Proposed

Lake County Policy	*Acceptable Use Policy*
	Approved by the County Board on: **Month DD, YYYY**

1. Purpose and Intent

1.1 The purpose of this Acceptable Use Policy is to establish appropriate and acceptable practices and responsibilities regarding the use of IT resources, which will protect proprietary, personal, privileged, or otherwise sensitive data.

2. Background

2.1 Lake County employees have access to County information and County systems, technology and other information resources, including County-owned hardware, software, and computer network access. This policy refers to all such information, data, systems, technology, and resources collectively as “Information Technology Resources (IT resources)”. As stewards of IT resources, each employee is responsible for protecting these resources.

2.2 Inappropriate use exposes the County to risks including cyber-attacks, compromise of network systems and services, information breaches and legal issues. Inappropriate personal use of IT resources on County time also deprives the County of another valuable resource, employee time and service.

2.3 To avoid these problems, every User who accesses IT resources must know and understand the following guidelines and conduct their activities accordingly.

2.4 This policy has been developed in alignment with and is derived from the State of Illinois Department of Innovation and Technology’s Acceptable Use Policy.

3. Scope

3.1 This policy applies to all County employees in departments supervised by the County Administrator, employees that fall under the authority of the Lake County Board’s Employee Policies and Procedures Manual, and all Users who have access to the County network or IT resources.

3.2 This policy shall be interpreted consistent with and subject to applicable law. This policy supersedes all previous Countywide policies and/or memoranda that may have been issued on subjects covered in this policy; department, office, board, or commission-specific policies may remain in effect to the extent they supplement and do not conflict with this policy.

3.3 This policy establishes the Countywide minimum standards for the use and protection of Lake County 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.

3.4 For department-managed applications and systems, department leadership may establish and enforce application-specific acceptable use, 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.

3.5 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 a County-wide acceptable use 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 General Use and Ownership

5.1.1 Every User must avoid all activity that compromises the security, performance or integrity of IT resources, or that negatively impacts the IT resources or other Users.

5.1.2 County Users, vendors, business partners, and other governmental agencies must first be authorized by Enterprise Information Technology (EIT) or through the system access request (SAR) process before accessing IT resources.

5.1.3 All individuals who access IT resources may be required to undergo personnel screening determined by each department.

5.1.4 Users must use IT resources within the scope of their employment or contractual relationship with the County only and must agree to abide by the terms of this policy. Such agreement will be evidenced by the User's acceptance of the terms and conditions of this policy.

5.1.5 Users shall promptly report to their supervisor and their helpdesk all security incidents, disruption of service, actual or suspected theft, loss and/or unauthorized disclosure of IT resources.

5.1.6 The County reserves the rights to audit IT resources to secure its information systems and ensure compliance with this policy.

5.1.7 Limited, reasonable personal use of County network resources, in accordance with this policy, is allowed.

5.1.8 Users should be aware that all usage may be monitored and there is no reasonable expectation of privacy in the use of IT resources. All such personal use must be consistent with conventional standards of ethical conduct.

5.1.9 The County will comply with requests for records under the Freedom of Information Act (FOIA).

5.1.10 Personal Equipment Approval - Users must not connect their personal computers, computer peripherals, phones, or computer software into the County network without prior authorization from EIT. Public WIFI is available for guest Internet connectivity if needed.

5.1.11 Users should not connect personal peripheral devices that provide storage or system-level connectivity (e.g., USB drives, external hard drives, disk drives, or docking stations) to County-owned equipment unless authorized by EIT or their Department IT/liaison.

5.1.12 Custodians for Equipment - The primary User of a personal computer is considered a custodian for the equipment. If the equipment has been damaged, lost, stolen, or is otherwise unavailable for normal business activities, a custodian must promptly inform their helpdesk. With the exception of laptops, tablets, and phones, computer equipment must not be moved or relocated without the knowledge and approval of their department.

5.1.13 Users accessing the Internet with IT resources do so at their own risk. The County is not responsible for material viewed, downloaded, or received by Users through the Internet or email.

5.2 Security and Information

5.2.1 All Users must follow both the Cybersecurity Awareness Training Policy and the AI Usage Policy.

5.2.2 Users may access, use or share IT resources only to the extent necessary to fulfill assigned job duties only in ways consistent with the policies set forth herein. All IT resources must be handled with due care and confidentiality. Users who create, receive, process, edit, store, distribute or destroy IT resources which are confidential, sensitive in nature, and/or governed by federal or state laws, rules or regulations must understand their responsibilities to protect such information.

5.2.3 Users must not establish unauthorized third-party storage solutions (such as Google Drive, Dropbox, or other cloud-based services) to store or manage County information without pre-authorization from EIT or their Department IT/liaison.

5.2.4 All computing devices that-connect to the Lake County internal network must first be pre-authorized.

5.2.5 System and user level passwords must meet EIT's password standards.

5.2.6 Use of another user's password or any other authentication capabilities is strictly prohibited.

5.2.7 User privileges must not be elevated without formal approval.

5.2.8 Technical personnel must utilize accounts specified for elevated privileges to only perform their job functions.

5.2.9 Computing devices must be secured with a password-protected screensaver enabled, as applicable. Users must lock the screen or log off/sign out of the device when the device is unattended.

5.2.10 Users must use caution when opening e-mail or chats received from unknown senders, as attachments may contain malware. Users must also use caution when clicking on hyperlinks in email, as this could result in a successful cyber-attack. When in doubt, Users should report suspicious emails to their helpdesk or the phish report button in Outlook.

5.2.11 Accepting Security Assistance from Outsiders - Users must not accept cybersecurity assistance or use free cybersecurity tools, software, or online services unless the provider has been approved by EIT

5.3 Unacceptable Use

The following activities are prohibited. County Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access if it is disrupting production services). Under no circumstances should any County resource be used to engage in any illegal activity. The examples listed below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

5.3.1 Prohibited System and Network Activities

5.3.1.1 Violations of any copyright, trade secret, patent or other intellectual property, or any similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" or any other software products that are not licensed for use by the County.

5.3.1.2 Unauthorized copying, sharing and/or distribution of copyrighted material.

5.3.1.3 Exporting software, technical information, or encryption technology in violation of export control laws. Consult management before exporting any such materials.

5.3.1.4 Careless introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, malware, and e-mail bombs).

5.3.1.5 Users must not share passwords or allow anyone else to use their accounts. If credentials are lost or compromised, Users must immediately report it to their helpdesk.

5.3.1.6 IT resources must not be used to access, transmit, or distribute any material that violates sexual harassment or hostile workplace laws, including pornography, child exploitation, cyberbullying, or threats of violence. This does not apply if access, transmission or distribution of the materials is within a User’s job duties.

5.3.1.7 Knowingly causing a security breach or network disruption.

5.3.1.8 Port scanning or security scanning is expressly prohibited unless approval is granted from EIT.

5.3.1.9 Conducting network monitoring without the approval from EIT.

5.3.1.10 Circumventing User authentication or security features of any host, network or account.

5.3.1.11 Installing password crackers, denial of service tools, key loggers or any other software or tools designed to acquire unauthorized access to data or IT resources. Use of such tools can be acceptable, but only with express authorization from EIT or their Department IT/liaison.

5.3.1.12 Utilizing tools such as unauthorized browsers to access the ‘dark web’ unless expressly authorized by EIT or their Department IT/liaison.

5.3.1.13 Introducing honeypots, honeynets, or similar technology on the County network unless expressly authorized by EIT or their Department IT/liaison.

5.3.1.14 Interfering with or denying service to any User (for example, a denial-of-service attack).

5.3.1.15 Providing information about, or lists of, County employees to parties outside of established processes.

5.3.1.16 Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation, or which may compromise the security of the County, IT resources, and/or County agencies.

5.3.1.17 Installing software that has not been authorized by EIT or their Department IT/liaison.

5.3.1.18 Unauthorized Software and Data Copies - The County strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet Users or other system Users make unauthorized copies of software, the Users are doing so on their own behalf, since all such copying is strictly forbidden by the County. Likewise, the County allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

5.3.1.19 Using IT resources for non-business online gaming or entertainment streaming/downloading, or installing/using gaming platforms or related software, unless expressly authorized for a business purpose.

5.3.1.20 Prohibition Against All Forms of Adult Content - All forms of adult content and pornography are prohibited on County computers and networks unless required as part of the Users job duties.

5.3.1.21 Using peer-to-peer or file sharing software must be authorized by EIT or their Departmental IT/liaison.

5.3.1.22 Externally supplied USB drives, and other removable storage media should not be used unless authorized or used as part of their normal job duties.

5.3.1.23 Users must not move, modify, or alter security settings on County-owned devices, software, or network equipment without permission from EIT.

5.3.1.24 Sharing or storing IT resources via unauthorized cloud services.

5.3.2 Prohibited Email, Chat and Communication Activities

The purpose of the County's e-mail and chat systems is for correspondence relating to the mission of the County. E-mail and chat is a resource provided to departments, boards and commissions, and Users to enhance work performance and productivity, enable efficient communication, and to record and preserve the work performed in accordance with State law. The following are prohibited activities:

5.3.2.1 Sending "junk mail" or advertising material to individuals who did not specifically request such material (email spam).

5.3.2.2 Any form of harassment via email, telephone, or instant messaging. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.

5.3.2.3 Unauthorized use, or forging, of email header information.

5.3.2.4 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5.3.2.5 Users are prohibited from creating offline archives of their emails (e.g., .PST files) without prior approval from their department.

5.3.2.6 Sending broadcast messages to all County email Users within the scope of the Enterprise Email system without Department Head authorization.

5.3.2.7 Users must never respond to electronic mail messages that request personal or sensitive company information, even from internal sources unless the request is verified through an approved County process or trusted channel and is required for official business.

5.3.2.8 Responding to Offensive Messages - Users must not respond to communications that are abusive, harassing, or threatening. Any message that appears threatening or abusive must be reported promptly to a supervisor, HR, and/or EIT, as appropriate.

5.3.2.9 Users may not create email rules or other automated processes to forward any email to external email accounts: personal or otherwise. This includes carbon copying to personal accounts.

5.3.2.10 Users will not directly or by implication employ a false identity. Identity Misrepresentation - Users must not misrepresent, obscure, suppress, or replace their own or another person's identity on any County electronic communications with exceptions for law enforcement purposes.

5.3.2.11 Users must not intentionally destroy, delete, alter, or conceal County records or data in a way that prevents authorized access or violates County records retention, legal hold, or public records requirements**.**

5.3.2.12 Users must not attempt to access, probe, or bypass security controls to gain unauthorized access to IT resources.

5.3.3 Prohibited Activities When Using Collaboration Tools (Audio, Video, File Sharing, Group Chat, Remote tools and Online Meeting tools):

5.3.3.1 Using collaboration resources for personal profit or for purposes not directly related to County business.

5.3.3.2 Users must not intercept, monitor, or access another person's collaboration account, meetings, messages, or content without authorization, except as required for approved County business duties.

5.3.3.3 Users shall not state directly or imply they are speaking or acting on behalf of the County unless it is part of their official job duties.

5.3.4 Prohibited Blogging and Social Media Activities

5.3.4.1 Nothing in this Policy is intended to restrict lawful, protected activity. County IT resources are provided for official County business and authorized use and are not a public forum."

5.3.4.2 Users must not upload, post, or store County Sensitive Information on publicly accessible internet sites or file-sharing services unless it is required for official County business and is approved by their department head**.**

5.3.4.3 Users are prohibited from making comments or otherwise communicating about customers, residents, vendors, suppliers, coworkers, or supervisors in a manner that is vulgar, obscene, threatening, intimidating, harassing, libelous, or discriminatory on any grounds.

5.3.4.4 Privacy and confidential information requirements also apply to blogging and social media activities. As such, Users are prohibited from revealing any private, confidential or proprietary information, trade secrets or any other material protected from disclosure by applicable statutes, rules, standards, contracts and policies when engaged in blogging and/or social media activities.

5.3.4.5 When using social media in a non-official, or personal capacity:

a. Users who identify themselves as a County employee or have a public- facing position should ensure their profile and related content conforms to applicable requirements, such as (but not limited to) the State Officials and Employees Ethics Act (5 ILCS 430).

b. Users shall not use IT resources to access public forums to discuss any County-related information that is not available to the public. County employees and contractors are expected to exercise professional judgment and restraint when using social media or participating in public forums. Employees and contractors should not discuss, comment on, reference or otherwise engage in online discussions regarding County cases, matters, or proceedings on personal social media accounts, even when such information is publicly available, unless doing so is part of their official job duties and authorized by the User's Department Head.

5.3.4.6 Users must comply with all applicable laws regarding trademarks, logos, intellectual property, rights of publicity, and any other third-party rights. Users may not infringe on County-owned trademarks, logos, intellectual property, or rights of publicity.

5.3.5 Internet Access

5.3.5.1 Internet access is provided to meet informational needs and support the mission and goals of the County. All Internet usage utilizing IT resources falls under this Acceptable Use Policy, regardless of equipment ownership. Misuse of Internet access may result in loss of Internet access privileges, or discipline, up to and including discharge. Internet use may be monitored. Suspected misuse of the Internet should be reported to the User's Department head for review and determination of appropriate action.

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 – n/a

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 **Cloud Services - Internet-based platforms that provide storage, computing, or collaboration tools.**

9.2.1 Authorized Cloud Services: Approved by EIT for business use (e.g., Microsoft 365, SharePoint).

9.2.2 Unauthorized Cloud Services: Any cloud tools not vetted or approved for use with County data.

9.3 **Collaboration Tools** - Digital platforms used for remote communication and teamwork, including video conferencing, screen sharing, instant messaging, and shared document editing. (e.g., Microsoft Online Tools, Microsoft Teams, SharePoint, OneDrive, Zoom, and Webex).

9.4 **Confidential or Sensitive Information** - Any data that must be protected due to legal, regulatory, ethical, or business requirements. This includes, but is not limited to:

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

9.4.2 Internal County information not intended for public release.

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

9.5 **Cybersecurity Tools** - Software, hardware, or online services designed to monitor, detect, prevent, or respond to security threats. Examples include antivirus programs, firewalls, vulnerability scanners, browser security extensions, and password managers. Use of such tools must be approved by EIT.

9.6 **EIT (Enterprise Information Technology)** - The County's official information technology department, responsible for managing and securing County IT systems, data, networks, and digital services. EIT also handles technology approvals and policy enforcement.

9.7 **Elevated Privileges -** Access rights that allow users to make significant changes to systems or data, such as installing software or modifying operating system settings. These are granted only when necessary and must be approved.

9.8 **Equipment -** County-owned computing devices and related hardware assigned to a User or Department (e.g., desktops, laptops, monitors, docking stations, printers, and network-connected peripherals). This does not include minor, short-term shared accessories such as mice, keyboards, or headsets.

9.9 **Helpdesk** - The designated IT support for your department or agency. The Helpdesk is your first point of contact for:

9.9.1 Technical issues or problems with County equipment or software.

9.9.2 Requesting access or reporting problems with passwords or system login.

9.9.3 Reporting incidents, such as suspicious emails, lost or stolen devices, or anything unusual that may affect the security or performance of County IT systems.

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

9.10.1 Computers, laptops, servers, and mobile devices

9.10.2 Software and applications

9.10.3 Email, collaboration, and file-sharing platforms

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

9.11 **Integrity -** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

9.12 **Malware -** Programs intended to damage or disrupt systems, steal data, or gain unauthorized access. Includes viruses, worms, ransomware, spyware, and similar tools.

9.13 **Monitoring -** Any activity in which a user attempts to observe, record, analyze, or intercept network traffic, system activity, user behavior, or communications using software tools, scripts, or system configurations.

9.14 **Personal Use** - The occasional limited use of County IT resources for non-work-related activities permitted under the following conditions:

9.14.1 Occurs during break times or outside of scheduled working hours

9.14.2 Is brief, infrequent, and does not interfere with job responsibilities or County operations

9.14.3 Does not involve accessing inappropriate or restricted content

9.14.4 Complies with all applicable County policies, including those on conduct, ethics, and cybersecurity

9.15 **Privileges -** The access rights, roles, or permissions granted to a User or account that determine what systems, data, and functions the User can access or perform.

9.16 **Security Incident -** Any event that threatens or may threaten the confidentiality, integrity, or availability of County IT resources. Examples include:

9.16.1 A lost or stolen laptop

9.16.2 A suspicious email or file

9.16.3 Unauthorized access to sensitive data

9.17 **Sensitive Information** – See the definition Confidential Sensitive Information above.

9.18 **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	May 10, 2016	16-0418	Replaced the Electronic Communications Policy.
New	Month DD, YYYY	26-0233	Rewritten and replaces the 9.4 Acceptable Use Policy.