Proposed

Lake County Policy	***Identification and Authentication Policy***
	Approved by the County Board on: **Month DD, YYYY**

1. Purpose and Intent

1.1 The purpose of this policy is to ensure that only authorized users and devices can access Lake County's Information Systems by establishing secure and consistent processes for verifying identity. This policy provides the foundation for managing user and device access, protecting County data, and supporting compliance with cybersecurity standards.

2. Background

2.1 Identity and authentication are critical components of Lake County's overall cybersecurity strategy. Without proper controls, unauthorized access can lead to data breaches, service disruptions, and loss of public trust. This policy addresses those risks by requiring secure methods for identifying users and devices, managing credentials, and verifying access. These standards help ensure that only authorized individuals and systems can interact with County resources in a secure and accountable manner.

2.2 This policy aligns with recognized cybersecurity frameworks, including:

2.2.1 NIST 800-53 controls for user and device authentication, account management, and secure cryptographic access

2.2.2 CIS Controls v8, specifically those related to managing accounts, enforcing access rules, and securing login credentials

3. Scope

3.1 This Policy applies to Employees of Enterprise Information Technology (EIT) and all Lake County decentralized IT teams within other departments that manage information systems. The term IT Departments will incorporate any group who acquires, supports, or manages information technology assets or capabilities.

3.2 This policy shall be interpreted consistent with and subject to applicable law. It supersedes all previous policies and/or memoranda that may have been issued on subjects covered in this policy. Should any provision in this policy conflict with a specific provision in any other Board approved policy, the provisions in this policy shall take precedence.

3.3 This policy is not intended to supersede or limit the County from enforcing programs or provisions in any applicable collective bargaining agreement.

4. Authority

4.1 The County Administrator through the Chief Information Officer (CIO) is directed and has the authority to establish, maintain, and enforce an Identification and Authentication policy.

4.2 The County Administrator is authorized to develop and issue directives and procedures for the effective implementation and enforcement of this policy and to adapt to changing circumstances and business needs, consistent with County's commitment to maintaining cyber security.

4.3 Department, office, and commission leadership must ensure compliance with this policy, but have the authority to require additional requirements, not to conflict or replace the requirements directed by the County Administrator through the CIO.

5. Policy

5.1 Identification and Authentication

5.1.1 The County's Information Systems shall require every user to have a unique login ID and password (or other approved method) to prove their identity before gaining access.

5.2 Device Identification and Authentication

5.2.1 Any device that connects to the County network shall be verified as an approved device before access is allowed.

5.3 Account (Identifier) Management

5.3.1 Usernames and device IDs shall only be created or approved by authorized County staff.

5.3.2 Each person, group, or device shall be given a unique login ID.

5.3.3 Login IDs shall not be reused for a set period of time once they are deactivated.

5.3.4 Accounts shall be disabled after being inactive for a defined period.

5.4 Authenticator Management – Passwords, Tokens, and other Login Methods

5.4.1 The County shall confirm a person's or device's identity before giving out a password, token, or other login method.

5.4.2 All passwords and login methods shall meet standards set by EIT.

5.4.3 Passwords, tokens, or other login methods shall meet applicable standards set by EIT

5.4.4 The County shall have procedures for issuing, resetting, replacing, and removing login credentials.

5.4.5 Default passwords on new systems shall be changed before they are put into use.

5.4.6 All passwords and login methods shall be kept secure and protected from disclosure.

5.4.7 Users and devices shall follow security practices to protect their login credentials.

5.4.8 Shared or group accounts shall have their passwords changed whenever membership changes.

5.5 Login Screen Feedback

5.5.1 The system shall hide passwords or other login details during entry (for example, showing dots instead of characters) so they cannot be seen or stolen.

5.6 Cryptographic Module Authentication

5.6.1 When encryption tools are used for login or security, the County shall follow all applicable federal laws, regulations, and standards for how those tools are secured and used.

6. Severability

6.1 If any section or provision of this policy should be held invalid by operation of law, none of the remainder shall be affected.

7. Non-Discrimination

7.1 Lake County prohibits the discriminatory application, implementation, or enforcement of any provision of this policy on the basis of race, color, sex, age, religion, disability, national origin, ancestry, sexual orientation, marital status, parental status, military discharge status, source of income, gender identity, housing status, or any other protected category established by law, statute, or ordinance.

8. Definitions

8.1 **Authenticator** - A piece of information or object (e.g., password, token, smart card) used to confirm the identity of a user or device.

8.1.1 **Login Screen Feedback** -The visible response or cues provided during the login process (e.g., typing a password). This must be obscured (e.g., masked with asterisks) to prevent unauthorized observation.

8.1.2 **Authenticator Strength** -The measure of how secure an authenticator is based on its complexity and resistance to attacks (e.g., password length, use of special characters, two-factor authentication).

8.1.3 **Reuse Conditions** (for Authenticators) - Rules that restrict how frequently an old password or authenticator can be reused.

8.1.4 **Lifetime Restrictions** (for Authenticators) - Defined time periods for how long an authenticator (like a password or token) remains valid before it must be changed.

8.2 **Authorized Personnel** - Individuals who have been granted the authority to approve and manage system identifiers or authenticators, typically within EIT or designated department leadership.

8.3 **Cryptographic Module** - Hardware or software component that performs encryption or decryption and requires authentication.

8.4 **Device** - Any hardware asset that can connect to the Lake County network, including but not limited to desktops, laptops, mobile phones, servers, tablets, and IoT devices.

8.5 **Group/Role Account** - An account assigned to a set of users performing the same role or function. For example, a shared account used by a department for a specific purpose.

8.6 **Identifier** - A unique name or code (e.g., username, device ID) assigned to a user, device, group, or role to distinguish it from others in the system.

8.6.1 **Inactive Identifier** - An account or identifier that has not been used within a defined period. The system must disable such identifiers to prevent unauthorized access.

8.7 **Information System** - A system that includes hardware, software, networks, and processes used to collect, store, process, and transmit Lake County data. This includes County-managed devices, applications, infrastructure, and any technology used for County operations.

8.8 **IT Departments** - Any team, centralized or decentralized within Lake County, that supports, manages, or acquires information technology assets or services.

8.9 **User** - Any individual who is granted access to Lake County Information Technology (IT) resources, regardless of employment status or affiliation. This includes, but is not limited to, County employees, elected officials, contractors, consultants, temporary personnel, volunteers, board or commission members, and individuals affiliated with external agencies or governmental bodies who are provided credentials or access by the County.

Policy History			
Version	**Date Adopted**	**Legistar Item #**	**Notes**
Original	Month DD, YYYY	26-0234	--