PIERPONT
COMMUNITY & TECHNICAL COLLEGE

Pierpont's Information Technology Security Policy is made up of various sub-policies that guide the management of data, computing and password authorization standards. The following are the specific sub-policies involved.

1. Data Security Policy

Pierpont data that is classified as non-public must be protected. This includes any data that is labelled sensitive, protected, or confidential. Non-public information must be secured against disclosure, modification, and access by unauthorized individuals. It must be secured at rest, secured in transit, and securely destroyed when no longer needed.

College Computing Devices containing Non-public Information must be Secured

Any College computing device, including mobile devices, that is used by an authorized user to store, process, or transmit non-public information must be secured in a manner that is consistent with contractual or legal restrictions and is reasonable and appropriate for the level of sensitivity, value, and risk that the information has to the College and its user community, including:

a. Restrict physical and login access to authorized users.
b. Maintain up-to-date software patches and anti-virus software.
c. Enable and use host-based firewalls if available.
d. Perform regular security scans on the computing systems, equipment and networks.

Computing systems, equipment, and networks that contain data elements from multiple classifications must be protected at the highest level of information represented.

Authorized Users are Responsible for Non-public Information in their Custody

Maintaining the confidentiality, integrity, availability, and regulatory compliance of non-public information stored, processed, and/or transmitted at the College is a requirement of all Authorized Users. This maintenance includes:

a. Notify their manager or the appropriate College official if non-public information, passwords or other system access control mechanisms are lost, stolen or disclosed or suspected of being lost, stolen or disclosed.
b. Restrict physical access to laptop and mobile computers when you are physically away from your office or work space. This includes locking the door or using security cables or locking devices.
c. Secure your computers using a screen saver or built-in lock feature when you are physically away from your office or work space.
d. Maintain possession or control of your mobile devices and apply appropriate safeguards to the extent possible to reduce the risk of theft and unauthorized access.
e. Secure computers and mobile devices by requiring passwords.
f. Log out when finished using a system.
g. Use IT-approved secure methods to transmit non-public information. College-provided email services are enabled with security features for securely transmitting emails to other Pierpont email addresses. Information that is sent by e-mail to external or non-College

recipients is not encrypted and therefore at risk.

h. Understand and follow contractual requirements for data security that apply to themselves or data in their custody.
i. Do not store export-controlled data in any cloud-based application.

Security Breaches

Actual or suspected security breaches, or loss of a computing device containing non-public information, must be reported immediately to the Vice President of Information Technology. Incident response procedures will be initiated to identify the suspected breach, remediate the breach, and notify appropriate parties.

2. **Computer Security Policy**

- Users must ensure reasonable physical security for devices issued to them. At a minimum, systems should be in locked rooms when not in regular use or at the end of the working shift. Laptops should be secured through the use of locking cables and similar devices or containment in a locked drawer such that they cannot be easily removed. Lab machines, kiosk machines, and other devices that are in publicly accessible areas shall use physical locks or equivalent systems to prevent theft.
- Users shall not bypass any control that automatically locks their device after a period of inactivity.
- Users must present a valid end user license to IT upon request for any personally-installed software. Users may not replace College-issued software with personally-owned versions of the same software.
- Users may not disable, uninstall, or interfere with software and systems that provide update, backup, encryption, management, or anti-malware services.

Computing systems deployed by IT must conform to the standards listed below:

- Systems must be running an operating system with the latest patches and updates.
- Appropriate Anti-Virus/Anti-Malware must be installed and kept current.
- IT may use management technologies to retrieve system data from and/or push mandatory software deployments to systems.
- All systems are to be configured to use Active Directory for user authentication and management. Users are required to use IT-provided authentication to access any networked resource.
- Systems containing sensitive material will have the appropriate encryption software installed and configured. IT may require encryption on other devices at its discretion.

Systems deviating from this standard will not be supported by Information Technology, and may be isolated from the College’s networking resources at any time without notice.

3. **Password Policy**

For all Pierpont user accounts and systems require a password sufficiently complex to prevent unauthorized access is required. The rules for password complexity are established in the standard hereunder. Different levels of password security, if appropriate, may be created for users and accounts with differing levels of access and authorization, as detailed in the standards, guidelines and procedures derived from this policy.

Password Complexity Requirements

Password requirements for all Pierpont system and user accounts:

- The minimum number of characters that a password must contain is 8.
- Password must contain characters from two of the following four categories:
    1. Lowercase characters a-z (Latin alphabet)
    2. Digits 0-9.
    3. Special characters (!, $, #, %, etc.)
- Passwords must be changed at least every 90 days.