EI&O Acceptable Use and Information Security Procedures

Enterprise Infrastructure and Operations

a unit of The Office of the Vice President for Information Technology (OVPIT)

February 2017

Mark Zimmerman
EI&O Information Security Officer
The Pennsylvania State University

1.1. Table of Contents

1 Document Overview

The Mission of Enterprise Infrastructure and Operations (EI&O) is to serve as the central resource responsible for supporting University Information Services. As a unit of the Office of the Vice Provost for Information Technology (OVPIT), EI&O participates in the development, maintenance, and secure operation of Penn State student, business, and alumni systems.

EI&O's system environment is a diverse mixture of client/server applications, web services, and database services run on a variety of platforms. Customers include University departments, University campuses, students, and the general public. These systems are used for educational and business purposes in serving the interests of the students, our clients and customers.

Effective security is a team effort involving the participation and support of all University, employees and affiliates who deal with information and/or information systems. It is the responsibility of every computer user to be familiar with appropriate policies and procedures to conduct their activities accordingly. Penn State University is committed to ensuring that all systems solutions and networks within the organization meet all appropriate state, federal and compliancy requirements for data security and information protection including Payment Card Data Security Standards (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPAA) and The Family Educational Rights and Privacy Act (FERPA). Policies and procedures encompassed within Penn States proactive Security posture include, but are not limited to those referenced in Section 4 – Related Policies and Training.

This is a "living" document. With tracking through a revision history, this document will change and grow over time as security requirements change and as policies and procedures are developed. This document will be reviewed by the EI&O Information Security Office no less than annually to ensure that the content remains current. All references to "devices" in this document refer to University owned devices unless specifically noted.

2 Purpose

The purpose of this document is to define an EI&O Acceptable Use and Information Security Procedure and outline best case use of computer equipment within the department. This documentation is in place to protect the employee, students and institution. Inappropriate use exposes PSU to risks including virus attacks, compromise of network systems, data and services, and exposure to potential legal and compliance issues.

3 Scope

These procedures apply to employees, students, contractors, and consultants, casual and other workers within EI&O. Anyone connecting (wired or wireless) personal or other electronic devices to any EI&O network, application, system or server should adhere to these procedures.

4 Related Policies and Training

4.1. Policies Pertaining to Security

AD11	*University Policy on Confidentiality of Student Records (FERPA)*
AD20	*Computer and Network Security, with ADG01 Glossary of Computer Data and System Terminology*
AD22	*Health Insurance Portability and Accountability Act (HIPPA)*
AD23	*Use of Institutional Data*
AD24	*Identification Cards for Students, Faculty/Staff, Affiliates and Retirees*
AD35	*University Archives and Records Management*
AD53	*Privacy Policy (Formerly Privacy Statement)*
AD68	*University Access Policy (Formerly SY19)*
AD71	*Data Categorization and guidelines for ADG02 Computer Security and ADG07 Data Categorization Examples*
AD80	*Identity and Access Management (IAM)*
ADG08	*Collection, Storage and Authorized use of Social Security Numbers and Penn State Identification Numbers*
FN14	*Use of University Tangible Assets, equipment, supplies and Services*
RP07	*HIPPA and Research at Penn State University*
RP08	*HIPPA and Research at the Milton S. Hershey Medical Center and Penn State College of Medicine*
SYS2001	*University Access: Clearances, Keys and Access Devices; Authorization, Issuance and Fees*

4.2. Training Requirements

All EI&O employees are responsible for accomplishing and completing Information Security training as tasked by EI&O Management and the Information Security Office.

5 Confidential Information

1. The University, through its employees, will treat all of its information pertaining to students and employees as confidential, disclosing that information only when authorized by the student or employee in question, approved by the appropriate University Official, or required by local, state or federal law. Student and employee information is accessed by University Staff formally authorized on a need-to-know basis only for the business purposes of the University and approved by the appropriate EI&O Access and Security Representative (ASR). Aggregate information may be released by an appropriate University Official for example, to respond to a survey. Faculty, staff and employees shall take all necessary steps to prevent unauthorized access to confidential information.

6 Acceptable Use of Computing Resources

The following procedures apply to use of EI&O computing resources. These rules are not an exhaustive list of proscribed behaviors, but are intended to illustrate the standards. Additional rules may be promulgated for the acceptable use of computer systems or networks by departments and system administrators.

6.1. Computer Resources

The following activities and behaviors are prohibited:

- The use of restricted-access University computer resources or electronic information without authorization or beyond one's level of authorization

- The unauthorized copying or use of licensed computer software

- Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential or restricted under the University's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records, or as defined by the Data Steward

- Intentionally compromising the privacy or security of electronic information

- Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction).

- Privately owned personal computers used to work on University information is subject to review and oversight to ensure appropriate data security.

- Tampering with or disabling antivirus software.

All hosts used by the employee that are connected to the University Internet/Intranet/Extranet, whether owned by the employee or Penn State, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

6.2. Endpoint Desktop Devices

EI&O Systems shall be centrally managed to address licensing, ensure the use of EI&O operating systems, ensure appropriate authentication and authorization, and guarantee the appropriate use of anti-virus and Data Loss Prevention (DLP) software.

- A documented request must be made to the EI&O Information Security Office and Senior management for a system to be individually managed

- All machines will require installation of a PSU security profile in addition to desktop management access and a combination of manual and automated controls to include, but not limited to, the following:

  - All devices shall have appropriate Data Loss Prevention software installed (as appropriate) and scheduled to scan on a regular schedule (monthly, at minimum). Remediation of DLP events will occur in a timely fashion.

  - PSU Acceptable Use/PSU Legal Notice Warning

  - Embedded agent for real-time client status reporting, patching, software distribution, and security policy enforcement

All desktop equipment and associated peripherals (e.g., monitors, external drives) assigned to EI&O personnel shall be ordered and inventoried annually by the desktop management team.

Systems are coordinated and provisioned through Central EI&O Desktop Management.

Asset data shall be inventoried and maintained in an appropriate asset tracking solution including those assets provisioned and used at non-University locations.

All installed software shall be in compliance with Penn State licensing policies.

All devices shall be configured to ensure that only authorized personnel are able to access data on the device, and that administrative and local user accounts are created and removed in accordance with University policies.

All devices shall run anti-virus programs (as appropriate), and the anti-virus definitions shall be updated in a timely manner.

All devices shall be configured to ensure that data stored are properly encrypted and safeguarded in compliance with the University's data classification standards.

6.3. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

- Installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the user or Penn State.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Penn State or the end user does not have an active license is strictly prohibited.

- Exporting software, hardware, information, encryption software or technology, in violation of international or regional export control laws, is illegal. Appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or endpoint systems (e.g., viruses, worms, Trojan horses, e-mail phishing, etc.).

- Attempting to circumvent access codes, passwords or authentication procedures using loopholes, vulnerabilities or malicious code. This activity is deemed unethical and illegal. Unintentionally gained access must be reported to the appropriate system administrator immediately.

- Anonymous activity (unless the recipient expressly accepts anonymous information) or any attempt to disguise the identity of computing resources is prohibited.

- Using a Penn State computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

- Making fraudulent offers of products, items, or services originating from any Penn State account.

- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to EI&O is made.

- Executing any form of network monitoring which will intercept data not intended for the user’s host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.

- Interfering with or denying service to any user (for example, denial of service attack).

- Financial solicitation not related to official University business.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the

Internet/Intranet/Extranet.

- Providing information about, or lists of, Penn State students, employees or faculty to parties outside Penn State.

- The use of encryption technology for the purpose of masking or tunneling the inappropriate use of University infrastructure (for example, copy-infringed Peer-to-Peer file transfers).

6.4. Legal Notice Warning

All user and administrative systems will be configured with a Login Banner or text notice reflecting:

This system is Property of The Pennsylvania State University. Its use is reserved for persons authorized by Penn State and is governed by Penn State Security and acceptable use policies.

7 Application and Operating System Protection

One of the biggest exposures for many computer systems today is the software running on it. Whether this software is the operating system, a service provided by the OS, an application, or database, efforts must be taken to prevent system vulnerabilities and compromise. The following sections outline the minimum steps for protecting the "core" software components of EI&O systems.

7.1. Operating System Hardening and Patching

Operating Systems are loaded by the Systems Engineering Mid-Tier Infrastructure or Desktop Support groups and follow a standard procedure that includes evolving best practice and integration of appropriate patches and Hotfixes identified by Mid-Tier, the Information Security Office and the Office of Information Security.

Existing systems shall receive updates on a periodic basis as determined by the MTI, Database, and LAN/Desktop Groups. Any update determined to be of a "Critical" nature shall be applied to systems within a week after it is released from the vendor. The MTI, Database, and LAN/Desktop Groups are responsible for ensuring that testing of patches is performed prior to installation. On desktop systems, the installation of these updates shall be automated where possible.

7.2. Application Hardening

For applications that have been developed external to the organization, Penn State employees responsible for supporting the applications must keep EI&O support staff aware of security-related updates. Implementation of such updates shall be coordinated with the MTI and Desktop Management groups.

7.3. Authentication Standards

All user authentication for restricted access is accomplished by the use of WebAccess filters, 2-Factor authentication (as directed by EI&O management) or by confirming user ID and password combinations against the OVPIT centrally managed user account repository. Authorization is performed in conjunction with group definitions in the OVPIT LDAP repository where possible. If LDAP authorization is not possible, authorization methods may occur through the OS, Database, or application level security.

7.4. Application and Web Application Vulnerability Scans

All applications hosted within EI&O will be initially scanned for vulnerabilities and Web application (if applicable) issues for vulnerabilities prior to initial deployment.

Continuing periodic scans must be performed thereafter on systems in Production environments.

All servers shall use encryption and cipher suites approved by the EI&O Information Security Office and Senior Director.

8 Perimeter Protection

There are a number of layers that help provide a secure computing environment. These areas include subnet assignment, vulnerability scanning, anti-virus scanning, firewalls, intrusion detection scanning, and physical security.

8.1. Requirements

8.1.1. Wired

- No system shall have concurrently active network cards configured to bridge between network segments without permission from the Information Security Office. Such machines act as a bridge between the two subnets and bypass firewall controls.

8.1.2. Wireless

- Production, Acceptance, or Test servers shall not use wireless subnets.
- Only PCs and laptops and mobile devices may use wireless subnets.
- Adapters shall only be used in “Infrastructure” mode, not “Ad Hoc.” That is a user shall not use his/her machine as a wireless access point for other users or devices.

8.2. Network Firewall

A Firewall shall be used to provide perimeter protection for the EI&O subnets against unauthorized access and common port probes. By default, no traffic is allowed to pass through the firewall. An exception list, which is stored on the firewall, will allow authorized traffic to reach EI&O servers.

8.2.1. Exceptions

Requests for firewall exceptions and changes shall be initiated and submitted and approved by the EI&O Information Security Office. Once approved, changes shall be implemented and maintained by the Network Infrastructure group.

All change requests shall be submitted via the appropriate EI&O service request application. Requests shall include the following information:

- Reason for Request (Business Justification):
- Name of Destination Server:
- Destination server's IP Address:
- Source system's name or owner:
- Source system's IP address:
- Port to be opened:
- Purpose of port:
- Protocol to be used (TCP/UDP):

8.2.2. Firewall Auditing

The Information Security Office shall periodically scan all EI&O subnets from an address outside PSU in order to audit firewall protection. Results shall be reported to OIS, Mid-Tier Management and LAN/Desktop group, as appropriate.

8.3. Host-Based Firewall

A secondary host-based firewall system may be established on critical systems. The implementation should, however, be reviewed by MTI and the EI&O Information Security Office.

Telecommuters who are connected through external ISP are required to use personal firewall software on their system.

8.4. Network and Protocol Vulnerability Scanning

Vulnerability scanning is an integral part of EI&O's security management strategy. It ensures policy compliance and detects vulnerabilities that leave systems open to compromise. Scans are performed by the EI&O Information Security Office or Penn State's OIS department as requested.

Systems may be required to disable local or host based firewall software prior to scanning.

Scan results shall be maintained by the EI&O Information Security Office.

Scanning for all systems is required before going into Production/Acceptance prior to deployment. Scanning shall occur after all required software and patches have been loaded.
Existing systems shall receive security scans a minimum of two times annually.

All vulnerabilities of *critical* and *high* threats, as classified by the scanning solution and Common Vulnerability and Exposure (CVE) catalog must be addressed unless determined to be an exception by OIS and the EI&O Information Security Office. Vulnerabilities of *medium* threat classification may be addressed as judged by the Information Security Office.

9 Passwords

All passwords for EI&O systems will, at a minimum, abide by and be in compliance with the OVPIT Password Policy published by OVPIT and the EI&O Password Standard Operating Procedures. Departmental and system level processes can be implemented that are more stringent than the OVPIT policy. The guidelines for password creation from the OVPIT Password Policy will be followed for all EI&O passwords.

9.1. Account Revocation Guidelines

- Upon employment termination an employee's supervisor and Human Resources Representative are responsible for initiating the OHR Workflow Termination Process (IBIS TRMN form) to ensure that access credentials are disabled by EI&O Security in a timely manner.

  https://guru.psu.edu/policies/OHR/hr102.html

- Additionally, In the event of involuntary termination of employment and to protect Penn State University data and prevent data loss, credentials and accounts can be immediately disabled via a verbal request from HR or OIS to EI&O Data Security.

10 Other Protections and Depth of Defense

10.1. Anti-Virus Software

Anti-Virus software shall be used as part of the standard server and PC configuration at EI&O. Virus signatures shall be configured to update on a daily basis at minimum.

10.2. Access to Sensitive Data and Storage

EI&O employees who require access and download subsets of sensitive data to their PCs or Servers as a result of a database queries or testing during the due course of their job responsibilities shall appropriately safeguard and delete such data after use. Employees are strongly encouraged to do this only when necessary. Sensitive data needed for development or testing purposes needed on local PC's should be "anonymized" or modified in such a way that the contents of the data no longer contain sensitive information. Employees shall also make sure that deleted data is not stored in a system "recycle bin" or "trash can."

Employees requiring access to this type of information will be required by the EI&O Access and Security Representative (ASR) to read, understand and validate that they understand all aspects of Penn State Policy AD23 Use of Institutional Data.

10.3. Remote Access and Remote Transfers

EI&O employees and EI&O batch processes shall use a secure FTP, SSH or VPN for file transfers and terminal access to/from areas outside of the Penn State data backbone. Examples of this include transfers to PHEAA and mygrades.com. When transfer and access functions are not achievable with a secure connection, the Information Security Office shall be notified.

EI&O employees shall not send Email messages that contain sensitive data to non psu.edu recipients. Employees with this need should contact the EI&O Information Security Office.

EI&O Home Users and Traveling Users shall use Penn State University hosted VPN sessions for accessing EI&O systems, data, and email. When access is not possible through the VPN, the EI&O Information Security Office shall be consulted for alternate access methods.

EI&O employees are prohibited from using unauthorized remote access software such as pcAnywhere, Remote32, and gotomypc.com.

10.4. Use of Password-Protected Screensavers

All EI&O desktop systems and server systems shall have password-protected screensaver or session timeout enabled that will activate after no longer than 15 minutes of idle time.

11 Reporting, Logging, and Auditing

The Information Security Office shall be given access to all logs and log reports related to security for Production, Acceptance, Dev, and Test servers. Automated methods for alerting when logon thresholds are exceed should be leveraged whenever possible. Logs shall be reviewed as detailed below:

11.1. Authentication Logging

Authentication logs shall be captured including Login user ID, Login time, Login success/failure status. Origin of request (IP address) should also be captured if possible.

Systems for which manual reviews are accomplished should occur daily.

11.2. Database Logging

All production databases shall generate logs that, at a minimum, capture the following information: Login user ID, Login time, Login success/failure status.

11.3. Firewall Logging

Firewall logging is enabled and shall capture both inbound and outbound connections.

11.4. Intrusion Detection Logging

Intrusion Detection logs shall be reviewed by OIS and the Information Security Office.

11.5. Application Logging

If an application has the capability of security logging, that logging shall be enabled and reports will be reviewed on a periodic basis as determined by the Information Security Office. Any exceptions or anomalies will be followed up and assigned to the appropriate parties for review and remediation.

11.6. Web Logging

Automated logging of all successful and unsuccessful access attempts must be captured.

11.7. Operating System Logging

Enable auditing for logon and object access events

Enable auditing for policy change

Enable auditing for account management

12 Disposition of Storage Media

Storage media at end of life must be disposed of properly to avoid unintentional data exposure.

In compliance with and extension to, PSU Minimum Security Standards, EI&O will extend the standard to all server data storage media regardless of the classification of the data that was stored on the media.

All server data storage media will be physically destroyed when it has reached end of life.

13 Disaster Recovery and Business Continuity

13.1. Schedule

System Administrators are responsible for annually planning, testing and implementing Disaster Recovery and Business Continuity plans and mechanisms to ensure continuous operations.

14 Definitions

For the purposes of this document, the following definitions will be used:

14.1. Server

Any EI&O computer that provides services to other remotely connected computers and users. EI&O servers are *dedicated* computers or VM hosts running on *server-class* hardware.

14.2. PC Server

Any EI&O computer that provides services to other remotely connected computers and users. EI&O PC servers run on *personal computer* hardware. Examples include user workstations running ftp or web services for development purposes.

14.3. Personal Computer

A personal computer is any EI&O computer used for day-to-day work and end-user access to PSU resources. EI&O PCs have a standard OS and application installation managed by Desktop Support.

14.4. Production

A server is considered to be in Production if code changes and application configuration changes have been frozen. Future changes are handled through the application group's change control processes. Production servers are generally monitored for service interruptions and data is backed up on a periodic basis.

14.5. Acceptance

Prior to going into Production, a system is considered to be in Acceptance. The Acceptance environment should be as close as possible to what will exist in Production. Pilot projects may be conducted on Acceptance machines.

14.6. Development / Test

Prior to going into Acceptance, a server is considered to be in Development or Test.

14.7. System/Service Account

A system/service account is an account that is utilized by an application for restricted access authentication and authorization. A system account does not represent an individual person, it represents an individual application or system.