PTC PITTSBURGH TECHNICAL COLLEGE

STAND UP FOR **A HIGHER STANDARD**

INFORMATION SECURITY POLICY

Physical and Electronic Information Controls

Current as of August 4, 2023

TABLE OF CONTENTS

PURPOSE

Pittsburgh Technical College (PTC) is committed to safeguarding its information resources including personal and confidential data through the use of appropriate physical, administrative and technical safeguards. PTC regularly monitors computer systems to detect unauthorized access by external sources. The purpose of the Data Security Policy (DSP) is to outline essential roles and responsibilities, within the PTC community, for creating and maintaining an environment that protects its information resources. This policy addresses the roles and responsibilities of PTC's Data Security Team, Information Systems Security, and Vendor Oversight.

SCOPE

This policy applies to each member of the PTC community, including employees, temporary and contract workers as well as other Authorized Users. This policy covers all information resources collected, stored, or used by or on behalf of any operational unit, department, and person within the community in connection with PTC's operations. This policy applies regardless of whether the authorized user is working in the office, at home or from any other location. Authorized Users accessing information remotely are required to follow the security restrictions specified in this and other PTC related data security and privacy policies.

DEFINITIONS

Confidential information includes sensitive personal and institutional information and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal confidential information may result in a significant invasion of privacy or may expose members of the PTC community to significant financial risk. Unauthorized access or modification to confidential institutional information may result in direct, materially negative impacts on the finances, operations, or reputation of PTC.

Examples of personal confidential information include information protected under privacy laws (including, without limitation, the Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) including the FTC Safeguards Rule, and the Payment Card Industry Data Security Standard (PCI DSS)). Also included is information concerning the pay and benefits of PTC employees, and PII pertaining to members of the PTC community.

Institutional confidential information may include the College's financial and planning information, and legally privileged information.

Internal Use Only information includes data that is less sensitive than confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of PTC. Examples of this type of data from an institutional perspective include internal memos meant for limited circulation, or draft documents subject to internal comment prior to public release.

Public Information is information that is generally available to the public, or that if it were to become available to the public, would have no material adverse effect on individual members of the PTC community or upon the finances, operations, or reputation of the College.

DATA CLASSIFICATION

All information covered by this policy is to be classified among one of three categories according to the level of security required. In descending order of sensitivity, these categories (or "security classifications" are "Confidential", "Internal Use Only," and "Public."

ROLES AND RESPONSIBILITIES

Chief Information Officer

The Chief Information Officer (CIO) has network administration and security expertise and is the authority regarding information management at PTC. The CIO's responsibilities include, but are not limited to the following duties:

1. Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of PTC data. This identification and risk assessment shall include adopting means for detecting security system failures and monitoring the effectiveness of the College's data security program.
2. The CIO shall work with the Data Security Team (DST) and Senior Management Team to investigate any violation of this policy and incident(s) in which the security or integrity of data may have been compromised, including taking the steps set forth in PTC's Data Breach policy.
3. The CIO shall work with the Data Security Team to develop and review training materials to be used for employee awareness under this plan.

Director of Human Resources

The Director of Human Resources is responsible for:

1. Educating incoming employees (including temporary and contract employees) regarding obligations under this plan
2. Ensuring that terminated employees no longer have access to PTC systems and

documentation

Data Security Team

The DST will be chaired by the CIO and include the Director of Financial Aid, Director of Human Resources, Manager of Compliance, and the General Counsel.

1. Monitor federal, state and local legislation concerning privacy and data security.
2. Stay abreast of evolving best practices in data security and privacy in higher education, and assess whether any changes should be made to the Risk Assessment or Data Security Plan.
3. Establish data privacy and security awareness programs for the PTC community and periodically assess whether these programs are effective.
4. Periodically reassess this Data Security Plan and associated policies to determine if amendments are indicated or if modifications should be proposed.
5. Discuss any material violations of this policy and Security Breaches, the College's actions in response, and any corresponding modifications.

Data Custodians

Data Custodians are Directors and/or Managers who are responsible for maintaining data security within their respective departments. Custodians are tasked with assigning a data classification to departmental documents and must determine who is authorized to access departmental data. In addition, Custodians will work with IT to ensure proper access controls are established for staff/faculty.

It is the responsibility of the Data Custodian to make sure all staff/faculty given access to Internal Use Only and Confidential data know and understand the security requirements associated with these classifications.

Authorized Users

Authorized Users are responsible for complying with all security-related procedures pertaining to electronic and physical documentation under their purview, and to which they have authorized access or any information derived from that data. Specifically, a User is responsible for:

- Provide appropriate physical security for IT equipment, storage media, and physical data. Files should not be left unattended without being locked or put away so that others are unable to obtain access to the data or the device(s) storing the data.

- Ensure that Confidential or Internal Use Only information is not distributed or accessible to unauthorized persons. ***Authorized Users must not share their authorization passwords under any circumstances.*** Authorized Users must lock workstations and physically secure printed materials when not in use or when stepping away from the work area.
- To the extent possible, Authorized Users should make sure that electronic information is stored only on secure servers maintained by the College and not on local machines, unsecure servers, or portable devices.
- Data with a Confidential or Internal Use Only classification, when removed from campus or when accessed off-campus, is subject to the same rules as on-campus information.
- When access to information is no longer required by a User, disposing of it in a manner to ensure against unauthorized interception is paramount. Generally, paper-based copies of confidential documents should be disposed of using designated receptacles to ensure the information is shredded and recycled.
- Immediately notifying his or her Manager/Director of any incident that may cause a security breach or violation of this policy.
- Reviewing and practicing procedures detailed in the policies listed in the "See Also" section of this plan.
- Taking the PCI DSS training if authorized to handle credit card transactions.

ASSESSING SECURITY RISKS

PTC conducts annual risk and security assessments. Such assessments will identify internal and external cyber risks. Risk Assessments will inform PTC's data security program and policies. In addition, PTC engages in regular testing and monitoring to protect information resources.

INFORMATION SYSTEMS UPDATES

PTC maintains appropriate and timely updates, patches and maintenance to ensure that systems and data are adequately protected. Critical updates/fixes will be applied as soon as is possible in accordance with institutional approval and sign-off procedures and will include, but not be limited to:

- External application and system hosting will conform to institutional requirements with written exceptions being made as necessary based on the abilities and contractual obligations between the institution and the hosting vendor.
- Operating System (OS) updates for servers, workstations, and other end-user equipment

should be installed in a timely manner in accordance to institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.

- End-user applications regular and critical updates should be installed in a timely manner in accordance with institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.
- Network infrastructure and systems regular and critical updates should be installed in a timely manner in accordance with institutional needs and requirements in order to minimize and avoid unduly exposing the institution to risks.
- All other enterprise information systems and components regular and critical updates should be installed in a timely manner in accordance with institutional needs and requirements, and to minimize and avoid unduly exposing the institution

NETWORK SECURITY

Network attacks launched from the Internet or from College networks can cause significant damage and harm to information resources including the unauthorized disclosure of confidential information. In order to provide defensive measures against these attacks, firewall and network filtering technology must be used in a structured and consistent manner.

PTC maintains appropriate configuration standards and network security controls to safeguard information resources from internal and external network threats. Firewalls and Intrusion Prevention Systems (IPS) are deployed at the campus to prevent denial of service attacks, malicious code, or other traffic that threatens systems within the network.

SECURITY MONITORING

Security Monitoring provides a means to confirm that information resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. Early detection and monitoring can prevent possible attacks or minimize their impact on computer systems.

Any equipment attached to the College’s network is subject to security vulnerability scans. The goal of the scans is to reduce the vulnerability of PTC’s computers and the network to hacking, denial of service, attacks, and/or other security risks from both inside and outside the College. PTC’s IT Department scans internal servers using a mixture of commercial and open source software to monitor and assess the security of the network.

IT also coordinates the vulnerability scans for departments that are required to use this service to meet the Payment Card Industry Data Security Standards (PCI DSS) for credit card processing. Suitably strong encryption measures are employed and implemented, whenever deemed appropriate, for information during transmission and in storage.

Security monitoring also includes video surveillance and card key identification systems controlled and monitored by the Director of Security. The Director will oversee the physical security standards, procedures, and guidelines for the College.

INFORMATION SECURITY INCIDENT RESPONSE

Security incidents are events that violate PTC's security policies, damage or have the potential to damage PTC's systems, information, or public image. An "IT security incident" could:

- Result in the misuse of confidential information (social security number, grades, health records, financial transactions, etc.) of an individual(s).
- Jeopardize the functionality of the college's IT infrastructure.
- Provide unauthorized access to college resources or information.

If an Authorized User suspects that college assets are being misused or are under attack, the Authorized User has an obligation to report the incident to the IT Department in a reasonable amount of time. If you suspect an IT security incident, immediate action should be taken to isolate the problem from the campus network.

1. Call the IT Department, or submit an urgent IT Helpdesk Request.
2. Send an email regarding the incident to the CIO, and Vice President of the Department affected.

The CIO and Senior Vice President of Academic Affairs will notify the U.S. Department of Education and any state regulator as required by applicable law.

VENDOR MANAGEMENT

PTC will conduct a vendor risk assessment before engaging any third-party service provider that will access or process PTC's information resources or IT systems. Third parties that have access to PTC's information resources or IT systems must maintain a comprehensive privacy and data security program and comply with all applicable laws and PTC policies. All third-party service providers will be required to implement appropriate administrative, technical and physical security measures to protect PTC information resources.

COMPLIANCE

PTC will ensure that the plan is being effectively carried out in accordance with regulatory and College requirements and meets or exceeds industry standards for information security.

SEE ALSO

Privacy Policies

- Privacy Policy: https://www.ptcollege.edu/about/consumer-information/privacy-policy
- FERPA: https://www.ptcollege.edu/uploads/pages/documents/consumer/FERPA.pdf
- Student Identity Verification: https://www.ptcollege.edu/uploads/pages/documents/consumer/ferpa-1a-student-identify-verification-policy.pdf
- Protection of Student Privacy: https://www.ptcollege.edu/uploads/pages/documents/consumer/ferpa-1b-protection-of-student-privacy-policy.pdf

Data Security Policies

The following policies are located on PTC's local intranet (Administration tab) for staff and faculty reference:

- Email Retention and Storage Policy
- Identity Theft Program and Red Flags Policy
- Computer Use and Electronic Communications Policy
- Data Breach