Policy Title	Original Adoption Date	Policy Number
Information Security	05/12/2015	IT-720
Responsible College Division/Department	**Responsible College Manager Title**	
Information Technology Services	Vice President of Administration	

Policy Statement

I. PURPOSE

This policy defines the actions, controls, and security configurations required to ensure the confidentiality, integrity, and availability of information systems and data at Lakeshore Technical College.

II. STATEMENT

A. Access Control

Information resources shall be protected by the use of access control systems. Access control systems include both internal (i.e. passwords, encryption, etc.) and external (i.e. firewalls, etc.).

Rules for access to resources are based upon the principle of least privilege; employees are granted access only to data or the level of access needed to complete their job duties and only for the length of time required to complete those duties. Access is granted only by the completion of a System Access Request Form (Appendix A). This form can only be initiated by the appropriate hiring manager or department VP/Director. The System Access Request Form is also used when an employee changes positions at the college and requires a different access level.

User Accounts

Employees shall sign out of their user accounts (i.e., log off) at the end of the workday to ensure active application and network sessions are properly terminated and protected from cyber threats.

Upon termination of an employee, whether voluntary or involuntary, HR initiates a process that disables all user account access within (1) business day. In cases where termination is immediate, HR may alert IT verbally to expedite access removal. HR shall be responsible for insuring that LTC-owned IT equipment and property is returned to prior to the employee leaving the college on their final day of employment.

At least annually, the IT System Administrator shall review privileged system access with department managers to ensure that all employees have the appropriate level of access necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate FERPA and HIPAA compliance and protect student, employee, and patient data.

External Entities

At least quarterly, the IT System Administrator shall review third party system access. Access to LTC computer systems or networks for outside contractors/vendors should not be granted until a review of the following concerns have been made and appropriate restrictions are included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the LTC Information Security Policy have been reviewed and considered.
- An LTC Vendor Security Management Checklist has been completed by the party requesting access. The Checklist can be found on the Technology Bridge site.
- Each service, access, account, and/or permission made available should be only the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to LTC computer systems must be maintained and auditable.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding the handling and protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.

B. Audit and Accountability

The IT System Administrator and Network & Security Administrator shall conduct operational reviews of system activity including, but not limited to, user accounts, system access, file access, audit logs and access reports on a daily basis to protect systems and sensitive information. Any suspicious activity shall be brought to the Director of Technology and, if warranted, the Incident Response Plan will be activated.

C. Awareness and Training

All LTC employees shall receive training on LTC's IT security policies, procedures, and best practices.

- Security Training Program
  - Training shall be provided to all new employees through normal onboarding and to all employees on an annual basis.
  - The IT Network & Security Administrator will coordinate with the Organizational Development Center on appropriate training.
- Security Reminders
  - The Director of Technology shall generate and distribute routine security reminders on a regular basis.
  - The Director of Technology and/or IT Network & Security Administrator shall generate and distribute special notices to all staff members providing urgent updates such as new threats, hazards, vulnerabilities and/or countermeasures.

D. Configuration Management

Tracking configuration changes to networks, systems, and workstations allows efficient troubleshooting of IT issues that arise due to an update, new implementation, reconfiguration or other change to its systems.

- IT staff member or other designated LTC employee who is updating, implementing, reconfiguring, or otherwise changing an LTC information system shall carefully log critical

changes made to the system in the designated repository for such documentation.

- The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
- The employee implementing the change shall also be versed with the appropriate rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

E. Incident Response

The Director of Technology shall establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. The Network & Security Administrator shall track, document, and report incidents to the Director of Technology.

F. Maintenance

All members of the Technology Department shall perform regular maintenance, including updates, on organizational systems under their responsibility. They shall document and keep up-to-date their maintenance schedules in the designated repository for such documentation. Any deviation from the maintenance schedules, except for emergent threat situations, shall be pre-approved by the Director of Technology.

G. Physical Protection

Physical access to organizational systems, equipment, and the respective operating environments shall be limited to authorized individuals. The physical facility and support infrastructure for organizational systems shall be protected and monitored.

H. Risk Analysis

The Director of Technology shall develop and implement a risk plan to serve as the basis for LTC's ongoing information security compliance efforts. The plan shall include risk identification, analysis, response, and action plans.

I. Security Assessment

The Technology Department shall:

- At least annually, assess the security controls in organizational systems to determine if the controls are effective in their application.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are

implemented, and the relationships with or connections to other systems.

J. System and Information Integrity

All members of the Technology Department shall:

- Identify, report, and correct system flaws in a timely manner.
- Provide protection from malicious code within organizational systems.
- Monitor system security alerts and advisories and take action in response.

Reason for Policy

This policy is needed to prescribe security safeguards and controls for LTC information systems operating in an increasingly volatile cyber threat landscape. A data breach and/or other major security incident could be extremely damaging to the college's financial resources and reputation and impair its ability to continue business operations. As such, all possible precautions must be implemented to mitigate the risk of such an incident occurring.

Historical Data, Cross References and Legal Review

Legal Counsel Review and Approval: N/A
Board Policy: III.F. Asset Protection

Definitions

Appendix A. System Access Form

The Hire in HIGHER EDUCATION

Lakeshore Technical College
System Access Form (SAF)

WHEREVER AND WHENEVER NEEDED
Will Be A Dealer In HOPE

Note: The SAF is distributed via email to a group of stakeholders after a position is posted. Incomplete forms may delay the process of ensuring the new hire has all the tools and access needed on their first day at LTC.	
Hiring Manager **Department**	**Today's Date**
Position Title	**Employment Category**
Position Type	**Position Number** **(For HR Staff use only)**
Workstation Location **Cubicle ☐ Highwall ☐ Enclosed Office ☐**	**Phone Access** **Extension #**
Computer Needs ☐ Desktop ☐ Not Applicable/Computer is already @ Workstation	☐ Laptop (20% Off Campus Requirement) ☐ Other:
Please Note: IT supplies the computer. Peripheral devices may be requested by submitting a software/hardware request ticket to the Help Desk via email to LTCHelpdesk.gotoltc.edu.	
☐ **Network Drives** Any specific I-Drive requirements/security:	☐ **PeopleSoft Security Level Needed** ☐ **Bridge (Intranet) Security Needed**
☐ **Connection to LTC Network from home (VPN)**	☐ **ImageNow Security Needed** ☐ **OnContact Software Needed** ☐ **Cognos Security Needed**
☐ **Content Manager for the Bridge for your Division/Department**	☐ **Content Manager for the LTC website**
Office/Department Keys	☐ **Purchasing Card (P-Card) Needed**
☐ **Position is responsible for managing a budget** **(specify department number(s))**	☐ **Authorized Signor in Image Now – Financial Services**
☐ **ImageNow: Student Access**	**Cash Handling Responsibilities?** ☐ **Yes** ☐ **No**
Additional Comments **New hire will meet with:** ☐ **Executive Director of HR** ☐ **Benefits & Comp Manager** ☐ **HR Specialist**	