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	Director of Information Technology	

Policy Statement

I. PURPOSE

This policy defines the technical controls and security configurations Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Lakeshore Technical College.

II. STATEMENT

A. Access Control

Information resources are 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 that data or 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 Logon Entitlement Reviews

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 and patient data.

To do this, the System Administrator shall provide a list of all active user accounts for both network and application access, including access to the email system and the SIS/ERP system to department managers for review. Managers shall review the employee access lists within ten (10) business days of receipt. If any of the employees on the list are no longer employed by LTC, the department head will immediately notify IT of the employee's termination status so privileges may be revoked.

Termination of User Logon Account

Upon termination of an employee, whether voluntary or involuntary, HR initiates a process in the ERP system 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 all keys, LTC-owned equipment and property is returned to the College prior to the employee leaving the college on their final day of employment.

Access Control in Third Party Contracts

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 (Appendix B) has been completed by the party requesting access.
- 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.

C. Change Management

Tracking changes to networks, systems and workstations allows IT to efficiently troubleshoot 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 all changes made to the system in the designated repository for such documentation (located on the private IT website on the Bridge (staff intranet)).
- 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.

D. Information System Activity Review

LTC shall conduct, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs and access reports to minimize security violations

- IT shall be responsible for conducting reviews of LTC's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
- Review findings will be compiled in a report that shall include the reviewer's name, date and

time of performance, and significant findings describing events requiring additional action (e.g. additional investigation, employee training and/or discipline, modifications to safeguards).

- Such reviews shall be conducted annually. Audits shall also be conducted if LTC has reason to suspect wrongdoing. In conducting these reviews, IT shall examine audit logs for security-significant events including, but not limited to, the following:
    - Logins- Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
    - File accesses- Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
    - Security Incidents- Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g. viruses, worms), denial of service, or scanning/probing incidents.
    - All significant findings shall be recorded using the report format referred to above.
- IT shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the IT Director for review. The IT Director shall be responsible for maintaining such reports. The IT Director shall consider such reports and recommendations in determining whether to make changes to LTC's administrative, physical and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed promptly by the Information Security Team.

E. Security Awareness and Training

All LTC employees shall receive appropriate training concerning LTC's security policies and procedures. Such training shall be provided on an ongoing basis to all new employees and repeated periodically for all employees.

- Security Training Program
    - The Network Security Administrator and IT Director shall have responsibility for the development and delivery of initial security training. All staff members shall receive such initial training addressing IT security best practices and policies. Attendance and/or participation in such training shall be mandatory for all staff members. The Organizational Development Center shall be responsible for maintaining appropriate documentation of all training activities.
    - The Network Security Administrator and/or IT Director shall have responsibility for the development and delivery of ongoing security training provided to staff members in response to environmental and operational changes impacting the security of LTC's information resources.
- Security Reminders
    - The IT Director shall generate and distribute routine security reminders on a regular basis.
    - The IT Director and/or 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.

F. Risk Analysis

IT shall conduct a thorough risk analysis to serve as the basis for LTC's ongoing information security compliance efforts. IT shall also then re-assess the security risks to its information assets and evaluate the effectiveness of its security measures in light of changes to business practices and technological advancements.

- The IT Director shall be responsible for coordinating LTC's risk analysis and shall identify appropriate persons within the college to assist with the risk analysis.
- The IT Director shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. Such evaluations shall occur at least annually or upon the occurrence of one or more of the following events:
    - changes in the FERPA Security Regulations;
    - new federal, state or local laws or regulations affecting the security of PII;
    - changes in technology, environmental processes or business processes that may affect FERPA Security policies or procedures; the occurrence of a serious security incident.

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

Reviewed/Revised: 05/12/2015
Legal Counsel Review and Approval: N/A
Board Policy:

Definitions

Appendix A. System Access Form (from Staff Recruitment Requisition form)

STEP 3: SYSTEM ACCESS (SA) Note: The SA form 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**
Computer Needs: ☐ Desktop ☐ Laptop (20% Off Campus Requirement) ☐ Not Applicable/Computer is already @ Workstation ☐ Other:	
☐ **Network Drives** Any specific I-Drive requirements/security:	☐ **PeopleSoft Security Level Needed** ☐ **Bridge (Intranet) Security Needed** ☐ **OnContact Software Needed**
☐ **Content Manager for the Bridge for your Division/Department**	☐ **Content Manager for the LTC website**
Office/Department Keys	☐ **Purchasing Card (P-Card) Needed**
	☐ **Authorized Signor in Image Now – Financial Services**
Additional Comments: **New hire will meet with: ☐ Judy ☐ Lisa**	

Appendix B. Vendor Security Management Checklist

VENDOR CONTACT INFORMATION

Vendor Company Name: _____

Primary Business Address: _____

_____

City: _____ State: _____ Zip: _____

Years In Business: _____

Primary Industry Classification: _____

(e.g., ISP/Network, ASP/Hosting, Application Development, Managed Security, Consultancy)

Primary Business Contact Name: _____

Title: _____

Telephone: _____

Email: _____

Primary Security Contact Name: _____

Title: _____

Telephone: _____

Email: _____

TYPES OF SERVICES TO BE PROVIDED TO CLIENT

Identify which services are being offered/provided to LTC by vendor (check all that apply):

☐ Internet Service Provider (ISP) or Other Data Network Services.

☐ Commercial Co-location/Cloud Hosting (Physical, Network, and/or System-Level Only).

☐ Commercial Co-location/Cloud Hosting (P, N, and S – plus Application/ASP-Level).

Date Printed: 5/7/2018

- ☐ Original Application Development.
- ☐ Payment Processing Services.
- ☐ Outsourced Retail Sales/Fulfillment/Service.
- ☐ Outsourced Commercial Business Operations Processing.
- ☐ Outsourced Healthcare-Related Provider, Back-Office, or Insurance Services.
- ☐ Managed Service Services Provider.
- ☐ Business/Marketing Consultancy Services.
- ☐ IT/Technical Consultancy Services.
- ☐ Independent Audit/Compliance Services.
- ☐ Other (include description):

_____

_____

_____

_____