Proposed

Lake County Policy	*System and Communications Protection Policy*
	Approved by the County Board on: Month DD, YYYY

1. **Purpose and Intent**

   1.1. This policy defines minimum requirements to protect Lake County IT resources and County information, including data transmitted across networks and data stored on systems and devices. It is intended to reduce the risk of unauthorized access, data compromise, and service disruption by requiring County-established safeguards, consistent with applicable law and regulatory obligations.

2. **Background**

   2.1. County IT resources and the communications that connect them are frequent targets for cyber threats. Attackers may attempt to intercept data, disrupt services, or gain unauthorized access by exploiting weaknesses in network connections, system interfaces, or encryption practices. This policy sets Countywide expectations for protecting system boundaries and communications and for using County-approved safeguards to reduce these risks.

   2.2. This policy is aligned with recognized cybersecurity guidance, including the NIST Risk Management Framework and the NIST SP 800-53 System and Communications Protection (SC) control family.

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. 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.

3.6. 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.

3.7. 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 this policy.

4.2. The County Administrator is authorized to issue directives and procedures for implementation of this policy and to adapt them to changing circumstances and business needs, consistent with County-established standards and Lake County's commitment to 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 and communications. 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. **Network Access Controls and Separation**

5.2.1. IT Departments shall use County-established safeguards to control and monitor network connections into and out of County IT resources and, based on risk, between important internal network areas.

5.2.2. Publicly accessible services shall be kept separate from internal networks using network separation or equivalent isolation.

5.2.3. Connections to external networks and third-party systems shall use County-approved connection methods and safeguards.

5.3. **Secure Connections and Data Transmission**

5.3.1. IT Departments shall use standard secure connection methods (e.g., encrypted sessions and service authentication) to help ensure Users and systems connect to the intended service and to reduce the risk of interception or unauthorized takeover, where technically feasible.

5.3.2. IT resources shall terminate sessions or require re-authentication after a period of inactivity, based on risk and supported capabilities.

5.4. **Encryption and Digital Certificates**

5.4.1. IT Departments shall use County-approved encryption to protect Sensitive (Non-Public) Information when transmitted over networks and when stored, consistent with applicable law.

5.4.2. IT Departments shall manage encryption keys securely throughout their lifecycle (including creation, storage, use, rotation, and retirement).

5.4.3. IT Departments shall obtain, use, and manage digital certificates used to secure County systems and communications through County-approved services and processes.

5.5. **Protecting Stored Sensitive Information**

5.5.1. IT Departments shall protect Sensitive (Non-Public) Information when stored using safeguards appropriate to the risk and available technical capabilities, consistent with applicable law.

5.6. **Separating Administrative Functions and Shared Use Protections**

5.6.1. IT Departments shall separate system administration and management functions from end-user functions so that user-facing components cannot perform administrative actions.

5.6.2. IT Departments shall configure shared IT resources using available access controls to limit access to authorized Users and reduce the risk of unauthorized access or disclosure, based on the sensitivity of the information and technical capabilities.

5.6.3. IT Departments shall implement safeguards that reduce the ability of one running program, service, or process to interfere with another.

5.7. **Specialized Services and Internet-Facing Technologies**

5.7.1. IT Departments shall manage the use of web-based code and scripting technologies to reduce the risk of unauthorized code execution, data exposure, or malicious content being delivered through web applications or browsers.

5.7.2. IT Departments shall configure and manage internet-based voice and video services to reduce the risk of unauthorized access, eavesdropping, data leakage, or misuse (including inappropriate recording or external sharing).

5.7.3. Where the County operates services that translate website names into network addresses (commonly called the Domain Name System or DNS), IT Departments shall protect those services against tampering and unauthorized changes and shall implement reliability measures to support availability.

5.8. **Resilience and Availability Protection**

5.8.1. IT Departments shall implement safeguards to reduce the likelihood and impact of service disruptions, including denial-of-service conditions, consistent with the IT Department's security architecture.

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 800-53, System and Communications Protection (SC) control family

   8.2. NIST Risk Management Framework (RMF)

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

9. **Definitions**

   9.1. **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).

   9.2. **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.

   9.3. **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.

   9.4. **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.

   9.5. **Data at Rest** - Information stored on a device or system (including servers, endpoints, databases, cloud storage, removable media, and backups).

   9.6. **Data in Transit** - Information being transmitted between devices, systems, or services over a network (including the internet, wireless networks, and internal networks).

   9.7. **Digital Certificate (PKI Certificate)** - A digital credential used to prove the identity of a system or service and support secure, encrypted communications.

   9.8. **Encryption Key** - A digital value used to encrypt or decrypt information and to establish secure communications.

   9.9. **Externally Accessible Services** - IT resources or services that can be accessed from outside County networks (for example, public websites, external portals, remote access services, or internet-facing applications).

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

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

9.11.1. Computers, laptops, servers, and mobile devices

9.11.2. Software and applications

9.11.3. Email, collaboration, and file-sharing platforms

9.11.4. County networks, cloud services, internet access, and phone systems

9.12. **Network Separation** – The practice of keeping systems or network areas logically separated to reduce exposure and limit the impact of a security incident.

9.13. **Secure Connection** – A protected connection that helps ensure communications are encrypted and that Users and systems are connected to the intended service.

9.14. **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:

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

9.14.2. Internal County information not intended for public release.

9.14.3. Information protected under laws such as HIPAA, FERPA, or Illinois state privacy regulations.

9.15. **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.

9.16. **Vendor-Managed System or Service** – An IT resource hosted, operated, or technically administered by a third party on the County's behalf, where the County may have limited ability to configure certain controls.

9.17. **Web-Based Code and Scripts** – Code delivered through a website or web application (such as scripts or embedded code) that runs in a browser or application and may affect how content is displayed or processed.

9.18. **Website Address Services** – Services that translate website or service names into network addresses (commonly called the Domain Name System or DNS).

Policy History			
Version	**Date Adopted**	**Legistar Item #**	**Notes**
Original	Month DD, YYYY	26-0521	--