LCCC Cyber Security Policy

Created: 06/08/2023 Last Revision: 7/17/2023

1. **Introduction**
    a. **Purpose:** This security policy outlines the procedures, controls, and guidelines that employees and contractors of Luzerne County Community College (the College) must follow to ensure the security and confidentiality of our data and information systems and to safeguard the College IT infrastructure against unauthorized access, misuse, and potential threats.
    b. **Scope:** This security policy applies to all information systems, digital assets, and data managed by the College, including but not limited to servers, networks, databases, applications, storage devices, and endpoints.
2. **Roles and Responsibilities**
    a. **Senior Management**: Senior management is responsible for endorsing and supporting this policy, allocating necessary resources, and ensuring its effective implementation throughout the College. All access to information systems must be authorized by senior management and be reviewed periodically to ensure continued need and appropriateness.
    b. **IT Department**: The IT department is responsible for implementing and enforcing security controls, conducting regular security assessments, and maintaining the IT infrastructure's security posture.
    c. **Employees**: All employees must adhere to this policy, report any security incidents or vulnerabilities they discover, and actively participate in security awareness training. Also, refer to the College Information Technology Acceptable Usage Policy – all users (employees and students) must comply with this policy.
3. **Access Control**
    a. **Password policy:** Passwords must be complex and must be changed periodically. Reuse of passwords is prohibited. Multi-factor authentication is implemented for critical systems and privileged accounts. Employees must not share their passwords with anyone, including coworkers or managers. Refer to the College Information Technology Acceptable Usage Policy for more information.
    b. **User Account Management:** User access management is the process of granting or revoking access to information systems based on an individual's job duties or need to know. All access must be granted on a least-privilege basis. Access to sensitive systems and data is restricted to authorized individuals only. User access rights must be reviewed and updated regularly, especially during employee onboarding, transfer, or termination.
    c. **Access Control Policy**: HR sends official email notifications to a designation IT access control email group when an employee is added, changes status, or is terminated. The appropriate division senior manager of each position must request and approve the granting and revoking of access to systems, applications, and data based upon a least-privilege basis.
    d. **Account Termination**: When an employee leaves the College, their access to all College information systems must be terminated immediately with the exception of “Professor

Emeritus" faculty status which allow for indefinite email access per the Faculty Collective Bargaining Agreement terms.

4. **Data Security**
    a. **Data Classification:** Data should be classified based on its sensitivity, and appropriate security controls should be applied accordingly. Access to sensitive data must be restricted to authorized personnel.
    b. **Data Backup and Recovery:** Regular backups of critical data must be performed and tested to ensure data can be restored. Backups should be stored securely and offsite to protect against data loss or destruction.
    c. **Data Privacy:** Personal and sensitive data must be managed in accordance with applicable data protection regulations. Data encryption should be implemented for sensitive data both in transit and at rest.
5. **Network Security**
    a. **Network Perimeter:** Firewalls and intrusion prevention systems (IPS) are deployed to secure the College's network perimeter. Regular security updates and patches must be applied to network devices to address vulnerabilities.
    b. **Network Monitoring:** Network traffic is monitored for anomalies and suspicious activities. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) is utilized to detect and respond to potential network attacks.
    c. **Wireless security policy:** Wireless networks are secured using encryption, such as WPA2 or higher. Default wireless network configurations must be changed, including default passwords and SSIDs.
6. **System and Application Security**
    a. **Operating System Security:** Operating systems must be regularly patched and updated with the latest security patches. Unauthorized software installations are prohibited.
    b. **Application Security:** Applications must undergo rigorous testing before deployment to identify and mitigate potential security vulnerabilities. Web applications should be developed following secure coding practices and undergo regular security assessments.
    c. **Malware Protection:** Anti-malware software should be deployed on all systems and updated regularly. Regular system scans for malware should be conducted, and suspicious files should be quarantined or removed.
7. **Incident Response**
    a. **Incident Response Plan:** Please refer to LCCC Incident Management Plan. The College's incident response team will be responsible for investigating and resolving security incidents. Employees must cooperate with the incident response team and provide any necessary assistance or information. The College has contracted Security Operations Center (SOC) and Security Information and Event Management (SIEM) services (currently Arctic Wolf and Cyber Risk Services) and contracted cyber insurance incident response services (currently CFC Response). The College incident response team will engage these services immediately upon notification of security incidents.
    b. **Incident Reporting:** All security incidents must be reported to the College Information Security Manager, Infrastructure Manager, and the CIO. Please refer to the LCCC Incident Management Plan for details.
8. **Physical Security**

a. **Physical Access Control Policy:** Physical access to College facilities and equipment must be restricted based on an employee's job duties or need to know. Access must be monitored and logged.
b. **Equipment Protection:** Equipment must be protected against theft, damage, or unauthorized access. Laptops, tablets, and mobile phones must be encrypted and password protected.
c. **Equipment Disposal Policy:** All equipment to be disposed of is returned to the IT Department to be wiped and redeployed or destroyed and recycled. All equipment is tracked with LCCC inventory tags, and the IT department manages the asset assignments.

9. **Compliance**
    a. **Legal and Regulatory Compliance:** The College must comply with all relevant laws, regulations, and contractual obligations related to data protection and information security. Regular audits and assessments should be conducted to evaluate policy compliance and identify areas for improvement. Non-compliance with this policy may result in disciplinary actions, including termination of employment or legal consequences.
    b. **Third Party Compliance:** Third-party vendors must comply with the College's security policies and procedures. Vendors must provide evidence of their compliance when requested.
10. **Training and Awareness**
    a. **Security Training Policy:** - Employees must receive security training when they join the College and periodically thereafter, at least twice per academic year. Training must cover data classification, access control, incident response, and physical security. Security awareness training is currently delivered via KnowBe4 training and simulated phishing (with remedial training) campaigns.
    b. **Security Awareness Policy:** Employees must be aware of their role in maintaining the security of the College's data and information systems. The College must promote a culture of security awareness and encourage employees to report any security incidents or concerns.
11. **Conclusion**
    a. **Policy Violations:** Violations of the security policy will not be tolerated and may result in disciplinary action. Employees who suspect policy violations must report them to the security officer.
    b. **Policy Review:** The security policy must be reviewed periodically and updated as necessary to reflect changes in technology, regulations, or business practices. Employees will be notified of any changes to the policy.

Approved by: _____

[Senior Management Representative]

Date: _____

Glossary of Terms:

IDS – Intrusion Detection System – a device or software application that monitors network traffic for suspicious activity or policy violations.

IPS – Intrusion Protection System – a network security tool that continuously monitors a network for malicious activity and takes action to prevent it. Sometimes referred to as an IDPS – Intrusion Detection Prevention System.

SIEM – Security Information and Event Management – technology to support threat detection, compliance and security incident management, and analysis of data sources including log event collection.

SOC – Security Operations Center – team of IT security professionals that protect the College by monitoring, detecting, analyzing, and investigating cyber threats.