OPERATIONAL POLICY AND PROCEDURES

SUPERSEDES POLICY: NEW
PROCEDURE NUMBER: PSU-MA-IT-014
DATE: Nov. 20, 2014
SUBJECT: University Institutional Data and Personally Identifiable Information
PAGE COUNT: 8

PURPOSE:
To formally outline the campus’s actions to assure the appropriate use, confidentiality, integrity, and availability 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 policy applies to any device which contains or on which data or PII is stored and/or to personnel who use such data or information.

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 at the discretion of the University unit responsible for the computer resources, or by order of the Security Operations and Services Director if revocation is necessary to protect the overall security of the University's Computer and Network Resources (e.g., a summary suspension of computer access as outlined in Policy AD20). (See also Computer and Network Resources.) The Administrative Information Services Security Officer may also order revocation of an account on any Institutional Computer and Network Resource if continuation of the account places Computerized Institutional Data at undue risk.

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, system software, or configuration files that 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 AD20 and AD23 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 University Policy and any applicable local, state, and federal law. The University is not responsible for the content of users' personal web spaces, nor the content of servers, programs or files that users maintain either in their personally-allocated file areas on University-owned Computer Resources or on personally-owned computers connected to the University's Computer and Network Resources. However, the University reserves the right to suspend network access or computer account(s), or to impose other sanctions as defined in Policy AD20 if such user-maintained files, programs or services are believed to have been operating in violation of either University Policy or applicable local, state, and federal law. The term "Computer and Network Resources" shall specifically include any computer hardware or computer systems owned independently by a System User or third party which are connected to the University network and contain University Institutional Data. Use of independently owned hardware in connection with any account shall not, in any manner, limit the enforcement rights of the University under the computer and network policies and guidelines then in place regarding inappropriate use of University Computer and Network Resources.

*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 equipment 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.)

*Mont Alto Data Network* – The technology infrastructure, hardware, and software installed at the Penn State Mont Alto campus which are used to facilitate the flow of digital information between (but not limited to) personal computers, printers, servers, the Internet, etc.

*Personally Identifiable Information (PII)* – Includes the following but is not limited to, Social Security Numbers (SSN’s), Driver's License 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, admissions and financial aid information and donor information.

*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, ensuring appropriate security measures have been implemented pursuant to the type of data being transmitted or stored, and managing overall computer or network operation and availability. System Administrators may be members of the Mont Alto Information Technology Services (ITS) Department or faculty/staff members who have requested elevated administrative access to a computer or network resource and have completed the Administrative Access Request Procedure per campus procedure PSU-MA-IT-00R.

*System User* – any individual who uses University Computer and Network Resources.
POLICY:
Use of PII
Social Security & Driver’s License Numbers
The use and archival of SSN’s & Driver’s License Numbers in electronic format is restricted to departments or employees with an exception from the University Chief Privacy Officer as stated in University policy AD19. The Mont Alto campus has two exceptions:

1. Continuing Education facilitates certification exams which require the use of PII for reporting to state agencies.
2. Police Services which utilizes PII as the primary identification number for law enforcement and criminal justice records.

The storage of SSN’s on any media whether electronic or physical is strictly prohibited otherwise. If a campus department or employee requires access to SSN data, access to the University’s Central ID Repository (CIDR) is required. The campus Access and Security Representative (ASR) facilitates access requests to the CIDR system. Historical records containing SSN’s in off-line storage, such as paper, tape, cartridge, fiche, microfilm or magnetic media may be maintained, but access to these off-line records must be limited and secure. All records that are no longer needed must be purged and disposal of the records must follow University Policy AD35 - Archives and Records Management.

Credit Card Information
The storage of credit card information on any media whether electronic or physical is strictly prohibited.

Personal Employee Information
Electronic storage of personal PII such as the employee’s SSN, credit card, bank account numbers, or Personal Health Information (PHI) is prohibited. In certain situations, employee PII is used for grant applications or for research funding. This is a legitimate use of PII; however, upon completion of the application or document, PII must be removed from the document prior to archival. If a document must be archived with PII data enclosed, an appropriate AD19 exception must be sought from the Privacy Office.

University Institutional Data
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, assuring University computers are secure at all times, and passwords are changed on a regular basis and meet complexity requirements.

This applies to all PII and institutional data not otherwise defined by a specific portion of this policy. Refer to University policies AD20 & AD35 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.

All University employees should consider institutional data confidential and err on the side of caution when asked to distribute or provide institutional data. If a questionable request is presented, contact
the campus Access and Security Representative or Director of Information Technology to confirm the legitimacy of the request prior to complying.

**Remediation of PII**
In an attempt to eradicate archived or unnecessary PII from all University-owned computers that do not have an exception, the ITS department has installed software which searches all electronic data on a computer hard drive for PII. The scan tool (Identity Finder) allows system users and system administrators to conduct a scan and self-remediate at any time. Mandatory scans will run automatically on a bi-weekly schedule, and will present to the system user a report detailing potential PII items on at least a monthly basis.

ITS will review potential PII items which have been reported by the automatic scans on at least a bi-annual basis. If a computer is found to have positive results of PII, the system user, will be sent an e-mail (Appendix A) regarding their non-compliance with University and campus policy. The system user will be required to remediate the system within seven days of receiving the e-mail.

If a computer is found to have the same positive results of PII upon the completion of the next bi-weekly scan, the system user, and their supervisor, will be sent an e-mail (Appendix A) regarding their non-compliance with University and campus policy. The system user will be required to remediate the system within seven days of receiving the e-mail.

If a computer is found to have the same positive results of PII upon the completion of a third bi-weekly scan in succession, the system user, their supervisor, and the campus chancellor, will be sent an e-mail (Appendix A) regarding their non-compliance with University and campus policy. The system user will be required to remediate the system within seven days of receiving the e-mail.

If a computer is found to have the same positive results of PII upon the completion of a fourth bi-weekly scan in succession, the system user’s account will be locked with further disciplinary action to be determined by campus administration.

Campus System Administrators are responsible for the servers or workstations they maintain. System scans, using the scan tool where applicable, must be completed at least annually and upon request of the ITS Department. System Administrators have seven days to complete the scan after receiving the request. Notification of System Administrators will follow the same procedure as outlined above for system users. If a server is found to contain PII and is Internet facing (i.e. web server) ITS will disconnect the system from the data network immediately until a PII scan is completed, the system is remediated, and a subsequent scan confirms it is free of PII.

**Compromised PII**
If a computer system is found to be compromised by a virus or malware program, the device must be removed from the Mont Alto data network immediately and the following actions taken:

1. The Mont Alto ITS Department is required to take custody of the machine immediately.
2. The removal of data from the device once it is found to be compromised by either a system user or system administrator is prohibited.
3. The ITS Department will scan the compromised device for PII and provide the results to the Security Office for analysis.

4. If the device contains PII, the system user will be issued a temporary computer for use while an investigation of the compromised computer is conducted.

5. Depending on the outcome of the investigation, one of two actions will be taken:
   a. If the device is free of PII, the user’s files will be archived; the system will be restored to a non-compromised state and then returned to the user.
   b. If the device is compromised and found to have positive notifiable PII results, the case will be referred to the University Privacy Office for review and recommended action.

**Notification of Compromised PII**

In cases where a device is compromised and contains notifiable PII, the privacy office will advise the campus 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 PII compromise incident.

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

If a system user or system administrator is involved in an incident of this nature, the user will receive a letter (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 PII.

**SANCTIONS:**

Violation of any portion of this policy may result in initiation of legal action by the University and appropriate disciplinary action, which may include dismissal.

**CROSS REFERENCE:**

Other policies that should also be referenced:

*University Policies*
- AD20 - Computer and Network Security
- AD11 - University Policy on Confidentiality of Student Records
- AD19 - Use of Penn State Identifier and Social Security Number
- AD20 - Computer and Network Security
- AD22 - Health Insurance Portability and Accountability Act (HIPAA)
- AD23 - Use of Institutional Data
- Trusted Network Specifications
- AD35 - University Archives and Records Management
- AD53 - Privacy Statement
- ADG01 - Glossary of Computer Data and System Terminology
- ADG02 - Computer Facility Security
Campus Policies
PSU-MA-ITS-000 – End User Computer Agreement
PSU-MA-ITS-004 – Acceptable Use and Security Policy

Campus Procedures
PSU-MA-IT-00R – Administrative Access Request Procedure

POLICY HISTORY:
February 1, 2010 – Draft Finalized.
November 20, 2014 – Policy Revised and Ratified by Admin Council (Minimum Security Baseline)
To: System User  
From: Director of Information Technology Services  
Date: 11/20/2014  
Subject: Personally Identifiable Information  

Recently the device issued to you to conduct University business was scanned for Personally Identifiable Information (PII) which includes but is not limited to Social Security Numbers, Driver’s License Numbers, Bank Account Numbers, and Credit Card Information. Based on the scan results, it appears your device contains PII. This is a violation of University and campus policy. There is no need to store or archive PII electronically; this includes your own personal information.

If you believe that you are required to store PII electronically, contact me directly to discuss your needs.

Remediation of PII is an important task that must be done promptly. It is my expectation that you will complete the remediation within seven days. If you require assistance with the remediation process, contact the ITS helpdesk. If you do not remediate this PII in a timely manner, future e-mails regarding this matter will be copied to your supervisor and the campus chancellor with appropriate disciplinary action determined by campus administration at that time.

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

**Campus Policies**  
PSU-MA-ITS-004 – Acceptable Use and Security Policy  
PSU-MA-IT-014 - University Institutional Data and Personally Identifiable Information

**University Policies**  
AD19 - Use of Penn State Identifier and Social Security Number  
AD23 - Use of Institutional Data  
AD35 - University Archives and Records Management

I appreciate your prompt attention to this matter.
To: System User  
From: Director of Information Technology Services  
Date: 11/20/2014  
Subject: Computer Compromise Containing PII

I was recently informed that the device issued to you to conduct University business was compromised by a virus or other malware. Subsequently, the ITS department scanned the device to ascertain if it contained Personally Identifiable Information (PII) which includes but is not limited to Social Security Numbers, Driver’s License Numbers, Bank Account Numbers, and Credit Card Information. Based on the scan results, it appears your device contains PII. This is a violation of University and campus policy. There is no need to store or archive PII electronically; this includes your own personal information.

In line with University policy, the University Information Security and Privacy offices have been notified of this incident. 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 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 PII. Additionally, this letter and a summary 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 archival of PII.

**Campus Policies**
- PSU-MA-ITS-004 – Acceptable Use and Security Policy
- PSU-MA-IT-014 - University Institutional Data and Personally Identifiable Information

**University Policies**
- AD19 - Use of Penn State Identifier and Social Security Number
- AD23 - Use of Institutional Data
- AD35 - University Archives and Records Management

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