



Policy Title Information Security	Original Adoption Date 05/12/2015	Policy Number IT-720
Responsible College Division/Department Information Technology Services	Responsible College Manager Title Vice President of Administration	
Policy Statement		
<p>I. PURPOSE</p> <p>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.</p> <p>II. STATEMENT</p> <p>A. Access Control</p> <p>Information resources shall be protected by access control systems. 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 available from Human Resources (HR). 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.</p> <p><u>User Accounts</u></p> <p>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.</p> <p>B. Awareness and Training</p> <p>All LTC employees shall receive training on LTC's IT security policies, procedures, and best practices.</p> <p>C. Physical Protection</p> <p>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.</p>		
Reason for Policy		
<p>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.</p>		



Historical Data, Cross References and Legal Review

Created/Adopted: 5/16/16

Reviewed/Revised: 12/17/20

Legal Counsel Review and Approval: N/A

Board Policy: III.F. Asset Protection

Definitions