I. Purpose

Identification and authentication are the most prevalent techniques, along with a critical building block of information security, to protect the County's systems and infrastructure. Identification is the means of verifying the identity of users, devices and processes to grant explicit access to resources on County systems. Authentication is the means to verify the identify by requiring a unique challenge to the user, devices and processes in a manner such as a password or personal identification number (PIN). Access control requires that systems are able to identify and differentiate between users.

It is crucial to the safety and operations of County systems that access control is managed throughout its lifecycle of every provisioned identity. This policy addresses every facet of this lifecycle to ensure conformity, protection, and accountability of identities managed by security operations.

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

Application/Service Owner – individual, team or area having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of application and/or service.

Authorizing Official – An individual responsible for operating an information system at an acceptable level of risk to County operations.

Information System - discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

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

Designated Representative – An individual acting on behalf of the authorizing official in carrying out and coordinating some or all activities associated with security authorization of County systems

Registration Authority - A trusted entity that establishes and vouches for the identity and authorization of a digital identity on behalf of some authority.

IV. Policy

1. Supporting Identification and Authentication Procedures

The Director of Information Technology to manage the development, documentation, and dissemination of the identification and authentication policy. [IA-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 departments, as outlined in the scope of this policy, procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls.

b. Review and update the current identification and authentication procedures and 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. *[IA-1-T]*

2. Identification and Authentication (County Users)

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

a. Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. *[IA-2-T]*

b. Implement multi-factor authentication for local and remote access to privileged accounts. *[IA-2(1)-T]*

c. Implement multi-factor authentication for remote access to non-privileged accounts. *[IA-2(2)]*

d. When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources. *[IA-2(5)-T]*

e. Implement multi-factor authentication (including local, network, and remote access to both privileged accounts and non-privileged accounts) such that:

   i. One of the factors is provided by a device separate from the system gaining access; and
   ii. The device meets a second-factor (out-of-band token) that is verified through a channel separate from the primary factor. *[IA-2(6)-T]*

f. Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts. *[IA-2(8)-T]*

g. Provide a single sign-on capability for systems and identities that are classified as mission critical or high risk to County operations. *[IA-2(10)-T]*

h. Implement out-of-band authentication mechanisms through the use of the County's multifactor authentication (MFA) platform under the following conditions:
   - Accessing County systems and resources remotely
   - Invoking critical County operational tasks (i.e., ICSs/PLCs)
   - Accessing systems or resources that are classified by the County as high-risk. *[IA-2(13)-T]*

3. Device Identification and Authentication

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

a. Uniquely identify and authenticate non-County sanctioned devices (guest devices such as mobile phones, tablets, and notebooks) and all County-sanctioned devices such as desktops, notebooks, tablets, mobile phones, printers, and components before establishing a local, remote or network connection. *[IA-3-T]*

b. Authenticate non-County sanctioned devices (guest devices such as mobile phones, tablets, and notebooks) and all County-sanctioned devices such as desktops, notebooks, tablets, mobile phones, printers, and components before establishing local, remote or network connection using bidirectional authentication that is cryptographically based. *[IA-3(1)-O]*

c. Where Internet Protocol (IP) addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with dynamic host configuration protocol (DHCP) parameters settings defined by the IS&T division; and

d. Audit lease information when assigned to a device. *[IA-3(3)-T]*

4. Identifier Management

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

a. Manage system identifiers by:
   I. Receiving authorization from application or service owners to assign an individual, group, role, service, or device identifier;
   II. Selecting an identifier that identifies an individual, group, role, service, or device;
   III. Assigning the identifier to the intended individual, group, role, service, or device; and
   IV. Preventing reuse of identifiers is prohibited unless the original identifier has been properly decommissioned and removed from the system or device. *[IA-4-T]*

b. Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts. [IA-4(1)-T]

c. Manage individual identifiers by uniquely identifying each individual that is not an employee of the County such as contractors, consultants and temporary staff. [IA-4(4)-T]

d. Maintain the attributes for each uniquely identified individual, device, or service in the centralized directory services managed by IS&T operations. *[IA-4(9)-T]*

5. Authenticator Management

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

a. Manage system authenticators by:
   I. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
   II. Establishing initial authenticator content for any authenticators issued by the organization;

III. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
IV. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
V. Changing default authenticators prior to first use;
VI. Changing or refreshing authenticators every 90 days or when the risk environment has changed for the County's operating environment has occurred;
VII. Protecting authenticator content from unauthorized disclosure and modification;
VIII. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
IX. Changing authenticators for group or role accounts when membership to those accounts changes. *[IA-5-T]*

b. For password-based authentication:
   I. Maintain a list of commonly-used, expected, or compromised passwords and update the list quarterly and when County passwords are suspected to have been compromised directly or indirectly;
   II. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords from the requirement above;
   III. Transmit passwords only over cryptographically-protected channels;
   IV. Store passwords using an approved salted key derivation function, preferably using a keyed hash;
   V. Require immediate selection of a new password upon account recovery;
   VI. Allow user selection of long passwords and passphrases, including spaces and all printable characters;
   VII. Employ automated tools to assist the user in selecting strong password authenticators; and
   VIII. Enforce the following composition and complexity rules:
      - Upper or lowercase letters (A through Z and a through z)
      - Numeric characters
      - Non-alpha characters like $, # or %
      - Non-reuse of the previous 12 passwords
      - Cannot include any part of the user's name or username
      - Minimum of 12 characters. *[IA-5(1)-T]*

c. For public key-based authentication:
   I. Enforce authorized access to the corresponding private key; and
   II. Map the authenticated identity to the account of the individual or group; and

d. When public key infrastructure (PKI) is used:

I. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
II. Implement a local cache of revocation data to support path discovery and validation. *[IA-5(2)-T]*

e. Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage. *[IA-5(7)-T]*

f. Implement single sign-on, based on platform or system capability, or enforce one-time password through the County's multi-factor authentication (MFA) system to manage the risk of compromise due to individuals having accounts on multiple systems. *[IA-5(8)-T]*

g. Prohibit the use of cached authenticators after 30 days. *[IA-5(13)-T]*

h. For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications. *[IA-5(14)-O]*

i. Require that the issuance of identities for all County systems be conducted in person or validated by authorizing official or designated representative before provisioned or assigned with authorization by authorizing official, designated representative, or system owner(s). *[IA-5(16)-T]*

j. Provide password managers sanctioned by Information Systems and Telecommunications (IS&T) to help users generate and manage passwords; and

k. Protect the passwords using the appropriate encryption and hash methods approved by Information Systems and Telecommunications (IS&T). *[IA-5(18)-T]*

6. Authentication Feedback

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

a. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals. *[IA-6-T]*

7. Cryptographic Module Authentication

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

a. Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication. *[IA-7-T]*

8. Identification and Authentication (non-County Users)

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

a. Uniquely identify and authenticate non-County users or processes acting on behalf of non-County users. *[IA-8-T]*

b. Conform to the following profiles for identity management:
   - Guest profile
   - Contractor profile, and
   - Consultant profile. *[IA-8(4)-T]*

9. Service Identification and Authentication

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

a. Uniquely identify and authenticate the following services before establishing communications with devices, users, or other services or applications under the ownership and management of the County:
   - Web services such as applications and application program interfaces (APIs)
   - Other services that require system operability and availability to maintain County operations *[IA-9-T]*

10. Adaptive Authentication

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

b. Require all identities accessing County owned information systems to either reauthenticate, provide new credentials through forced password reset, or be denied access to County systems or resources under the following circumstances:

   - Users accessing the County's network remotely from locations unknown, change from normal patterns, or from suspicious or known malicious networks
   - Accessing greater quantities of information than what individuals would normally or routinely access

- Meet other suspicious behavior patterns or activities defined by IS&T operations. *[IA-10-T]*

11. Re-authentication

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

a. Require users to re-authenticate upon the following circumstances and situations:
   - Upon time out period on device or system inactivity
   - When roles, authenticators or credentials change
   - Upon the execution of privilege user functionality
   - Severed communication paths or connections, and
   - High-risk assets that require enhanced authentication. *[IA-11-T]*

12. Identity Proofing

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

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence. *[IA-12-T]*

d. Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization. *[IA-12(1)-T]*

e. Require that the validation and verification of identity evidence be conducted in person before a designated registration authority. *[IA-12(4)-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)

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