10.0 Information Technology

10.1 Information Technology
10.2 Employee Access to Technology Resources and Information
10.3 Appropriate Use of Technology Resources
10.4 Employees' Role in Security
10.5 Privacy
10.6 Retention of Data

Subject **Information Technology**
Board Policy **10.1**
Officer Responsible **CIO**

Policy Statement:

The College shall maintain an Information Technology environment that supports both academic and administrative computing in the following main areas.

- Academic technologies that support classroom and online learning.
- A secured and reliable wired and wireless networking environment that supports voice and data.
- A robust and dependable administrative system to support the business operation related to Human Resources, Financials, and Student System.
- Email and file servers, and other centralized computer system.
- Web and portal services for both external and internal users.

Procedure:

Lincoln Land Community College makes available to the members of the College Community an extensive continuum of technology resources for use in their professional and academic pursuits. The purpose of the IT policy is to safeguard the technological infrastructure of the institution by establishing appropriate use guidelines for all rightful users of technology resources. Ultimately, the primary goal of this policy is to prevent problems before they occur. Access to a wide array of technological resources is accompanied by a responsibility to conduct activities within the parameters of this policy – in an effective, ethical, and lawful manner. Violators of this policy may be subject to disciplinary action in accordance with the College's progressive discipline policy, up to and including discharge.

1. Definitions:
   A. Technology Resources
      This policy frequently refers to "technology resources." At Lincoln Land Community College, this term encompasses many components, including but not limited to:
      - network services (such as individual and shared network storage, Internet access, e-mail, and printing services);
      - web services (such as LLCC web site, portal, and Logger Central);
      - all IT mission critical systems (such as Ellucian, Colleague, and Canvas);
      - telecommunications systems (such as Skype for Business, telephone, cellular phones, smartphones, and voice mail);
      - IT physical equipment including computers and peripherals in all offices, classrooms, and common areas (labs, library, etc.);
      - all supplementary technology devices (such as scanners, digital cameras, video cameras, projectors, document cameras, satellite, and public display systems);

- all IT mobile equipment (such as laptops, tablets, and other personal computing devices);
- all retail software (such as Windows and Microsoft Office 365);
- all specialized academic applications (such as AutoCAD, Adobe Products, etc. as well as access to research databases such as FirstSearch).

Although this list is extensive, it is important to note that it is only representative. It cannot be exhaustive as technology resources at the College are in a constant state of change. The policy applies to all technology resources regardless of whether or not an individual item is included in this list.

B. Information

The term "information" in this policy refers to any data stored or utilized in any technology resource including, but not limited to network storage devices, cloud storage, telecommunication devices including voice mail, e-mail systems, all disk drives, portable storage devices owned by the College, and web pages. "Information" also includes College-owned data (such as student data stored in grade book programs) and business communications that are being stored, utilized or conducted on equipment that is NOT owned by the College. This includes data stored on personally owned equipment such as smart phones, laptops, home computers, personal cloud storage, and portable storage devices.

C. IT

IT or Information Technology refers to the study, design, development, implementation, support, or management of computer-based information systems, particularly software applications and computer hardware. IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and securely retrieve information.

D. User

The term "user" refers to anyone who utilizes any technology resource, including but not limited to students, employees, community members, vendors, contractors, and subcontractors, regardless of the location of the resource, or the location of the user. In other words, a user may be using systems remotely, such as is possible with Canvas or library databases, but will still be required to operate within the parameters of this policy. Users include those who may or may not possess a network or other account, as a user may not be required to have an account to use many technology resources.

E. Access

The term "access" refers to authorized ability to use information or technology resources. Access for each user is unique. It is based upon their "need to know" in order to adequately, effectively, and efficiently perform the tasks of their official position.

F. Systems Administrator

The term "Systems Administrator" generally refers to employees in the Information Technology department in the specific positions of Director, Systems, Network

Administrator or Systems Administrator I, II, and III. Systems Administrators may delegate specific tasks to other employees.

G. Cloud Storage
The term “Cloud Storage” refers to file storage on in which data is stored on remote servers accessed from the internet, or "cloud", such as Microsoft One Drive as part of its Office 365 solution. It is maintained, operated, and managed by a cloud storage service provider.

H. Individual Network Storage
The term “individual network storage” refers to file storage on a network device or in Cloud Storage that is a network service reserved for primary use by one specific employee. They use the assigned storage area for storing files that are not commonly needed by other College employees (shared files). While commonly referred to as “personal files” the information residing here is the property of the College, regardless of its content. Examples of authorized network service technologies supported by LLCC IT that provide individual network storage are Microsoft OneDrive, Microsoft SharePoint/Teams and Microsoft NTFS.

I. Shared Network Storage
The term “shared network storage” refers to a network service that is file storage on a network device or in cloud storage that is reserved for primary use by one department, department unit or other group of users such as a committee. The assigned shared network storage is used for storing commonly needed files by College employees. Examples of authorized network service technologies supported by LLCC IT that provide shared network storage are Microsoft SharePoint/Teams and Microsoft NTFS.

J. Local Storage
The term “local storage” refers to file storage on the computer “local drive”, such as the “C:\” drive. The local storage resides on the client computer. Local storage is not a network service.

K. LLCC Username
A LLCC Username is a unique user ID that is assigned to each employee. When a user utilizes their LLCC Username to log on, they will have access rights to resources on the College network. Collectively, these rights allow users to access enterprise systems (like Colleague and Canvas), e-mail, individual network storage, shared network storage, and other shared resources such as printing, Internet, and intranet access.

L. IT Help Desk
The IT Help Desk is an information and assistance resource that troubleshoots IT problems. It provides the users a central point to receive help. IT Help Desk support is offered via the web at http://it.llcc.edu, e-mail at helpme@llcc.edu or phone at 217-786-2555.

The user notifies the IT Help Desk of any IT related issues via the web, email, or phone and the IT Help Desk issues a ticket that has details of the problem. The ticket is routed to a technician for resolution. Ticket status updates are sent to the user until the ticket is closed.

M. BYOD (Bring Your Own Device)
The practice of allowing users to operate their personally own computers, smartphones, or other devices to access LLCC computer network for work or educational purposes.

2. Information Security Program

To ensure a secured and reliable wired and wireless networking environment LLCC has developed an Information Security Program that provides detailed procedures for implementation of a secure network environment. These procedures follow the Center for Internet Security (CIS) Controls version 8 cybersecurity framework. LLCC strives to ensure the following cyber security controls are addressed in that program:

Inventory and Control of Enterprise Assets (CIS Control 1):
Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Inventory and Control of Software Assets (CIS Control 2):
Actively manage (inventory, track and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Data Protection (CIS Control 3):
Develop processes and technical controls to identify, classify and securely handle, retain, and dispose of data.

Secure Configuration of Enterprise Assets and Software (CIS Control 4):
Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Account Management (CIS Control 5)
Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Access Control Management (CIS Control 6)

Use processes and tools to create, assign, manage and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Continuous Vulnerability Management (CIS Control 7)
Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Audit Log Management (CIS Control 8):
Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Email and Web Browser Protections (CIS Control 9):
Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Malware Defenses (CIS Control 10):
Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Data Recovery (CIS Control 11):
Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Network Infrastructure Management (CIS Control 12):
Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Network Monitoring and Defense (CIS Control 13):
Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Security Awareness and Skills Training (CIS Control 14):
Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Service Provider Management (CIS Control 15):
Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes to ensure these providers are protecting those platforms and data appropriately.

Application Software Security (CIS Control 16):
Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Incident Response Management (CIS Control 17):
Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Penetration Testing (CIS Control 18):
Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

The Lincoln Land Community College Information Security Program can be found on the Information Technology Department Portal.

3. Violation and Enforcement:
Lincoln Land Community College considers any violation of appropriate use guidelines to be a serious offense. Violators of this policy may be subject to disciplinary action in accordance with the College's progressive discipline policy, up to and including discharge.

In addition to College discipline, violators of this policy may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT system.

4. Related Documents:
All documentation, forms, and procedures related to the Security & Appropriate Use Policy may be obtained through the IT department.

5. Policy Maintenance and Development:
This policy document, as well as all appendices, addendums, forms, training documents, procedures, and reference materials are available to all users. Users may access the files via the College website, employee portal, or may request a printed copy from the Information Technology Department or the Human Resources Department.

This policy will be reviewed annually, or as needed, as is determined by the College. Concerns or questions about the policy may be directed to the Chief Information Officer.

Subject **Employee Access to Technology Resources & Information**
Board Policy **10.2**
Officer Responsible **CIO**

Policy Statement:

Many systems at Lincoln Land Community College require unique accounts and passwords. The rules and responsibilities described in this document apply to both the primary account and accounts in ALL other systems.

Procedure:

1. Eligibility for Access

All employees are eligible to receive a LLCC Username, Office 365 account, e-mail address, and storage space on the network in some cases. Accounts that provide access to other systems such as Colleague are either automatically granted based upon the official responsibilities of the employee's position or are assigned based upon the request of the employee's supervisor. Supervisors may submit change requests for an employee's access rights via the IT Help Desk.

2. Use of System Accounts

LLCC Usernames and passwords are non-transferable. A LLCC Username and password are to be used only by the employee to whom they are assigned. Employees are expected to protect and safeguard their password at all times. Allowing another individual to use a LLCC Username or password, either knowingly or negligently, may result in disciplinary action in accordance with the College's progressive discipline policy, up to and including discharge.

3. Position Changes

Access changes resulting from internal employment changes are managed on a case-by-case basis according to the needs of the unique situation. Typically, if an employee moves to a different department, the LLCC Username, e-mail address and phone extension move with them, but all access that was granted to the employee based upon the prior position will be suspended. The supervisor of the new department is responsible for submitting a new request for access to the Chief Information Officer for processing.

4. Disabling Access

Access can be disabled at the discretion of the Systems Administrator, Supervisor, Associate Vice President, Human Resources, or a Cabinet member. Any emergency request to disable an account needs to be submitted to the Associate Vice President, Human Resources. The latter will approve and forward the request to the Chief Information Officer for processing.

Computer system accounts (i.e., access) for terminated employees will be disabled at the time of termination. Human Resources will inform IT of employment terminations as soon as possible.

5. Remote Access

Remote access to local resources in the LLCC network environment shall be authorized and managed on a case-by-case basis based on the official responsibilities of the employee's position at the request of the supervisor. All remote access to the LLCC local network must use a secure, College provided solution.

Subject **Appropriate Use of Technology Resources**
Board Policy **10.3**
Officer Responsible **CIO**

Policy Statement:

Lincoln Land Community College provides information technology resources to support the various activities of the institution. These resources are intended for the sole use of Lincoln Land employees, students, and other authorized users. Information technology users are individually responsible for the appropriate use of technology resources. Individuals should familiarize themselves with the policy components below.

Procedure:

Information technology plays an integral role every day in allowing employees to accomplish their assigned duties. There is an ever-growing array of computing facilities that empower employees to create, access, evaluate, update, distribute, store, and report on information using a variety of media and formats. Lincoln Land Community College provides computing (technology) resources to support the various activities of the institution. These resources are intended for the sole use of Lincoln Land employees, students, and other authorized users. One may assert that an employee at Lincoln Land Community College is severely hindered if he or she lacks access to technology resources. Nevertheless, appropriate use of this access demands individual responsibility.

It is impossible to identify every situation that pertains to proper or improper use of technology resources. The list below focuses on some of the most significant responsibilities a user accepts when he or she agrees to use a College-owned technology resource, as well as general guidelines regarding prohibited activities.

1. General Restrictions
   Use of Technology Resources shall be within the spirit or principles of this policy. No one shall attempt to circumvent or undermine the intent of this policy relating to the use of Technology Resources. Doing so may result in disciplinary action in accordance with the College's progressive discipline policy, up to and including discharge.

2. Other Applicable College Policies
   Many information technology functions parallel familiar activity in other formats, making existing College policies important in determining what use is appropriate. For example, the College Copyright Policy applies not only to hard-copy documents, but to electronic documents as well.

3. Physical Misuse of Resources
   General physical misuse including theft, any unauthorized loan, removal of equipment from campus, damage or destruction is strictly prohibited.

4. Use of Resources and Information For Profit

Using resources for commercial use including, but not limited to, the promotion or day-to-day operation of "for profit" and/or privately owned businesses or commercial ventures is strictly prohibited. This includes any use of College-owned information for solicitation purposes.

5. Software

A. Software procurement

IT is responsible for all software acquisitions. Users who request new software acquisitions must submit the request via the IT Help Desk. All software must be purchased through the IT department. Users must not purchase software directly from the vendor. For more information refer to the Director, IT Services and Support.

B. Software Installation and Licensing

The IT department ensures that the College remains in legal compliance with all software licenses, subscriptions, and contractual agreements, regardless of the budget from which a resource was funded. Consequently, The IT department is responsible for installing and removing all software applications, or authorizing others to do so, for keeping copies of software license agreements, and for ensuring that the College is in compliance with these license agreements. The IT department is responsible for keeping all software media.

C. Software Application Availability

All College PCs are equipped with a set of "standard applications" including, but not limited to programs such as Microsoft Windows, Microsoft Office 365, and standard internet browsers. Software applications on Macintosh computers include Microsoft Office 365 and Safari among others.

Additional applications may be available. IT maintains procedures for requesting all additional applications.

D. Personally Owned Software

Lincoln Land Community College prohibits employees from bringing personally owned software into the workplace. Personally owned software may not be installed on any College-owned computer. Personally owned software is not supported by IT.

E. Internet Downloads

Users are prohibited from loading malware detection applications or utilities that are available via the Internet on LLCC owned computing devices. Often Internet downloads have a negative impact on a workstation. Some impacts are minor while others may jeopardize the functioning of the workstation.

Please note that "shareware" or "trial" applications are not the same as freeware applications and may be loaded with IT's prior consent. Many shareware programs and trial versions have licensing limitations that restrict organizational use and/or the length of trial period usage.

F. Free or For-Pay Internet Services

Use of any Free or For-Pay internet ("cloud") applications or services for any college business needs to be pre-approved by IT.

G. Removal of Software
The IT department retains the right to remove any personally or college owned software.

H. Reproduction of Software
Reproduction or duplication of software on any type of media or through any type of electronic transmission without prior authorization of IT is prohibited.

6. Hardware
A. Hardware Procurement
IT is responsible for all hardware acquisitions. Users who request new hardware acquisition must submit the request via the IT Help Desk. All hardware must be purchased through the IT department. Users must not purchase hardware directly from the vendor. For more information refer to the Director, IT Support.

The hardware standard for desktop computing is Microsoft Windows-based Personal Computers (PCs) for college operation and instruction. Mac or other hardware will be procured for operations and academic programs that required them and where Windows-based PC cannot suffice.

LLCC does not provide support on personally owned hardware; however limited documentation will be provided to assist connecting some personally owned devices considered BYOD (Bring Your Own Device) to LLCC guest wireless network.

B. Installation/Removal of Hardware
The IT department is responsible for acquiring, installing, moving, and removing all hardware devices including but not limited to classrooms, computer labs, and office areas.

C. Installation/Removal of Hardware in Assigned Office Spaces
With the exception of mobile computing devices assigned to the employee by LLCC, employees outside of the IT department may not disconnect or connect any other College or personally owned hardware devices without authorization from IT. Authorization for many peripheral devices such as mice and keyboards can be obtained by submitting an IT Help Desk ticket. A label or other means of identification with the employee's name must be affixed to all personal portable devices.

The IT department retains the right to remove any personally owned equipment.

7. Electronic Communications
The following policy guidelines apply to all forms of electronic communication by College employees when communicating in their official employment capacity. Electronic communication methods include, but are not limited to, phone, voice mail, e-mail, instant messaging, newsgroups, College-owned cell phones, smartphones,

radios, and fax and all other like devices whether or not listed here. Reasonable personal use that does not interfere with the employment responsibilities of the employee and that is in compliance with this Policy and all other policies of the College is acceptable. Except as otherwise excluded by law or collective bargaining language, all devices, files, messages and storage associated with all electronic communication methods are the property of the College, regardless of their content or location. However, Lincoln Land recognizes issues surrounding intellectual property rights, and will make every effort to respect the rights of the individual. In situations where ownership of content is in question, the College will abide by the law and established legal precedent with regard to these issues.

A. Responsibilities

The e-mail system is a primary means by which College information is disseminated. All employees are expected to check their e-mail for distribution of such materials regularly unless off-campus due to an official leave.

B. Restrictions

The etiquette commonly used for traditional written communications should be used as a guideline for use of electronic communication. Every employee should be continually aware that they represent Lincoln Land Community College with every communication they send. Inappropriate communications are prohibited and may result in disciplinary action in accordance with the College's progressive discipline policy, up to and including discharge. Inappropriate use of the College e-mail system includes, but is not limited to, the following:

1) Fraudulent Communications

Any fraudulent communication sent under an assumed name or modified address, or with the intent to obscure the origin, date, or time of the communication is prohibited.

2) Harassing or Discriminatory Communications

Any electronic communication that can be qualified as discrimination or harassment within the definitions provided by the Lincoln Land Community College Discrimination and Harassment Policy is prohibited.

3) Mass Communications

Employees may not knowingly create or send communications to large number of recipients including chain letters, non-collage business related messages, mail bombs, virus hoaxes, and/or other unsolicited mail messages.

4) Copyright

Employee communication may not include any materials, including attachments, which violate the Lincoln Land Community College Copyright Policy or state or federal copyright law.

5) Use in Violation of Policies

College technology resources shall not be used in any manner that is inconsistent with the College's mission or its policies and procedures.

6) Email Forwarding

System based email forwarding is prohibited. This means that users are not allowed to automatically forward their LLCC email to any external email accounts, including personal email accounts or other accounts not owned by the College. Exceptions must be approved in advance by the IT department and must be based on a legitimate business need. Any exceptions must be documented in writing and include a timeline for implementation and justification for the need for email forwarding.

8. Electronic Meetings

This policy is designed to establish guidelines for the recording and usage of meetings within LLCC's Microsoft Teams platform, with a focus on safeguarding privacy, preventing the generation of false information, and addressing potential misuse of AI technology. Meetings shall only be recorded with the explicit consent of all participants. This consent must be obtained at the beginning of the meeting and clearly communicated. Access to recorded meetings should be limited to authorized personnel. Recordings should not be shared with individuals who were not part of the original meeting without the consent of the participants. Recordings should be retained for the minimum period necessary for their intended purpose. A predetermined retention period should be established, and recordings should be deleted after this period has elapsed. Recorded meetings should be stored in a secure and encrypted environment to prevent unauthorized access. The use of AI or any other technology to manipulate the content of recorded meetings for the purpose of generating false information is strictly prohibited. Meeting organizers shall ensure that all recording and storage practices comply with relevant data protection regulations, such as GLBA, FERPA, or local privacy laws.

9. Internet Use

Information available through the computer and network systems, including the Internet, may be distracting, objectionable, or even disturbing. Since computers may be visible or audible to others, sensitivity in viewing and/or listening to such material is required. Computer users who disturb or distract others may be asked to stop their activities or leave the area.

A. Downloads

No one may utilize College-owned resources for the purposes of unauthorized downloading of copyrighted material without consent including but not limited to audio, graphics, video, and publications.

B. Pornography

Users may not use any Lincoln Land Community College owned technology resources for accessing images, sounds, or messages that are pornographic in nature. This does not apply to legal, sexually explicit literary/artistic expressions or materials that are relevant and appropriately related to course subject matter or curriculum.

10. Network Bandwidth Use

Distribution of such material as MP3 music or video files or the use of streaming, audio or video can cause excessive network loading which may cause a significant decrease in network performance for all employees. Therefore, media streaming sites may have restricted bandwidth.

Employees who believe they need to perform these types of actions within the confines of their job responsibilities must contact the IT department for assistance in completing the task in a manner that will not negatively impact other users.

11. Copyright Compliance
    All technology related media files (including, CD, DVD, USB drive, as well as any other electronic media) must comply with the specifications of the established LLCC Copyright Policy.

    A. Duplication of College-Owned Resources Outside of the IT Department
       Reproducing College-owned copyrighted material in any form without proper authorization or not in accordance with the College's copyright regulations (or federal and state laws) is prohibited.

    B. Duplication of Personal Resources
       College equipment and resources (such as media) may not be used for the duplication of personally owned copyrighted material.

    C. TEACH Act
       Employees who wish to take advantage of the allowances provided in the TEACH act to transmit copyrighted materials to online course participants must contact the Information Technology Department for assistance in technologically enforcing the regulations specified in the TEACH Act.

       For more information about the provisions of the TEACH Act, consult with LLCC's Associate Dean, Library.

12. Resource Activity Monitoring
    Lincoln Land Community College reserves the right to monitor its computing resources. The interest of maintaining the integrity of Lincoln Land Community College resources outweighs privacy and confidentiality interests.

    All technology resources available to employees through LLCC are the property of LLCC. LLCC reserves the right to and may monitor any such technology at any time. Therefore, employees do <u>not</u> have a privacy expectation in any technology resource, including e-mail.

13. Ancillary Use
    Limited, reasonable personal (ancillary) use of College resources is permissible but is conducted at the employee's own risk.

Subject **Employees' Role in Security**
Board Policy **10.4**
Officer Responsible **CIO**

Policy Statement:

The information owned by the College is one of its most valuable assets. It is the responsibility of all users to guard against misuse of this asset. Each person granted access to information must comply with the following College data security, confidentially requirements, and applicable laws.

Procedure:

1. LLCC Username and Password
   Employees will construct secure, private passwords. Employees are responsible for protecting their passwords from discovery by others and must immediately change any password that has been compromised.

   A. Sharing of Login Names and Password
   An employee may NOT transfer or share any Login Name or password to any system with any other person – including those who do and do not work for the College, nor should a person use any other employee's Login Name or password.

   B. Security Compromise
   The Systems Administrator has the authority to disable any employee's access and accounts if there is evidence of hacking attempts or reason to believe a password has been compromised.

   If an employee inadvertently encounters a gap in security, he or she must report it to the IT department via the Help Desk immediately. Employees are prohibited from exploiting any such gaps in security.

   C. Failed Password Attempts
   Accounts have security protocols that will temporarily disable an account after several failed login attempts.

   D. Multi-factor Authentication (MFA)
   Employees, students, and 3rd party contractor accounts will use multifactor authentication (MFA) to provide an additional layer of security whenever logging into LLCC systems remotely. MFA works by requiring an additional piece of verification (factor) when accessing your LLCC account from off campus. Current methods of secondary verification are as follows:

   - Microsoft Authenticator app

- SMS text message
- Voice calling
- FIDO2 security key

2. Personally Identifiable Information (PII)
   Per federal regulations (FERPA and GLBA below), Lincoln Land Community College and its employees are required to protect student Personally Identifiable Information (PII) to avoid privacy incidents.

PII refers to any information about an individual maintained by the college, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of privacy incidents include but are not limited to PII left on the printer, PII e-mailed without encryption, PII mailed to the wrong recipient, PII stored on a stolen laptop or thumb drive, PII posted to a public-facing website, PII stored on a personal storage device or web service.

A. Family Educational Rights and Privacy Act (FERPA)
   The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. The law applies to all educational institutions that receive funds under an applicable program of the U.S. Department of Education. Failure to comply with all FERPA regulations has both legal and funding implications for the institution. For FERPA details refer to board policy 5.13 or contact the Vice President, Student Services.

B. Gramm-Leach-Bliley Act (GLBA)
   The Gramm-Leach-Bliley Act (GLBA) was enacted by the Federal Trade Commission (FTC) in 1999 to safeguard the confidentiality of financial information such as names, addresses, phone numbers, bank and credit card account numbers, and Social Security numbers. Because colleges participate in financial activities, the FTC defines colleges as financial institutions. For GLBA details contact the Vice President, Administrative Services.

3. Cybersecurity Awareness and Training Program
   The college offers a cybersecurity awareness and training program to all employees consisting of the following:
   - Providing a cybersecurity site with frequently asked questions (FAQs) on the LLCC Employee Portal
   - Publishing security tips, best practices, and other relevant security information on LincIn employee newsletter once a week during the month of October, and periodically throughout the rest of the year
   - Emailing phishing and other high-impact cybersecurity threat alerts to all employees as needed

- Providing cybersecurity awareness training promoted during the month of October, and required cybersecurity awareness training at intervals throughout the rest of the year

All employees are expected to familiarize themselves with cybersecurity information available on the LLCC Employee Portal.

The cybersecurity awareness and training program is reviewed and updated annually. It assumes employees have no previous cybersecurity knowledge. Cybersecurity refers to the preventative steps and techniques used to safeguard and protect the integrity of a network, programs and data from attack, damage, and/or unauthorized access. There are many different types of security attacks that could potentially affect LLCC and its employees. Some to be aware of include, but are not limited to: Phishing, Ransomware, Malware, Rogue Software, and security attacks via your login credentials.

4. Controlled Use of Administrative Privileges
   IT uses automated tools to inventory all administrative accounts, including domain, O365/Azure, Colleague, and local accounts, to ensure that only authorized individuals have elevated privileges.

   All users with domain level or O365/Azure administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not day-to-day Internet browsing, email, or similar activities. These dedicated accounts use a multi-factor authentication and encrypted channels for all administrative account access.

   Using a log aggregator, systems issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. Systems also issue a log entry and alert on unsuccessful logins to an administrative account.

   Before deploying any servers and network switches, IT Systems changes all default passwords to have values consistent with administrative level accounts.

Subject **Privacy**
Board Policy **10.5**
Officer Responsible **CIO**

Policy Statement:

All information that resides on any Lincoln Land Community College technology resource is the property of Lincoln Land Community College, subordinate to recognized copyrights and legal statutes. Nonetheless, Lincoln Land Community College respects the privacy of the individual. College administrators or employees of Information and Telecommunication Systems do not ordinarily access the files created and stored by others. However, Lincoln Land Community College does reserve the right to do so.

Privacy must be balanced with the requirements of assuring system integrity or enforcing institutional policies. These necessities may result in Systems Administrator access to files with or without consent of the employee. In order to fully understand the scenarios by which this may occur, employees should familiarize themselves with the policy components below.

Procedure:

1. The Electronic Communication Privacy Act of 1994 (ECPA)
   Under the Electronic Communication Privacy Act, electronic communications may be intercepted when at least one of the communicating parties grants consent. Under this policy, the use of a Lincoln Land Community College technology resource grants consent to the College for monitoring all electronic communications.

2. System Maintenance
   Systems Administrators regularly scan volumes of data on network devices for routine maintenance purposes. As a byproduct of maintenance, the Director, Systems, and IT Infrastructure may see the contents of files and e-mail messages.

   The Systems Administrator is required to report any illegal activity that is discovered, or any information that indicates a violation of policy to the Chief Information Officer. If necessary, the report will be reviewed with the Associate Vice President, Human Resources. Policy violations will be pursued in accordance with Policy x.0, Section 2.

3. Access without Consent
   File and computer access without the consent of the employee may occur. The Chief Information Officer and the Associate Vice President, Human Resources will authorize all access that occurs without consent. The Systems Administrator or designee will log all instances of access without consent. An employee will be notified of College access to files without consent. Depending on the circumstances, such notification may occur before, during, or after the access. Situations that result in file or computer access include, but are not limited to the following:

A. Emergency Entry

Emergency entry may be necessary to preserve the system infrastructure, system integrity, and facilities or to preserve public safety. For example, if a virus exists in the network, the Systems Administrator may need to access directory storage assigned to individual employees.

B. Cause

Lincoln Land Community College reserves the right to examine files or computers should it determine cause exists to investigate whether an individual has violated internal policy, state or federal law. When an employee other than a Systems Administrator is more qualified to research a specific violation, the Chief Information Officer and the Associate Vice President, Human Resources, may authorize granting temporary access to another Lincoln Land Community College administrator so that he or she may research the alleged violation.

1) Deleted Files

Deleting a file does not reliably or permanently remove a file from a system. This is true of computer files and voice mail files. The file may reside in an archive or backup storage, potentially indefinitely. If a file is not in storage, it may be accessible by using recovery tools. Files that are retrieved through any of these methods are subject to examination under Section 6.2 of this policy.

2) Archive and Backup Files

Computer files stored in a network folder (individual or shared network storage) and e-mail systems are backed up on a regular basis. Some systems may be configured to create archives with or without the knowledge of the employee. The contents of these files are subject to examination under Section 2 of this policy. Files stored in a local drive are not backed up by IT. The user is responsible for backing up any files stored in the computer local drive.

3) Temporary Access Request

During a period of leave, a supervisor may request temporary access to a specific subordinate's files and/or directories when this access is important to maintaining day-to-day operations, when a high-priority, time-sensitive project requires access, or when necessary to support the overall mission of the College. The Associate Vice President, Human Resources has the discretion to grant or deny such requests.

Upon return from leave, an employee will be notified that temporary access was granted to their supervisor, and the temporary access will be discontinued.

4) File Ownership Transfer

If an employment relationship is terminated, a supervisor may request permanent access to a former subordinate's files and/or directories.

4. Access with Consent

Employees may request that IT grant temporary or permanent access to non-shared files and/or directories to another employee who is collaborating on a project, to an employee who shares the same responsibilities, or to an employee in the same College department. Access to other employees may be granted with the consent of the employee's supervisor. This includes email access and creation of email aliases. The request needs to be submitted via the Help Desk (http://it.llcc.edu).

5. Employment Termination
   When employment is terminated, employees are prohibited from removing any files other than personal files whether related to day-to-day operations of the College, or to special projects to which the employee was assigned, or which were created, copied, or edited as part of duties of the employee's position. Supervisors will have 30 calendar days to request transfer or archival of files and email of the terminated employee. IT may remove terminated employee files and email messages after 30 calendar days of termination.

Subject **Retention of Data**
Board Policy **10.6**
Officer Responsible **CIO**

Policy Statement:

The College will ensure that its institutional data is effectively managed through a data governance structure, and that such efforts support the goals of the College.

The College's document infrastructure will provide the ability to define and enforce document retention and deletion timeframes in accordance with local document retention mandates and College guidelines.

The College will provide a data backup system for mission critical systems as part of its Disaster Recovery and Business Continuity Plan.

Procedure:

1. Data Governance:
   The College will establish and maintain an enterprise data governance program to develop an inclusive data governance culture. A working group, named the Data Oversight Council, will lead the College's data governance program.

   LLCC's enterprise data governance program has four major components: executive sponsorship (the President's Cabinet); data stewards; an oversight group (the Data Oversight Council); and a home in the College's Institutional Research and Effectiveness office.

   A Data Oversight Council will be formed to oversee LLCC's data governance program. The Council will be led by the institution's Chief IR officer and report to the College's CIO and CAO. The Council's authority to operate and make decisions is derived from the President's Cabinet.

2. Email Retention and Deletion:
   Email messages in all mailbox folders and subfolders will be retained for 400 days. Messages older than 400 days will be automatically and permanently deleted.

3. Office 365 Document Retention:
   Messages, documents, and files stored in the rest of the Microsoft 365 ecosystem will be retained for 400 days. No automatic deletion will occur.

4. Retention Labels:
   Retention labels override any automatic deletion policies.
   The following Retention Labels can be used:
   Two-Year Retention
   Three-Year Retention

Five-Year Retention
Seven-Year Retention
Indefinite Retention

It is the user's responsibility to apply and remove retention labels as needed.
Transfer of electronic data, files, or documents to paper media for archival purposes must adhere to local document retention mandates, or to College documentretention guidelines.

All documents relating to impending or ongoing litigation, FOIA discovery requests, constituting records under the Local Records Act, or special projects are to be applied the "Infinite Retention" label.

5. Litigation Hold:
From time to time, the College may be required to institute an "administrative hold". Once a litigation hold is triggered; the College must override any active document deletion policy on the affected location. Relevant documents located on portable devices or stored in local storage or otherwise controlled by users must also be preserved. All users with relevant documents are subject to the preservation obligations of a litigation hold.

6. Instituting Litigation Holds:
Once a litigation hold is instituted, the Systems Administrator, in cooperation with legal counsel and the Associate Vice President, Human Resources or the appropriate Cabinet member, will identify and preserve relevant documents through the following process.

A. Location Identification
The Systems Administrator will identify the potential locations for relevant data.

B. User Identification
Users likely to have documents relevant to the dispute will be identified. Such identification may require use of a questionnaire, survey, or other inquiry. All users are required to respond immediately to any such inquiry.

C. Notice
Once identified, users will receive a litigation hold notice which will:

1. Identify the general subject matter of relevant documents.
2. Identify likely source locations of relevant documents; and
3. Identify steps that must be taken to protect and preserve documents that are in a user's possession or control.

D. Duty to Preserve
The duty to preserve documents and information in hard copy relevant to a legal dispute is an important legal duty for the College and its technology resource users. Failure to comply with this policy and any inquiries or

instructions received in connection with a litigation hold may subject you to discipline, up to and including discharge, pursuant to the College's policies and Collective Bargaining Agreements.

7. Data Backup:

The College performs daily and weekly data backups onsite and offsite of its core computer systems. The College keeps a detailed data backup schedule as part of its Disaster Recovery and Business Continuity Plan.