Proposed

Lake County Policy	*Access Control Policy*
	Approved by the County Board on: **Month DD, YYYY**

1. Purpose and Intent

1.1 The purpose of this Access Control Policy is to establish a structured, consistent, and risk-based framework for managing user access to Lake County's IT resources. This policy ensures that only authorized individuals are granted access based on their job responsibilities, and that access is appropriately reviewed, modified, or revoked in a timely manner. The intent is to reduce the risk of unauthorized access, protect sensitive information, and uphold the County's commitments to data security, operational continuity, and regulatory compliance.

2. Background

2.1 Access control is a foundational element of Lake County's information security program. Without clearly defined and enforced access controls, the confidentiality, integrity, and availability of County IT resources are at risk from accidental misuse, malicious activity, or insider threats. By implementing and maintaining effective account management, authentication, and least privilege principles, the County can prevent data breaches, limit exposure from compromised accounts, and ensure accountability for system usage. This policy formalizes the standards and responsibilities necessary to protect County IT resources while enabling appropriate access for Users to perform their duties.

2.2 This policy aligns with key requirements from national and industry-recognized frameworks, including:

2.2.1 NIST 800-53**:** Access Control, Identification and Authentication, and System Protection

2.2.2 CIS Controls**:** Account Management, Least Privilege, and Secure Remote Access

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 IT resources. The term IT Departments will incorporate any group who acquires, supports, or manages information technology assets or capabilities.

3.2 This Policy also applies to Information Owners and other designated Department authorities responsible for approving access to IT resources and Sensitive (Non-Public) Information.

3.3 Where IT resources are vendor-managed, legacy, or otherwise limited in available security controls, IT Departments shall implement the requirements of this Policy to the extent supported and shall document exceptions and compensating controls in accordance with County-established standards.

3.4 This policy establishes the Countywide minimum standards for the use and protection of Lake County Information Technology Resources (IT resources). Departments, elected offices,

boards, and commissions may adopt additional policies, procedures, and standards to address their specific operational, legal, regulatory, or program requirements. Such supplemental requirements are intended to complement this Policy and may be more restrictive but shall not diminish or conflict with the minimum requirements set forth in this Policy. Users are responsible for complying with this Policy and any applicable department, office, board, or commission-specific requirements.

3.5 For department-managed applications and systems, department leadership may establish and enforce application-specific access, and data-handling requirements (including vendor terms and regulatory obligations), provided such requirements supplement and do not conflict with this Policy or Countywide cybersecurity standards.

3.6 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.

3.7 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 Access Control 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 cybersecurity.

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 IT Departments shall implement and maintain safeguards to protect County IT resources. EIT shall maintain the Countywide security standards and baselines that support this policy, in coordination with IT Departments. Where a required standard does not yet exist, EIT and the responsible IT Department shall define and document interim requirements until a formal standard is established. Exceptions shall be documented and supported by compensating controls.

5.2 Account Management and Access Authorization

5.2.1 Access to County IT resources shall be requested or changed using an approved access request and approval process.

5.2.2 For EIT-managed systems, the approved process is the System Access Request (SAR). For IT resources not managed by EIT, the responsible IT Department may use an equivalent access request and approval process.

5.2.3 IT Departments shall define what types of User accounts are needed (such as group accounts, vendor accounts, emergency accounts, etc.) based on the business and operational needs of the IT resources they support.

5.2.4 Only authorized administrators shall create and assign User accounts for County IT resources as designated by the responsible IT Department.

5.2.5 Information Owners shall define the information required to approve a User's access request and the appropriate level of access for that User.

5.2.6 No accounts shall be created without documented approval by the designated Information Owner (or authorized Department approver). The Information Owner shall provide final approval for the User's access level based on job responsibilities.

5.2.7 Accounts that have elevated or administrative access shall be requested and approved through the System Access Request (SAR) process managed by EIT or through a Department-approved access request and approval process for Department-managed systems that provides equivalent documentation, authorization, and auditability.

5.2.8 IT Departments shall follow County or EIT-established procedures for creating, changing, disabling, and removing accounts (e.g., new hire, role change, separation). Where EIT procedures do not apply to a Department-managed IT resource the responsible IT Department shall maintain a process appropriate to the system and risk.

5.2.9 IT Departments shall ensure appropriate monitoring and regular review of account activity based on access level and system risk.

5.2.10 IT Departments shall have a process to notify Account Managers when a User's access should be changed or removed, for example, when someone leaves the County or changes jobs.

5.2.11 IT Departments shall regularly review accounts for systems that process, store, or transmit Sensitive (Non-Public) Information.

5.2.12 IT Departments shall regularly review privileged accounts consistent with EIT standards, where applicable.

5.3 Password Requirements

5.3.1 Password and other authentication requirements for County IT resources are governed by the County's Identification and Authentication Policy and EIT password standards. IT Departments shall ensure systems comply with those requirements and document approved exceptions and compensating controls where needed.

5.4 Access Enforcement

5.4.1 EIT shall configure and maintain County IT resources so that access is granted only to authorized Users, and approved permissions are applied consistently and updated when accounts, roles, or group memberships change.

5.5 Sensitive Data Sharing Governance

5.5.1 Before a new or changed method of sharing Sensitive (Non-Public) Information between systems is implemented, the designated Information Owner shall document the purpose, the information being shared, the intended recipients, and required protections. The responsible IT Department shall review the request before implementation.

5.6 **Separation of Duties**

5.6.1 High-risk privileged actions shall require separate individuals for approval and execution. Where this separation is not feasible, the exception shall be documented and compensating controls implemented (such as additional approval, independent review, and enhanced logging/monitoring).

5.7 **Least Privilege**

5.7.1 Information Owners shall define appropriate access based on job responsibilities. IT Departments shall implement access, so Users and system processes have only the minimum access needed.

5.8 **Unsuccessful Logon Attempts**

5.8.1 IT resources shall automatically lock an account after a maximum number of invalid or unsuccessful logon attempts, consistent with EIT standards and configuration baselines, where technically feasible.

5.9 **System Use Notification**

5.9.1 IT Departments shall display a system use notification (banner), where technically feasible, on remote access services, administrative interfaces, and IT resources that process, store, or transmit Sensitive (Non-Public) Information, prior to granting access.

5.10 **Publicly Available IT Resources**

5.10.1 Publicly available IT resources that provide interactive access (e.g., user input, accounts, transactions, or services) shall, where technically feasible, display a system use notice that describes authorized use and any applicable monitoring, recording, or auditing. The notice shall remain visible until the User acknowledges it before proceeding. IT resources used only to view publicly available information may be exempt from this requirement.

5.11 **Session Lock**

5.11.1 IT resource sessions shall lock after a period of inactivity, or upon receiving a request from the User, in accordance with EIT-established standards in coordination with IT Departments and configuration baselines, where technically feasible.

5.11.2 A session lock shall remain in place until the User re-authenticates using established identification and authentication methods.

5.12 **Session Termination**

5.12.1 IT resources shall automatically terminate user sessions after a period of inactivity, consistent with EIT-established standards in coordination with IT Departments and configuration baselines, where technically feasible.

5.13 **Unauthenticated Access**

5.13.1 IT Departments shall document any system functions available without user authentication as part of system onboarding or periodic security review. The Information Owner shall provide the justification for allowing unauthenticated access, and IT Departments shall document the safeguards, with priority given to IT resources involving Sensitive (Non-Public) Information.

5.14 **Remote Access**

5.14.1 Remote access to Lake County IT resources shall be provided using EIT-provided remote access services and configurations (e.g., VPN/secure access gateways) to support access control, monitoring, and logging.

5.14.2 If a non-standard remote access method is required, the exception shall be documented (including justification and safeguards) and include compensating controls by the responsible IT Department. Privileged remote access shall follow County privileged access requirements where applicable.

5.15 **Wireless Access**

5.15.1 EIT shall define and maintain wireless configuration and connection requirements for access to Lake County IT resources and the Lake County network, including the use of encryption and authentication for Users and devices.

5.15.2 Public or guest wireless networks shall be separated from the Lake County network and shall not provide a path to internal County systems or infrastructure.

5.16 **Access Control for Mobile Devices**

5.16.1 Mobile access to Sensitive (Non-Public) Information shall use safeguards appropriate to the risk and available technical capabilities to reduce exposure if a device is lost or compromised.

5.16.2 Where technically feasible, mobile access methods shall minimize or prevent local storage/offline caching/download of Sensitive (Non-Public) Information; regulated or high-risk use cases shall use managed mobile controls appropriate to the information.

5.17 **Information Sharing**

5.17.1 Information that is restricted by applicable law, regulation, or County policy may be shared only with documented authorization by the designated Information Owner (or documented designee) and in accordance with applicable law and County information security policies and standards.

5.18 **Publicly Accessible Content**

5.18.1 Information Owners shall designate who is authorized to post content to publicly available IT resources or websites.

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. References

8.1 NIST SP 800-63 (Digital Identity Guidelines)

8.2 NIST Cybersecurity Framework (CSF)

8.3 CIS Critical Security Controls v8 — Identity and Access Management related safeguards

8.4 County-established standards and baselines maintained by EIT in coordination with IT Departments

9. Definitions

9.1 **Access Control** – The process of granting or denying specific requests to obtain and use information and related IT resource services.

9.2 **Account Manager** – An individual authorized by EIT or a Department to create, modify, disable, and remove user accounts and group/role memberships for designated IT resources.

9.3 **Authentication** – The process of verifying a user's identity before granting access to County systems or data, typically using usernames, passwords, security tokens, or multi-factor authentication (MFA).

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

9.5 **Compensating Controls** – Alternative or additional safeguards implemented to reduce risk when a required control cannot be fully implemented. Compensating controls may include, but are not limited to, enhanced logging/monitoring, management approval, multi-factor authentication, network segmentation, time-bound access, independent review, or increased audit frequency.

9.6 **County-Approved** – Formally authorized for use within Lake County based on County-established standards, governance, or documented risk acceptance. County approval may be granted through EIT processes or, for Department-managed systems, through a Department-approved process that provides equivalent documentation, authorization, and auditability.

9.7 **County-Established Standards** – Security and technology standards maintained by Enterprise IT (EIT) in coordination with IT Departments that define minimum requirements and configuration expectations for County IT resources, including any approved exceptions and compensating controls.

9.8 **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.

9.9 **Emergency (Break-Glass) Account** – A privileged account intended for use during outages or emergency conditions when normal authentication or administrative access methods are unavailable, subject to heightened monitoring and post-use review.

9.10 **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.

9.11 I**dentifier** - 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.

9.12 **Inactive Identifier** - An account or identifier that has not been used within a defined period.

The system shall disable such identifiers to prevent unauthorized access.

9.13 **Information Owner** – The designated Department authority responsible for a system, application, or dataset, including approving access, determining appropriate access levels, and ensuring information is handled according to law and County policy.

9.14 **Information Technology Resources (IT resources)** - All technology tools and services owned or managed by the County. This includes:

9.14.1 Computers, laptops, servers, and mobile devices

9.14.2 Software and applications

9.14.3 Email, collaboration, and file-sharing platforms

9.14.4 County networks, cloud services, internet access, and phone systems

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

9.16 **Least Privilege** – Granting only the minimum access necessary for a user or process to perform authorized duties, for the minimum time required.

9.17 **Privileged Account** – An account with elevated permissions that can administer systems, manage security settings, change configurations, access sensitive data broadly, or impact system availability (e.g., administrator, root, domain admin, application admin).

9.18 **Sensitive (Non-Public) Information** – Any data that must be protected due to legal, regulatory, ethical, or business requirements. This includes, but is not limited to:

9.18.1 Personally Identifiable Information such as Social Security numbers, health records, or financial data.

9.18.2 Internal County information not intended for public release. Information protected under laws such as HIPAA, FERPA, or Illinois state privacy regulations.

9.19 **System Access Request (SAR)** - Process for departments to request authorized access to an IT resource.

9.20 **Third-Party (Vendor) Account** – An account issued to a non-County user (e.g., vendor/partner/contractor) to support or access County IT resources under an agreement and defined authorization.

9.21 **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	26-0520	--