged role or attribute assignments are no longer appropriate. [AC-2(7)-T]

u. Only permit the use of shared and group accounts that meet the acceptable level of risk approved by the system and application owners. [AC-2(9)-T]

v. Monitor system accounts for abnormal or atypical usage based on:
   - Usage and activity outside normal time periods, and
   - Usage and activity from new or foreign locations;

w. Report atypical usage of system accounts to application and system owners along with other key stakeholders defined by the Director of Information Technology. [AC-2(12)-T]

x. Disable accounts of individuals as soon as possible, based on a request from the Human Resources Department, upon the discovery of account activity that has observed abnormal or unusual behavior which has been deemed a risk to the County's operational environment. [AC-2(13)-T]

The Human Resources Department shall:

a. Notify account managers and designated personnel in Information Systems and Telecommunications (IS&T):
   i. Within five business days prior to the last day when accounts are no longer required;
   ii. When users are terminated or transferred; and
   iii. Within five business days when system usage or need-to-know changes or access is planned to be changed for an individual; [AC-2-T]

3. Access Enforcement

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

a. Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies of the County. *[AC-3-T]*

b. Enforce discretionary access control policy requirements over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following:
   i. Pass the information to any other subjects or objects;
   ii. Grant its privileges to other subjects;
   iii. Change security attributes on subjects, objects, the system, or the system's components;
   iv. Choose the security attributes to be associated with newly created or revised objects; or
   v. Change the rules governing access control. *[AC-3(4)-T]*

c. Prevent access to security-relevant information and control capabilities such as:
   - All applicable access-control lists
   - Filtering and access rules for router and firewalls
   - System configuration parameters
   - Any cryptographic key management information (i.e., private keys, etc.) except during secure, non-operable system states. *[AC-3(5)-T]*

d. Enforce a role-based access control policy over defined subjects and objects and control access based upon pre-established user or role-based entitlements or newly proposed access requirements as stated through the approved Identity Access Request Process. *[AC-3(7)-T]*

e. Restrict access to data repositories based on the assigned data classification level. *[AC-3(11)-O]*

f. Enforce attribute-based access control policy over defined subjects and objects and control access based upon organizational, environmental, and resource attribute schemas. *[AC-3(13)-T]*

4. Information Flow Enforcement

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

a. Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on flow control policies established by IS&T operations, based on the characteristics of the information and/or the information path. [AC-4-T]

b. Uniquely identify and authenticate source and destination points by organization (in or out of County boundary), system, application, service or individual for information transfer. [AC-4(17)-T]

c. Separate information flows logically or physically using the various mechanisms and techniques provided to IS&T operations to accomplish separation based on the type of communication traffic, type of system service, or information security and classification levels. [AC-4(21)-T]

d. When transferring information between different security domains, sanitize data to minimize:
   - delivery of malicious content,
   - command and control of malicious code,
   - malicious code augmentation,
   - steganography encoded data or
   - spillage of sensitive information

   in accordance with the County's Data Disposal Policy. [AC-4(25)-T]

5. Separation of Duties

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

a. Identify and document a County-wide separation of duties schema based on each type of identity on the system; and

b. Define system access authorizations to support separation of duties. [AC-5-T]

6. Least Privilege

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

a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. [AC-6-T]

b. Authorize specific personnel with the roles of security administrators, system administrators, system security officers, system programmers, and other privileged users to:
   i. Security functions that include:
      - establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters; and
   ii. Security-relevant information that includes:
      - filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. [AC-6(1)-T]

c. Require that users of system accounts (or roles) with access to security functions and security-relevant information use non-privileged accounts or roles, when accessing non-security functions. [AC-6(2)-T]

d. Authorize network access to privileged commands on County systems and supporting infrastructure only for compelling operational requirements and document the rationale for such access in the County's security plan for the system. [AC-6(3)-T]

e. Restrict privileged accounts on the system to only County personnel that have been authorized based on title, role, or job function. [AC-6(5)-T]

f. Prohibit privileged access to the system by non-organizational users. [AC-6(6)-T]

g. Review annually the privileges assigned to all identities on County systems to validate the need for such privileges; and

h. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs. [AC-6(7)-T]

i. Prevent any County employee and/or contractor from executing approved and installed software at higher privilege levels for advanced/enhanced execution and/or functionality. [AC-6(8)-T]

j. Log the execution of privileged functions. [AC-6(9)-T]

k. Prevent non-privileged users from executing privileged functions. [AC-6(10)-T]

7. Unsuccessful Logon Attempts

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

a. Enforce a limit of 5 consecutive invalid logon attempts by a user during a 10-minute period; and

b. Allow the use of alternative authentication factors defined by IS&T that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded. [AC-7-T]; and

c. Enforce a limit of a two invalid logon attempts through use of the alternative factors by a user during a time period assigned by IS&T. [AC-7(4)-T]

8. System Use Notification

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

a. Display the County-approved notification banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

   i. Users are accessing a County system;

   ii. System usage may be monitored, recorded, and subject to audit;

   iii. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

   iv. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:
   i. Display system use information based on conditions identified by County stakeholders, before granting further access to the publicly accessible system;

   ii. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

iii. Include a description of the authorized uses of the system. [AC-8-T]

9. Concurrent Session Control

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

a. Limit the number of concurrent sessions to a defined number assigned by IS&T operations based on attributes that include account type, access privileges assigned, and criticality and sensitivity of the target system or asset. [AC-10-O]

10. Session/Device Lock

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

a. Prevent further access to the system by initiating a device lock after 15 minutes of inactivity or requiring the user to initiate a device lock before leaving the system unattended; and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures. [AC-11-T]

c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image. [AC-11(1)-T]

11. Session Termination

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

a. Automatically terminate a user session on certain systems after a period on inactivity. *[AC-12-T]*

b. Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to the County's information or system resources. *[AC-12(1)]*

c. Display an explicit logout message to users indicating the termination of authenticated communications sessions. *[AC-12(2)-T]*

12. Permitted Actions without Identification or Authentication

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

a. Identify specific user actions and service availability and functionality that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication. [AC-14-T]

13. Security and Privacy Attributes

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

a. Provide the means to associate various types of security and privacy attributes with associated attribute values for information in storage, in process, and/or in transmission;

b. Ensure that the attribute associations are made and retained with the information;

c. Establish a set of permitted security and privacy attributes from the attributes defined in (a. above) for specific County systems which includes various forms of metadata as defined by the County Administration;

d. Determine a set of attribute values or ranges for each of the established attributes as defined by the County Administration;

e. Audit changes to attributes; and

f. Review the defined security and privacy attributes for applicability on a frequency that is relevant to the source of data. *[AC-16-O]*

14. Remote Access

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

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections. [AC-17-T]

c. Employ automated mechanisms to monitor and control remote access methods. [AC-17(1)-T]

d. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. [AC-17(2)-T]

e. Route remote accesses through authorized and managed network access control points. [AC-17(3)]

f. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs:
   - Not technically feasible for local execution
   - Provides the necessary system maintenance to ensure system availability to County personnel; and

g. Document the rationale for remote access in the security plan for the system. *[AC-17(4)-T]*

h. Protect information about remote access mechanisms from unauthorized use and disclosure. *[AC-17(6)-T]*

i. Provide the capability to disconnect or disable remote access to the system based on mission, business functionality and/or criticality of the system or operating environment. *[AC-17(9)-T]*

15. Wireless Access

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

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections. *[AC-18-T]*

c. Protect wireless access to the system using authentication of users and/or devices and encryption. *[AC-18(1)-T]*

d. Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment *[AC-18(3)-T]*

e. Identify and explicitly authorize users allowed to independently configure wireless networking capabilities. *[AC-18(4)-T]*

f. Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries. *[AC-18(5)-T]*

16. Access Control for Mobile Devices

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

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems. *[AC-19-T]*

c. Employ full-device encryption and/or container-based encryption (based on the device and business purpose) to protect the confidentiality and integrity of information on mobile County devices which include mobile phones, tables, and laptop computers. *[AC-19(5)-T]*

17. Use of External Systems

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

a. Establish County-defined terms and conditions and identify the required controls consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

   i. Access the system from external systems; and

   ii. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of any external system that has not been explicitly reviewed and approved for use and consumption by the appropriate County leadership and stakeholders. [AC-20-T]

c. Permit authorized individuals to use an external system to access the system or to process, store, or transmit County-controlled information only after:

   i. Verification of the implementation of controls on the external system as specified in the County's security and privacy policies and security and privacy plans; or

   ii. Retention of approved system connection or processing agreements with the organizational entity hosting the external system. [AC-20(1)-T]

d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using the set of restrictions as defined by IS&T. *[AC-20(2)-O]*

e. Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using set of restrictions as defined by IS&T. *[AC-20(3)-T]*

f. Prohibit the use of any Internet- and/or cloud-based storage capability or service unless explicitly approved by County operation in external systems. *[AC-20(4)-O]*

g. Prohibit the use of County-controlled portable storage devices by authorized individuals on external systems. *[AC-20(5)-O]*

18. Information Sharing

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

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for information sharing circumstances where user discretion is required; and

b. Employ automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions. [AC-21-T]

19. Publicly Accessible Content

The Information Systems and Telecommunications (IS&T) division, in coordination with relevant application owners, shall:

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information periodically and remove such information, if discovered. [AC-22-T]

20. Data Mining Protection

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

e. Employ data mining prevention and detection techniques for County data storage objects such as database records and data fields to detect and protect against unauthorized data mining. [AC-23-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

Identity Access Request Process

Data Disposal Policy

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)

VII. Responsibility

Information Technology Department

VIII. Authority Approval and Signature

Approved:

_____

Michael Zito

Interim County Administrator

VIII. History

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