INFORMATION SECURITY POLICY

PTC PITTSBURGH TECHNICAL COLLEGE

Revised September 8, 2020

Contents

INFORMATION SECURITY POLICY AND PROCEDURES

Pittsburgh Technical College (PTC) has developed the Information Security Policy (the "Policy") pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, and the Gramm-Leach-Bliley Act (GLBA). The policy was developed with oversight by the Vice President of Financial Services and Chief Information Officer. It is approved by the Finance Committee of the Board of Trustees and adopted by the Board of Trustees.

The college 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 Information Security Policy is to outline how the college manages information systems security, vendor oversight, identity theft prevention, and data breach protocols. Furthermore, it identifies the essential roles and responsibilities within the PTC community for creating and maintaining an environment that protects its information resources.

SCOPE

This policy applies to each member of the PTC community, including employees, temporary and contract workers, as well as other Authorized Users. It 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. The policy applies to all Authorized Users who are working in the office or remotely from another location. Authorized Users accessing PTC information must comply with the security restrictions specified in the policy and other related PTC 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), 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.

Identity Theft means a fraud committed or attempted using the identifying information of another person without authority.

Covered Account means (i) an account that a creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions or (ii) an account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft.

Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Data Acquisition Unencrypted electronic personal information/notice-triggering information will be considered to have been acquired, or reasonably believed to have been acquired, by an unauthorized person in any of the following situations.

Equipment Lost or stolen electronic equipment (including smartphones, laptops, desktop computers, and USB storage devices) containing unencrypted personal information.

Hacking A successful intrusion of computer systems via the network where it is indicated that unencrypted personal information has been downloaded, copied, or otherwise accessed

Unauthorized Data Access Includes situations where someone has received unauthorized access to data, such as sending nonpublic mail/email to the wrong recipient, incorrect computer access settings, inadvertent posting of personal information in electronic format or other non-hacking incidents. Unauthorized data access also includes indications that the Information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Data Owner, The individual with primary responsibility for determining the purpose and function of a record system. Encryption. All encryption algorithms, with the exception of trivial ciphers, meet the minimal campus requirements for encryption. If personal information stored on the compromised electronic equipment is encrypted, no notification is required.

Health Insurance Information An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Medical Information Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

Notice-Triggering Information. Specific items of personal information identified in PA 73 P.S. §§ 2301. This information includes an individual's name in combination with Social Security Number, driver's license/identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Security Breach An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by Pittsburgh Technical College or its auxiliary organizations.

Security Incident A collection of related activities or events which provide evidence that confidential information could have been acquired by an unauthorized person.

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) 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:

4. Educating incoming employees (including temporary and contract employees) regarding obligations under this plan

5. 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 Vice President of Financial Services, Chief of Police, Vice President of Education, the Director of Human Resources, Manager of Compliance, and the General Counsel. The team will -

6. Monitor Federal, State, and local legislation concerning privacy and data security.

7. 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.

8. Establish data privacy and security awareness programs for the PTC community and periodically assess whether these programs are effective.

9. Periodically reassess this Data Security Plan and associated policies to determine if amendments are indicated or if modifications should be proposed.

10. 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 have a need to 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 the following:

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. Immediately notifying his or her Manager/Director of any incident that may cause a security breach or violation of this policy.

17. Reviewing and practicing procedures detailed in the policies listed in the "See Also" section of this plan.

18. Taking the PCI DSS training if authorized to handle credit card transactions.

STAFF TRAINING

An annual employee training program is offered on PCI DSS data security. The training, via Percipio, covers PCI DSS standards, safeguarding cardholder data, and how to spot fraud.

PTC COVERED ACCOUNTS

PTC has identified the following covered accounts:

STUDENTS

Plus Loans – Federal Direct Lending Program, which is mostly bank serviced, and PTC participates; servicing is performed by a U. S. Government-approved agency. Stafford Loans – Federal Direct Lending Program which is mostly bank serviced, and PTC participates; servicing is performed by a U. S. Government-approved agency.

Alternative Private Student Loans are offered by banks and are not guaranteed by any government agency or PTC.

Perkins Loans – Funded by the Federal Government and serviced by PTC – the program is not currently active.

Deferred Tuition Payments – Quarterly and monthly payment plans through Facts Management Corporation.

Emergency Loans – Distributed from a fund maintained by PTC to help students in immediate need.

One-Card Balances – Combined access, services, and debit card held by each student. Processed and managed by an outside service provider. PTC maintains no internal financial account but has control of some of the uses of the card.

Student Accounts – An account is maintained for each student through which all financial transactions, including all financial programs, are recorded.

EMPLOYEES

Computer Loans – Established by the institution to assist full-time and part-time faculty and staff members to obtain a computer and related equipment through a payroll deduction plan.

Emergency Loans – Employees actively employed at PTC for two or more years are eligible to apply for an emergency loan up to $5,000.00. The minimum monthly payment (including interest) must be at least $110.00 per month and paid through payroll deduction.

SERVICE PROVIDER COVERED ACCOUNTS

Student Loan Services – (see above)

1098T Forms prepared by ECSI – PTC must send any student who paid "qualified educational expenses" in the preceding tax year the form 1098-T to complete. Qualified expenses include tuition, fees, and course materials required for enrollment.

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:

19. 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.

20. Operating System (OS) updates for servers, workstations, and other end-user equipment 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.

21. 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.

22. 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.

23. 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 from CISA, a division of Homeland Security. 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.

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.

RISK ASSESSMENT

For the student-related PTC administered covered accounts, the existing risk is that a fraudulent request is made for a draw on an overpaid account resulting from a loan and/or direct payment. Since PTC is solely responsible for issuing draws on these accounts, the risk resides at the financial aid personnel level.

There is no perceived risk associated with employee computer loan programs. At no point in the computer, the loan process is there a position where funds are owed to the employee. However, if a case did exist where an employee was owed funds due to an "over-withholding," the funds would be returned to the employee through the standard payroll process. This process maintains its own control structure to ensure proper payment to employees.

There is risk in the activity of service providers if not conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

However, the processes transacted by these providers represent funds owed to PTC, mitigating the risk of theft to the account holders. Additionally, PTC will take steps to review the Red Flag policies and procedures enacted by these providers.

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.

IDENTITY THEFT PREVENTION

The policy includes measures to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of this policy. Procedures include:

24. Identify relevant red flags for covered accounts it offers or maintains and incorporates those red flags into the policy;

25. Detect red flags that have been incorporated into the policy

26. Respond appropriately to any red flag that has been detected to prevent and mitigate identity theft; and

27. Ensure the policy is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the creditor from identity theft.

The policy shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

CONTROL PROCEDURES

The primary risk associated with covered accounts relates to refunds on student accounts and loan accounts. The following control procedures mitigate this risk:

All refunds on student accounts (including one-card balances) that are in an overpaid position must be initiated by the student owning the account. The request may be initiated either in person or in writing from the student's PTC email account. Phone requests will not be honored due to the difficulty in assessing the individual's identity.

Requests made in person must be made at the Student Financial Aid Office during standard operating hours. The student must present his/her valid PTC photo identification.

Checks are mailed to the official name and address within the system or may be picked up in person. The student must once again provide his/her valid PTC

photo identification when receiving the check-in person. A student may request a specific payee or address that is different from the system data; however, this must be requested in writing and submitted either in person, with valid PTC photo identification, or directly from the student's PTC email account.

Students must make any permanent name or address change with the Registrar. A change in name requires the appropriate legal document subject to the specific instance, such as a marriage certificate. These changes require the student to visit the Registrar in person and present his/her valid PTC photo identification. A change in address may be requested either through the student's PTC email account or in person. If requested in person, the student must show his/her valid PTC photo identification.

A change in name or address for an alumnus with loan balances must be made through the Registrar. Each alumnus must provide his/her requests in writing and identify his/her student identification number for verification.

RED FLAGS

The following red flags are potential indicators of fraud. Any time a red flag or a situation closely resembling a red flag is apparent, it should be investigated.

28. Documents provided for identification appear to have been altered or forged;

29. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;

30. A request to mail something to an address not listed on file; and

31. Notice from students, parents, PTC personnel, and victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

RESPONSE TO RED FLAGS

The policy provides appropriate responses to detect red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

32. Deny access to the covered account until other Information is available to eliminate the Red Flag. Contact the student or

employee:

33. Change any passwords, security codes or other security devices that permit access to a covered account;

34. Notify law enforcement; or

35. Determine no response is warranted under the particular circumstances.

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:

36. Result in the misuse of confidential information (social security number, grades, health records, financial transactions, etc.) of an individual(s).

37. Jeopardize the functionality of the college's IT infrastructure.

38. 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 is obligated 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.

39. Call the IT Department, or submit an urgent IT Helpdesk Request.

40. Send an email regarding the incident to the CIO and Vice President of the Department affected.

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

SECURITY INCIDENT REPORTING

In the event that a staff or faculty member or Information Technology representative identifies a potential security incident involving a computer/unit, the computer/unit shall first be disconnected from the network, then shutdown. In all instances, the computer/unit in question will await further instructions from Information Technology prior to the continued operation of the computer/unit.

Any employee or IT staff member who believes that a security incident has occurred shall immediately notify the CIO.

Upon notification by an employee, or Information Technology staff member, of a suspected unauthorized acquisition of confidential information, the CIO shall promptly notify the President of the College and the DST members.

SECURITY INCIDENT INVESTIGATION

The CIO and/or the Network Administrator will investigate the security incident to determine whether there has been a security breach. All investigatory work will be documented within a confidential Security Incident Report by the Information Technology department.

LOW/NO RISK INCIDENT

A Low/No Risk incident typically occurs but is not limited to, an instance when a User or College staff or faculty member will observe a problem with a computer/unit. The computer/unit may have been compromised due to a form of malware installed on the compute/unit:

41. Information Technology staff will notify CIO.

42. College Information Technology staff will consult the Network Administrator to determine the level of risk with the incident.

43. If it is determined, the incident is a "High Risk" follow the corresponding procedure.

44. If it is determined the incident is considered "Low/No Risk," the Information Technology staff will work with the User or appropriate Department Director to complete a report, if deemed necessary by the CIO.

HIGH RISK INCIDENT

45. A High-Risk incident typically occurs but is not limited to, an instance when Network Services notices an alert or spike in network activity. The computer/unit may have been compromised due to remote program execution, unusual data traffic, RTP services, etc.

College Information Technology staff will notify CIO.

46. The affected computer/unit will be temporarily transferred to IT

custody for forensic analysis.

47. Information Technology staff will conduct an incident investigation, which may include:

48. A follow-up interview with the User.

49. A follow-up interview with College staff or faculty.

50. A follow-up interview with the appropriate administrator.

Upon completion of forensic analysis and interviews, the Information Technology Staff member, the CIO, the Network Administrator, and appropriate College administrators will meet to review all evidence and determine if there was a security breach.

51. If there was no breach, College Information Technology staff would work with the User and appropriate Administrator to complete a review of all security protocols, if deemed necessary by the appropriate College administrators.

52. If there is a breach, follow the steps outlined in Part II: Security Breach Notification Protocol

Upon completion of the investigation, the CIO will inform the President of the College and/or Vice President of Information Technology.

SECURITY BREACH NOTIFICATION PROTOCOL

INTERNAL If it is determined after an investigation that a security breach involving notice triggering Information has occurred, the CIO shall notify the President of the College, DST team members, and Office of General Counsel.

If it is determined that a breach is of the appropriate magnitude and may require a press release, the Vice President of Information Technology shall notify the President of the College, Director of Public Relations, as well as the Chief of Police.

The CIO will notify the responsible department, confirming the security breach of notice triggering Information, and provide advice and guidance. The CIO shall work jointly with the police department for controlling access to, and security of, the breached electronic equipment to ensure the appropriate handling of the breach response and inquiries. The CIO or the Network Administrator will provide guidance to designated employees responsible for responding to breach notification inquiries.

EXTERNAL If it is determined after an investigation that a security breach involving credit/debit card information has occurred, the Chief Financial Officer will direct notification to the appropriate merchant bank(s). Within three (3) business days of a confirmed breach, the CIO shall provide an Incident Report to the appropriate merchant bank(s). Within ten (10) business days, the Chief Financial Officer shall provide to the appropriate merchant bank(s) a list of all potentially compromised accounts.

NOTIFICATION OF AFFECTED INDIVIDUALS

The Information Technology Department shall compile the list of the names of persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A list of individuals to notify shall be compiled based on the following criteria:

- Residents of Pennsylvania.
- Residents of other states which have specific breach notification requirements as advised by General Counsel
- All individuals who are likely to have been affected, such as all whose Information had been stored in the files involved, when the identification of specific individuals cannot be made.

If required, the CIO or CFO shall notify the following consumer credit reporting agencies:

- Experian
- Equifax
- TransUnion

The process for identifying affected individuals as part of notification shall be included in the confidential Information Security Incident Report.

TIMING OF NOTIFICATION

Individuals whose notice-triggering Information has been compromised shall be notified in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The Information considered when determining the notification date shall be included within the Confidential Information Security Incident Report.

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 comprehensive privacy and data security policy 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.

UPDATING THE POLICY

This policy will be periodically reviewed and updated to reflect changes in risks to students and employees and the soundness of PTC from identity theft related to the noted covered accounts. At least once per fiscal year, the Senior Vice President Financial Affairs and Information Technology and Vice President of Academic Affairs will consider PTC's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts that PTC maintains and changes in PTC's business arrangements with other entities, as they relate to this policy.

After considering these factors, the Senior Vice President Financial Affairs and Information Technology and Senior Vice President of Academic Affairs will determine whether changes to the policy, including the listing of red flags, are warranted. If warranted, the policy will be updated.

SEE ALSO

DATA SECURITY AND PRIVACY POLICIES

- Student Handbook (FERPA)
- Protection of Student Privacy
- Customer Payment Card Data Policy

- Email Retention and Storage Policy
- Computer Use and Electronic Communications Policy