PennState
New Kensington

University Institutional Data and Personally Identifiable Information

Procedure Number: PSU-NK-ITS-014
Date: September 28, 2017
Page Count: 10

Purpose:

To formally outline the campus's actions to ensure the appropriate use, confidentiality, integrity, availability, and security of University Institutional Data and Personally Identifiable Information (PII), to assure PII is used in compliance with University policy and, when used inappropriately or compromised, outline the steps taken to remediate the loss of PII at the campus.

Scope:

This procedure applies to any device which stores, contains, or uses institutional data or Personally Identifiable Information (PII).

Definitions:

Account - the means by which an individual establishes access to a specific University Computer and Network Resource. The term "Account" also is often used to apply to the file space or services reserved for that individual on the specific resource. Accounts are a privilege, and access to an account can be revoked if just cause is found by the University unit responsible for the computer resources, or by order of the Office of Information Security (OIS) in order to protect the overall security of the University's Computer and Network Resources

Computer and Network Resources - all computers, computer systems, other information systems (e.g., interactive video or voice networks), telecommunications equipment (e.g., routers, switches) or devices that are owned by the University or that connect to University network assets. Computer and Network Resources also include all institutional data, user data, programs or system software, or configuration files, which are contained in or transmitted via University computers, networks or other information systems. This definition is not intended to inhibit access to information services that University employees and students have made accessible for public inquiry (e.g., WWW or anonymous ftp).

However, use of such services to access or attempt to access information not intended for public display or use, or to circumvent or violate the responsibilities of system users, system administrators or information associates in Policies AD95 and AD96 is prohibited. System users are solely responsible for ensuring the content of files, programs or services that they operate, maintain, store or disseminate using University Computer and Network Resources (to include personally-owned computers connected to such resources) are compliant with both law and University Policy. The system user is responsible for all content that they place on devices that content to the Penn State New Kensington Data Network as well as following all University Policies related to Institutional Data. The University reserves the right to suspend network access or computer account(s), or to impose other sanctions as defined in Policies AD95 and AD96 if such user-maintained files, programs or services are believed to have been operating in violation of either law or Policy.

Computerized Institutional Data - Institutional Data that is captured, stored, maintained, accessed or used by a computer system. (See also Institutional Data.)

Device – A computer, electronic tool or communication apparatus with the ability to connect to a data or communication network.

Institutional Data - information that is necessary to the management and operation of Penn State. This information is a University asset, owned by the University and intended to be used solely for the operation of the University in carrying out its mission. (See also Computerized Institutional Data.)

New Kensington Data Network – The technology infrastructure, hardware, and software installed at the campus which is used to facilitate the flow of digital information between (but not limited to) computers, printers, servers, mobile devices, the Internet, etc. This includes both the wired and wireless networks at Penn State New Kensington.

NK ITS Department - the campus Information Technology staff consisting of the System Administrator, IT Specialist and the Director of IT

Personally Identifiable Information (PII) – Includes the following but not limited to, Social Security Numbers (SSNs), credit card numbers, Driver's License numbers, passport numbers, Personally Identifiable Health Information (PHI), salary and tax information related to individuals, details of University budgets, tenure or promotion information, staff employee review information, password or other system access control information, human subject information, admission and financial aid information and donor information.

Sanitization of Institutional Data - The removal and permanent destruction of all data physically present on any computer media device e.g. hard drive, flash drive, floppy disk, CD/DVD, etc.

System Administrator - an employee of the University whose responsibilities include system, site, or network administration. System administrators perform functions including, but not limited to; installing

hardware and software, managing a computer or network, ensuring appropriate security is in place, and keeping a computer or network operational.

System User - any individual who uses University Computer and Network Resources.

Procedure:

University Institutional Data

1. All University institutional data stored electronically or via off-line means, such as paper, must be secured both physically and via access controls to assure appropriate access rights. This includes locking campus office doors and filing cabinets, ensuring University computers are secure at all times, and passwords are changed on a regular basis and meet complexity requirements.
2. This applies to all PII and institutional data not otherwise defined by a specific portion of this policy. Refer to University policies AD95 (http://guru.psu.edu/policies/AD95.html) & AD96 (http://guru.psu.edu/policies/AD96.html) regarding the appropriate use, distribution, and responsibilities of deans and administrative officers, system users, and system administrators in the use and protection of institutional data and network resources.
3. All University employees should consider institutional data confidential and err on the side of caution when asked to distribute or provide institutional data. Questions regarding the distribution of University Institutional Data should be directed to Jason Bush, the campus Access and Security Representative.

Remediation of PII

In an attempt to eradicate archived or unnecessary PII from University-owned computers, the NK ITS department has installed software which searches all electronic data on a computer hard drive for PII. The scan tool runs automatically each week and prompts the user to remediate the PII after the scan completes. Individuals that have been assigned University computing assets are responsible for ensuring that PII is remediated from their device within two days from which the scan occurred. The NK ITS Department is responsible for ensuring that all multi-user computing assets (computer labs) and servers are PII free.

The NK ITS Department will audit the centrally-stored PII scan reports on a quarterly basis to ensure that all University-owned computer assets at Penn State New Kensington are PII free. If a computer is found to have positive results of PII, the system user, and their supervisor, will be sent a notification (Appendix A) regarding their non-compliance with University and campus policy. The system user will be required to remediate the system utilizing the PII scanning client within 2 days of receiving notification of the

violation. If a system user does not comply with the remediation request, the computer access account will be locked.

All University high-risk computers must be scanned for PII. The computer access account of system users and system administrators that do not comply with this policy will be locked.

Compromised device that contains Personally Identifiable Information (PII)

Desktop, Laptop, or Server

1. If a computer system is found to be compromised by a virus or malware program, the device must be removed from the New Kensington data network immediately and the following actions taken:
2. The ITS department is required to take custody of the machine immediately. Removal of data from the device once it is found to be compromised is prohibited.
3. The ITS department will create an incident report with the Office of Information Security (OIS).
4. The ITS department will work with the Office of Information Security (OIS) to determine if recent PII scan data exists. If no recent PII scan data exists, a PII scan will be run and the data will be provided to the Office of Information Security (OIS) for review and recommended action.
5. If the computer contains PII, the system user will be issued a temporary computer for use while an investigation of the compromised computer begins. The case will be referred to the University Privacy Office and the Office of Information Security (OIS) for review and recommended action.
6. If the device or server is found to contain PII and is Internet facing (web server), the system must be disconnected from the New Kensington data network until all PII is remediated and a subsequent scan confirms the device is free of all PII. The case will be referred to the University Privacy Office and the Office of Information Security (OIS) for review and recommended action.
7. If the computer is PII free, the system will be restored to a non-compromised state and the user's files will be restored from their backup copy prior to returning the computer to the user.

Notification of Compromised PII

1. In cases where a computer is compromised and contains PII, the privacy office will advise NKITS to notify all affected persons of the compromise as required by the Pennsylvania State Breach Notification Law. The specific campus unit and/or department are financially responsible for all costs associated with a compromised-PII incident.
2. Incidents of this nature are confidential and should not be discussed outside of the personnel involved in investigating and remediating the incident.
3. If a system user or system administrator is involved in an incident of this nature, the user will receive notification (Appendix B) regarding their non-compliance with University and campus policy. The user will be expected to take an active role in the remediation process, accept sanctions as assigned by the campus administration, and attend a training program regarding the appropriate use of institutional data and PII.

PennState
New Kensington

Sanitization of Institutional Data and Proper Disposition of Computer Assets

When an individual who has a University assigned computer asset leaves the University, the necessary steps must be taken to sanitize all institutional data that resides on the computer asset before it is reassigned to another individual. When the computer asset is outdated or not in good enough condition to be reissued, the asset must be disposed of properly. The following procedures document the proper processes for sanitization of institutional data and the proper disposition of computer assets.

Reusing a University Asset when an Employee Departs Penn State New Kensington

When an employee leaves the University under any circumstance and the asset is to be reused by another individual, actions need to be taken to assure the complete destruction of University Institutional data and PII on their machine.

1. Penn State New Kensington Human Resources will notify the NK ITS Department as soon as they are aware of an employee's departure date from the University.
2. NK ITS Department will sanitize the university asset within 3 business days of their official departure. During this time, the asset's hard drive (or the entire asset) will be stored in a physically secure location. The department where the individual works is responsible for ensuring that all department data has been removed prior to the individual's departure.

Retiring a University Asset into "Salvage" at University Park

University Assets that have reached their end of life and utilization by the Penn State New Kensington Campus are marked to be transferred to "Lion Surplus aka Surplus and Salvage" by the NK ITS Department. University Assets that are marked as "Salvage" are transferred to University Park by the NK ITS Department.

1. Once a University Asset is marked as "Salvage" by the NK ITS Department, the hard drive(s) must be sanitized prior to delivery to University Park. During this time, the asset's hard drive (or the entire asset) will be stored in a physically secure location.

Destroying a "Dismantled" University Asset

University Assets that are inoperable and not economical to repair are marked as "dismantled".

1. Once a University Asset is marked as "dismantled" and documented with Human Resources, the NK ITS Department will sanitize the asset's hard drive(s) prior to destruction. During this time, the asset's hard drive (or the entire asset) will be stored in a physically secure location.
2. The University asset will be disposed of properly to comply with University policies.

Methods of Sanitization

Hard Drives

1. Software based

   a. The NK ITS Department will utilize software utilities such as “Killdisk” or "DBAN" for secure data destruction. These utilities, which meet the American Department of Defense 5220.22-M standard, securely wipes the computer hard disks and prevents data from being recovered from them and hinders all known techniques of hard disk forensic analysis.
2. Rendering device unusable
   a. This is an alternative for defective hard drives or for those that would be too costly to repair. For added security and if possible, the disk should be sanitized prior to physical destruction.

Flash Drives

The NK ITS Department is responsible for overseeing the sanitization of all flash drives that contain institutional data prior to disposal. Any flash drives that contain institutional data which need to be disposed of must be brought to the NK ITS Department for proper sanitization.

1. Software based
   a. The NK ITS Department will utilize the File Shredder feature in Identity Finder to ensure all data is permanently deleted.
2. Rendering device unusable
   a. If the flash drive is not operational, the NK ITS Department will render the flash drive unusable prior to disposal.

CDs and DVDs

All CDs and DVDs that contain institutional data, copyrighted, or University licensed materials must be rendered unusable prior to disposal.

Floppy Disks

1. Software based
   a. The NK ITS Department will utilize the File Shredder feature in Identity Finder to ensure all data is permanently deleted.
2. Rendering media unusable
   a. If the floppy disk is not operational, the NK ITS Department will render the floppy disk unusable prior to disposal.

Procedure History:

September 19, 2019 – Removed AD20 references from the definitions section
April 3, 2018 – Updated Appendix A & B to reflect new University policies
September 28, 2017 – Procedure created based off previous campus policy.

PennState
New Kensington

Appendix A

To: System User
From: Campus Administrator
Date: 01/01/2010
Subject: Personally Identifiable Information

Recently the computer issued to you to conduct University business was scanned for Personally Identifiable Information (PII). Based on the scan results, it appears your computer contains PII (Social Security Numbers (SSNs), credit card numbers, Driver's License numbers, passport numbers, Personally Identifiable Health Information (PHI), salary and tax information related to individuals, details of University budgets, tenure or promotion information, staff employee review information, password or other system access control information, human subject information, admission and financial aid information and donor information). This is a violation of University policy. If you believe that you are required to store PII electronically, contact me directly to discuss your needs.

The file(s) in question can be found at:

[Insert Location Information]

Based on campus procedures, you are required to remediate this PII data within two days of notification. Once remediation has occurred, please reply back to this ticket to confirm that the PII has been properly removed. If you require assistance with the remediation process, please visit http://newkensington.psu.edu/assistance and submit a Service Desk Request.

Remediation of PII is an important task that must be done promptly. If you do not remediate this PII within two days, your Access Account will be locked and additional sanctions may be applied.

I would also like you to review the following policies related to the use and archiving of PII. As you will note, there can be major costs to the campus both financially and to our reputation if this PII were ever compromised.

University Policy:

- AD95 – Information Assurance and IT Security
- AD96 – Acceptable Use of University Information Resources
- ADG08 – Collections, Storage and Authorization Use of Social Security Numbers and Penn State Identification Numbers
- AD22 – Health Insurance Portability and Accountability Act (HIPAA)
- AD35 – University Archives and Records Management

- AD53 – Privacy Policy

Training Resources:

- https://resources.ittraining.psu.edu/public/resources/IdentityFinder/Index.htm
- https://psu.app.box.com/v/using-spirion-for-windows

I appreciate your prompt attention to this matter.

Appendix B

To: System User
From: Campus Administrator
Date: 01/01/2010
Subject: Computer Compromise Containing PII

I was recently informed that the computer issued to you to conduct University business was compromised by virus or malware software. Subsequently, the ITS department scanned the computer to ascertain if it contained Personally Identifiable Information (PII). Based on the scan results, it appears your computer contains PII (Social Security Numbers (SSNs), credit card numbers, Driver's License numbers, passport numbers, Personally Identifiable Health Information (PHI), salary and tax information related to individuals, details of University budgets, tenure or promotion information, staff employee review information, password or other system access control information, human subject information, admission and financial aid information and donor information). This is a violation of University and campus policy.

In line with University policy, an incident has been created with the University Information Security and Privacy offices. Depending on the outcome of their investigation, the campus may be responsible for contacting all of the affected parties in accordance with the Pennsylvania State Breach Notification Law. This incident may create a substantial financial and reputation burden to the campus.

Incidents of this nature are confidential and should not be discussed outside of the personnel involved in investigating and remediating the incident.

Depending on the outcome of the investigation, you will be expected to take an active role in the remediation process and to attend a training program regarding the appropriate use of institutional data and PII. Additionally, this letter and an outline of the incident will be placed in your personnel records as your actions have violated University and campus policy.

Please take this time to review the following policies related to the use and archiving of PII.

University Policy:

PennState
New Kensington

- AD95 – Information Assurance and IT Security
- AD96 – Acceptable Use of University Information Resources
- ADG08 – Collections, Storage and Authorization Use of Social Security Numbers and Penn State Identification Numbers
- AD22 – Health Insurance Portability and Accountability Act (HIPAA)
- AD35 – University Archives and Records Management
- AD53 – Privacy Policy

Upon receipt of the final report and recommended actions by the University Information Security and Privacy Offices, I will advise you on your responsibilities in the remediation process.

Sincerely,
Me