Kutztown University COMPREHENSIVE INFORMATION SECURITY PROGRAM

Comprehensive Information Security Program Overview

- This document provides a condensed summary of the essential information security guidelines and approaches for Kutztown University employee use.
- The purpose of the comprehensive security program is to educate employees to lessen overall data security risks for Kutztown University.

KU Regulatory Compliance – Employee Responsibilities

- **All Kutztown University employees need to comply with Federal or Industry regulations regarding the way we use, store, and transmit confidential information/data, such as:**
  - PCI-DSS – Payment Card Industry Data Security Standards
    - Protection of Confidential Credit Card Information
  - FERPA – Family Educational Rights and Privacy Act
    - Protection of Confidential Student Record Information
  - HIPAA – Health Insurance Portability and Accountability Act
    - Protection of Confidential Student/Employee Medical Information

PASSHE Data Classification Guidelines

- Data are classified into three categories
  - "Confidential"
  - "Sensitive"
  - "Public"

Confidential Data

- Confidential data is personally identifiable information requiring the highest level of protection.
- Confidential data includes data that the State System of Higher Education must keep private under federal, state, or local laws and regulations, or based on its proprietary nature.

Confidential Data Categories – Confidential Data is "Personally Identifiable Information"

- Credit Card Information
- Social Security Numbers
- Driver's License Numbers
- Student Records
- Medical Records
- Personnel and Payroll Records
- Date of Birth
- Disability Records
- Personal Finance Information
- Privileged Legal Information
- Passwords

Confidential Data – Employee Responsibilities

- It is appropriate for employees to access confidential information for their required work use.
- Confidential data should always be deleted immediately, if in electronic format, or shredded, if printed or handwritten upon completion of work.
- Confidential Data, including credit card, social security or driver's license information, should never be stored on a Server, PC, Laptop, or Mobile Device such as an iPad, or Smartphone.
- Confidential Data should never be stored on a removable USB, CD or DVD device.

- Confidential Data fields should be cleansed from data reports whenever possible.
- Never publish Confidential Data on a public web server.
- Be careful to whom you provide confidential information.
    - Verify whether the individual has a legitimate university business need to view the information.
- Employees should always lock their office and password protect their Windows PC, Mac or Mobile Device, even when leaving for a few minutes.

Sensitive Data

- Sensitive data are information private to PASSHE and Kutztown University.
- Access is limited to PASSHE community members on a need-to-know basis and the data is not generally available to external parties.
- The unauthorized disclosure of Sensitive Data is not a violation of law, and does not impair Kutztown University business or result in a financial loss.
- However, disclosure of Sensitive Data may be damaging to our students, employees, or alumnae or to the university's reputation.

Examples of Sensitive Data:

- Donors' names and contributions
- University Partner or Sponsor Information, where no more restrictive confidentiality agreement exists
- Employee names and salaries
- Detailed building plans for buildings that contain secure locations, and data network maps
- Certain Research Records
- Library and archive circulation and order transactions

Sensitive Data – Employee Responsibilities

- Secure the sensitive information to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
- Store the information in a controlled environment (i.e. file cabinet or office where physical controls are in place to prevent disclosure) when not in use.
- Avoid posting the information on a public website unless prior approval is given by the Office of Legal Counsel.
- Destroy the information when no longer needed.

Public Data

- Public Data have no legal or other restrictions on access or usage and may be open to the university community and the general public.

Examples of Public Data:

- Kutztown University's public website: "www.kutztown.edu"
- The Pennsylvania State System of Higher Education public website: "www.passhe.edu"
- Approved official meeting minutes
- Official policies and documents
- Publicly-posted press releases
- Publicly-posted schedules of classes or course catalog
- Publicly-posted interactive maps, newsletters, newspapers, job announcements, and magazines

Data Breach Definition

- Data breaches include:
- When PASSHE or Kutztown University confidential or sensitive data is lost or stolen
    - Including confidential data access by an unauthorized individual
- When an Information Technology Device is lost or stolen
    - IT devices include desktop computers, laptop computers, mobile devices such as iPads or SmartPhones, and removable storage devices (USB or CD)

Breach Notification - Employee Responsibilities

- Immediately report a suspected data breach to your supervisor and to Kutztown University Information Technology Services (IT).
- Immediately report lost or stolen IT devices to your supervisor and Kutztown University Information Technology Services (IT).

Password Security – Employee Reponsibilities

- All Kutztown University employees should always use strong, cryptic, complex passwords to protect their information.
- Strong passwords are very difficult for another individual to decipher or guess.

PASSHE Password Guidelines

- Passwords must be at least 8 characters in length
- Password must contain 3 out of 4 of the following
    - Contain uppercase characters (e.g. A-Z)
    - Contain lowercase alphabetic characters (e.g. a-z)
    - Have at least one numerical character (e.g. 0-9)
    - Have at least one special character (e.g. ~!@#$%^&*()_-+=)
- Unique: Password must be different than the previous 3 passwords
- A Strong Password **must not**
    - Spell a word or series of words that can be found in a standard dictionary (ChevyCorvette1)
    - Spell a word with a number added to the beginning and the end (Kutztown1)
    - Be based on any personal information such as user id, family name, pet, birthday, etc.

Kutztown University Acceptable Use Policy

- Kutztown University provides computer resources to students, faculty, and staff for academic and business purposes. This document describes the college's standards and policies for the acceptable use of these resources.
  http://www.kutztown.edu/admin/AdminServ/policy/pdfs/ACA-069.pdf

Kutztown University Email Usage Guidelines

Email Usage – Employee Responsibilities

- Employees should protect individual account names and passwords, correspondences, and, in general, the university email system from unauthorized use.

Prohibited Email Activities per the Kutztown University Acceptable Use Policy

- Providing false or misleading information to obtain a university computing account
- Hiding or disguising one's identity to avoid responsibility for behavior in the use of information technologies
- Unauthorized use of another user's account
- Use of the university information technology resources to transmit abusive,

threatening, or harassing material, chain letters, spam, or other communications prohibited by state or federal law
- Copyright infringement, including illegal file sharing of video, audio, software or data
- Excessive or prohibited personal use by employees
    - Incidental and occasional personal use (that is, non-job-related use) of information technology resources by employees is allowed as long as it does not interfere with the user's productivity and performance or that of any other employee and as long as it does not adversely affect the efficient operation of the resources involved.
- Use of the university information technology resources for personal profit, commercial reasons, non-university fundraising, political campaigns or any illegal purpose
- The prohibition against using university information technology resources for personal profit does not apply to:
    - Scholarly activities, including the writing of textbooks or preparation of other teaching material by faculty members; or
    - Other activities that relate to the faculty member's professional development
    - Other activities as approved by the University President

Scam "Phishing" Email Scheme Characteristics

- Fictitious representation of an individual or an organization, such as a university department or a public company
- The email messages often requests personal information
- The email messages often request that you click on an unfamiliar web link
- Or, they requests your password
    - Kutztown Information Technology Services or Microsoft Corporation will never request your confidential password.

Safe Emailing Guidelines

- Never open, or reply to suspicious emails; delete them immediately.
- Never open email attachments unless you are sure what they are and who they are from.

Mobile Device Types

- Mobile Devices include Laptop Computers, and Tablet devices such as iPads, and SmartPhones.

Mobile Device Guidelines

- Confidential data should never be stored on a Laptop or Mobile Device.
- Keep Mobile Devices with you at all times (never leave them unattended in public places).
- Lock your office and password protect your mobile device, even when leaving for a few minutes.

Remote Access Guidelines (Guidelines for accessing KU systems from home or when traveling)

- It is the employee's responsibility to ensure the same level of security for University data and intellectual property remotely as if working on campus.
- Never share account names and passwords with anyone, not even family members.
- Confidential or sensitive information should not be shared with anyone who is not an authorized university employee.

- Never download or store KU confidential data on your home desktop computer, laptop computer or mobile device (iPad, SmartPhone, etc.) .
- Keep antivirus software current on your home desktop or laptop computer.
    - Activate automatic updating of anti-virus definitions
- Keep Microsoft/Apple patches and security updates current for your home desktop or laptop unit.
    - Activate Microsoft or Apple automatic software updating
- "Public" devices (e.g. computers, laptops and iPads provided by libraries, universities, coffee shops, hotel business centers, etc.) should not be used to access confidential PASSHE data.
- Recommended best practice: Protect the home broadband network with a home "router", rather than connecting your computer directly to the Internet.
- Recommended best practice: Always password protect your home network.

Kutztown University Wireless Network Guidelines

- Kutztown University provides wireless data network access in many locations on campus.
- Only wireless access points provided by the university are permitted on the academic campus wireless network.
- Network Interface Cards (NICs) installed on personal computers should not be configured as wireless access points.
- KU does not currently require all wireless communications to be encrypted, however recommends the use of secure websites, using SSH or HTTPS encryption for secure information transmission.