Administrative Information Services
a unit of Information Technology Services

Security Policy
Version 2.5

1.0 Purpose (Reason for policy)

1.1 To establish data protection and Information Security Policy within AIS.

2.0 Scope (Who is affected by this decision.)

2.1 This policy applies to employees, students, contractors, consultants, and other workers within AIS, Anyone connecting (wired or wireless) personal or other electronic devices to any AIS network, application, system or server is subject to this policy.

3.0 Policy (Clearly stated decision.)

3.1 Because of the need to protect PENN STATE's network, management may access or monitor data stored on any network device belonging to Penn State University.

3.2 Information created using or stored on University computer systems are subject to the Penn State University Copyright Policy IP05 POLICY GOVERNING COPYRIGHT CLEARANCE (Formerly AD46) , which covers copyright issues pertaining to University faculty, staff and students as well as commissioned works of non-employees.

3.3 Employees, students and faculty are responsible for exercising good judgment regarding the reasonableness of personal use of Penn State computing resources and are subject to ITS and AIS policies.

3.4 AIS recommends that any information that users consider sensitive or vulnerable be encrypted. See Security Operations and Services Encryption Resources and Support for guidance. http://sos.its.psu.edu/services/encryption.html

3.5 For security and network maintenance purposes, authorized individuals within the University may monitor equipment, systems and network traffic at any time.

3.6 Penn State University and AIS may review information contained in backups in conjunction with its data integrity and safeguarding activities or as part of an official investigation.

3.7 Penn State University and AIS may audit networks and systems on a periodic basis to ensure compliance with this and other industry standard policies.

3.8 Penn State University and AIS may take emergency action to safeguard the integrity and security of electronic computing resources.

Required Action (Necessary steps to meet policy.)

In the event of an information security compromise the Information Security Officer shall be sent notification immediately and AIS shall work with Security Operations and Services (SOS) and the University Computer Emergency Response Team (CERT) to mitigate the threat. Additionally. The Information

Security Officer shall brief appropriate AIS employees as well as AIS senior management.

In the event of an attack, AIS's primary goal will be to protect confidentiality and integrity of its data even if this means an interruption in service to customers.

If a system is compromised, it shall (at a minimum) be reformatted, rebuilt and passwords changed. A post-attack analysis shall be completed to determine long-term corrective action and an after-action report created.

4.0 Enforcement (Actions taken by the owner when policy is disregarded.)

4.1 Disregard and failure to adequately protect Penn State computing resources and institutional information may result in disciplinary sanctions ranging from a disciplinary warning to termination or expulsion from the University.

5.0 Definitions (Terms used to define policy.)

Term	**Definition**

6.0 Revision History

Revision	Release Date	Description of change	Auth
1.0	April 21, 2003	Initial release.	Todd Litzinger
1.1	Oct 1, 2003	Inserted section on password auditing; modifications to Firewall section to account for new Change Control procedures; adding wording to section 5.1.1 on using PCs on production subnet and having two active network cards; added section 7.4 on Prohibited use of Remote Access Software;	Todd Litzinger
2.0	April 2004	Modified definitions section to allow for sensitive data on non-production systems; modified Application and OS Protection section to define distinction between NIS and LAN/Desktop Groups; changed Subnet Assignment section to include new test network and reference of diagram; modified section on physical security to include new policy on card access; moved sections on risks and CERT to appendix; added policy prohibiting use of personally-owned systems; added policy on use of password-protected screensavers; replaced network diagram with new architecture; other minor edits of wording.	Todd Litzinger
2.1	December 11, 2006	Updated for annual review	Carl Seybold
2.2	December 16, 2007	Updated for annual review	Carl Seybold

2.3	March 5, 2009	• Added section on Application Vulnerability scanning • Added section on Acceptable Use of AIS systems • Added section on Disposition of storage media • Updated many sections to keep them current	Carl Seybold
2.4	January 12, 2015	• Content Updates (OS revisions and reference to new AIS Password SOP) and added section on sensitive information access process by Application Developers.	Mark Zimmerman
2.5	May 11, 2015	• Document Review/Update. ACF2 Deprovisioning content added. Document separated into Policy and separate Acceptable Use and Information Security Procedures document.	Mark Zimmerman

7.0 References to other related policy within AIS, ITS or PSU.

All AIS users are expected to know and understand their responsibilities pertaining to system and data access including University Policies AD20 and AD23 along with University Guideline ADG01. The user affirms this by signing the "Request to Security Office for UserID to Access Administrative Computer System" form, which states that the user has read these policies and shall abide by them.

AD71 Data Categorization

AD20 Computer and Network Security

AD23 Use of Institutional Data

ADG01 Glossary of Computerized Data and System Terminology

Additional University policies concerning computer & data security:

AIS Security Policy (this document)

AIS Acceptable Use and Information Security Procedures

AIS Password Standard Operating Procedures

Penn State Minimum Security Standards

AD11 University Policy on Confidentiality of Student Records

AD35 University Archives and Records Management

ADG02 Computer Facility Security Guidelines