

## Steps to Information Privacy and Security

**Step 1:** Protection from the public Internet or external network segments (direct probes).

**Step 2:** Systems connecting to the Penn State network will be free from known vulnerabilities.

**Step 3:** Access to systems will be individually controlled. All actions must be traceable to a unique user ID.

**Step 4:** Access to systems and applications (beyond public display) will be logged.

**Step 5:** Data will be secured at rest and in transit commensurate with its sensitivity.

**Step 6:** Sensitive data must be sanitized or destroyed prior to system re-use by another entity.

**Step 7:** Physical and facility security must be maintained.

**Step 8:** A development and risk assessment process must be in place commensurate with the sensitivity of the data.

**Step 9:** Units will maintain local policies in accordance with, and augmenting, University Policy AD20 (Computer and Network Security) and applicable external regulations.

**Step 10:** Backup and Disaster Recovery measures must be in place commensurate with the value of the computer and network resources, and the category of data held.

[ipas@psu.edu](mailto:ipas@psu.edu) | 814.867.1340 | [www.ipas.psu.edu](http://www.ipas.psu.edu)



### Contact Us

E-mail: [ipas@psu.edu](mailto:ipas@psu.edu)  
Phone: 814.867.1340  
Web: [www.ipas.psu.edu](http://www.ipas.psu.edu)

### IPAS Team

**Mike Leach**, Project Manager  
Phone: 814.865.0740  
E-mail: [mjl9@psu.edu](mailto:mjl9@psu.edu)

**Craig Henninger**, Senior Network Analyst  
Phone: 814.863.8816  
E-mail: [cah9@psu.edu](mailto:cah9@psu.edu)

**Jenn Stewart**, Project Technical Coordinator  
Phone: 814.863.7820  
E-mail: [jas72@psu.edu](mailto:jas72@psu.edu)

U.Ed. SOS 08 5001

This publication is available in alternative media upon request.

Penn State is committed to affirmative action, equal opportunity, and the diversity of its workforce.



## PHASE II

### *The Early Stages*

**Including Scanning, Encryption and Data Classification**

### *Our Mission*

The Information Privacy and Security (IPAS) Project is a University-wide project with the mission of enhancing the information security practices at Penn State.

The primary project goals are to ensure the privacy of critical information and to comply with internal policies and external regulations affecting Penn State.

[ipas@psu.edu](mailto:ipas@psu.edu) | 814.867.1340 | [www.ipas.psu.edu](http://www.ipas.psu.edu)

## *Project Overview*

The primary project goal is to ensure the privacy of critical information and to comply with internal policies and external regulations affecting Penn State. The steps required are highly technical and include reviews of information technology infrastructure, network design, application architecture, policies, procedures, and processes.

To achieve the overall goal of improving the state of network security at Penn State, the IPAS project requires two phases, one of which has been completed. Phase I addressed PCI DSS compliance (credit card processing). Phase II will focus on overall information privacy and security practices relative to current statutory compliance obligations and improve our ability to respond to new legislation.

There are 14 issues, for which the IPAS team was charged with developing recommendations, for Phase II. A list of these 14 issues can be found at: <http://ipas.psu.edu/phase2/project2.pdf>. Some of Penn State's security initiatives include the need for scanning and encryption. Both initiatives will be implemented by fall of 2008.

## *Sensitive Information*

The goals of Phase II focus on the protection of sensitive information. Examples of sensitive information include but are not limited to:

- \* Social Security Numbers (SSN)
- \* Driver license numbers
- \* Personally Identifiable Health Information (PHI)
- \* Details of University budgets
- \* Tenure or promotion information
- \* Staff employee review information
- \* Password or other system access control information
- \* Human Participant information
- \* Admission and financial aid information
- \* Bursar bills that are personally identifiable

## *Data Classification Scheme*

In support of Phase II and University Policies, AD23 and AD20, a Data Classification Scheme was developed. The Scheme consists of:

Two primary classifications of systems/networks:

- \* Public
- \* Non-Public

Three primary classifications of data  
(Examples are not exhaustive):

- \* Public (campus maps, directory information, e-mail addresses)
- \* Internal (class rosters, employment applications, library collections)
- \* Restricted (SSNs, budget info, credit card numbers, donor information)

## *Scanning Tool*

Proventsure's Governance and Compliance Platform scanning tool is available to all Penn State departments. This client-server application scans systems for:

- \* Trojan Horse programs
- \* Rootkits
- \* Social Security Numbers
- \* Credit card numbers
- \* Bank account information

Visit <http://ipas.psu.edu/phase2/scanning.html>.

## *Encryption*

Encryption software when properly installed, configured and used can help protect sensitive information at rest and greatly limit the number of reportable data breaches requiring victim notification. The University has negotiated a site license with Utimaco Safeware for encryption tools for full disk and removable media encryption.

## *Ongoing Compliance Obligations*

Regulatory and industry security requirements include the need to continuously review security safeguards and evolving threats. Penn State is currently bound to the following:

- \* Payment Card Industry Security Standards (PCI DSS)
- \* Health Insurance Portability and Accountability Act (HIPAA)
- \* Gramm-Leach-Bliley Act (GLBA)
- \* Family Educational Rights and Privacy Act (FERPA)
- \* PA Mental Health Law
- \* PA Breach of Personal Information Notification Act [73 P.S. § 2301 et seq]
- \* 21 USC Chapter 16 - Drug Abuse Prevention, Treatment, and Rehabilitation
- \* The Privacy Act of 1974 5 U.S.C. § 552a
- \* Confidential Information Protection and Statistical Efficiency Act

Visit: <http://ipas.psu.edu/phase2/links2.html>.

## *IPAS Support*

The IPAS team assists departments in complying with ongoing regulatory and industry security requirements. In addition, policy and procedure review is done at the department level.

IPAS provides training on-demand in areas such as Payment Card Industry Data Security Standards (PCI DSS), Data Classification, and applying common sense security measures. There are multiple online training modules available as well. Visit <http://ipas.psu.edu/education/offerings.html> for a list of offerings.

Other responsibilities of the IPAS team include researching and testing new technologies to help meet compliance obligations. The IPAS team has made recommendations for a variety of centralized solutions, some of which have since been implemented.