

# Data Classification

Kathy Kimball and David Lindstrom

ITS - Security Operations and  
Services

and

University Privacy Office

July 29, 2008

# Penn State: We Have a Problem

- 1790 systems scanned: 1004 have sensitive data
- Laptop theft or loss is a growing concern
- 4 Penn State Web sites allegedly serving malware (June 17-19), part of a global trend
- Continuous hostile probes of PSU network
- ~ 9,000 individual record breach notifications in past 12 months by Penn State or its data sources
- > 12,000 known compromises of PSU systems since 2002

# Data Classification

- Why?
  - Legal and Regulatory Compliance
  - More Effective IT Management
  - First step - We must know what needs protection and define the appropriate security commensurate with data value and risk

# Proposed Classifications

- Public
- Internal/Controlled
- Restricted

# Public

- Intended for distribution to the general public, both internal and external to the University
  - Release of the data would have no or minimal damage to the institution

# Internal/Controlled

- Intended for distribution within Penn State only, generally to defined subsets of the user population
  - Release of the data has the potential to create moderate damage to the institution. (Such damage may be legal, academic (loss or alteration of intellectual property), financial, or intangible (loss of reputation))

# Restricted

- Data which the University has a legal, regulatory or contractual obligation to protect
  - Access must be strictly and individually controlled and logged
  - Release of such data has the potential to create major damage to the institution. (Such damage may be legal, academic (loss or alteration of intellectual property), financial, or intangible....)

# Other

- Some data or projects have special restrictions imposed by the originator. Those restrictions may be over and above the security required by the general University standard

# Examples

- Public
  - Campus Maps
  - Directory information (where no Confidentiality Hold applies)
  - Email addresses of individuals (not bulk listings of all entries data mined from central services)
  - News stories (subject to copyright restrictions)

# Internal/Controlled

- Library Collections limited to Penn State use only
- Bulk email address listings containing all members of a major population (e.g., all students, all faculty/staff)
- Class rosters not containing SSN or other restricted information
- Employment applications unless restricted information is included

# Restricted

- Social Security Numbers
- Drivers' License numbers
- Personally Identifiable Health Information (PHI) - May have additional HIPAA controls
- Salary and tax information related to individuals
- Details of University Budgets
- Tenure or promotion information
- Staff employee review information

## Restricted (Continued)

- Password or other system access control information (to include biometric identification parameters)
- Human Subject Information (May have additional security requirements as identified by the originator or the Institutional Review Board)
- Non-directory information, to include photographs of individuals unless permission has been obtained for their use

## Restricted (Continued)

- Workman's Compensation or Disability Claims
- Employee background check information
- Admission and financial aid information
- Bursar bills that are personally identifiable
- Personally identifiable grade or transcript information
- Donor information
- Security settings or details of security configurations (e.g., detailed firewall rulesets)

## Restricted (Continued)

- Information to/from University Legal Counsel unless otherwise designated
- Ethnicity data other than aggregate statistics
- Disability status other than aggregate statistics

# Security Standards

- Security requirements are geared to the level of the data. On a practical basis due to the similarity of measures needed for internal/controlled and restricted, there are only two sets of requirements: public and non-public
  - Non-public=(internal/controlled or restricted)

# Important Caveats

- Some requirements may not be able to be implemented right away. These are identified as future/goals
- Controls required for non-public data are always good practice even for public data/systems
- If a unit cannot meet all requirements, compensating controls may be asserted
  - Will be evaluated individually
- Some communities may need exceptions to a limited number of requirements
  - Also evaluated on a case-by-case basis

# Security Requirements

- **Category 1: Protection from the public Internet or external network segments (direct probes)**
  - **The system will be segregated from direct hostile access initiated from the public Internet or network segments external to the local network**

# Security Requirements (Cont.)

- Public

- Unnecessary services off



- Non-Public

- Same as public plus:

- Firewall
- DMZ or equivalent
- Host-based firewall as appropriate
- Network Intrusion Detection

- Future/Goal

- Network Intrusion Prevention
- Host Intrusion Detection or File Integrity Monitor
- Host Intrusion Prevention

## Security Requirements (Cont.)

- **Category 2: Systems connecting to the Penn State network will be free from known vulnerabilities**
  - **Systems will be free from known vulnerabilities upon attachment to the network**

# Security Requirements (Cont.)

## Public:

- Automatically updated anti-virus as appropriate;
- Anti-virus software checks multiple vectors (web, email, etc);
- Anti-spyware measures as appropriate;
- Automatic updates for the operating system;
- Timely updates for applications.
- Future/goal:
  - Network Access Control

## Non-Public:

- Same as public



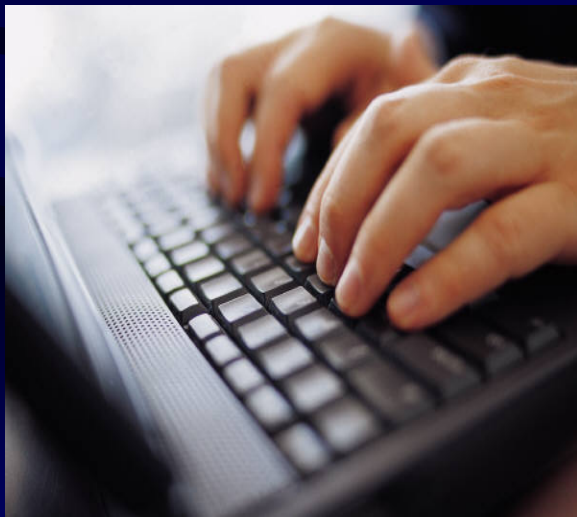
## Security Requirements (Cont.)

- **Systems will be checked periodically after joining the network to help ensure they do not contain known vulnerabilities**

# Security Requirements (Cont.)

## **Public:**

- No stated requirement; vulnerability scan(s) recommended



## **Non-Public:**

- **Regular vulnerability scan by ITS**
- **Future/goal: Regular vulnerability scan by unit**

# Security Requirements (Cont.)

- Applications made accessible over the Web will be scanned for known web application vulnerabilities



# Security Requirements (Cont.)

- Public
  - Application scan by ITS for web applications
- Non-Public
  - Same as public plus:
    - Regular vulnerability scan by ITS
    - Future/goal: regular vulnerability scan by unit; application level firewall for web applications involving restricted data

## Security Requirements (Cont.)

- **Category 3: Access to systems will be individually controlled. All actions must be traceable to a unique user id.**
  - **Access to multi-user systems will be individually controlled/authenticated**

# Security Requirements (Cont.)

- Public:
  - Strong password authentication
  - Local administrator rights disallowed to general users
  - Account access logged
- Non-Public:
  - Same as public, plus:
  - Future/goal:
    - Authentication beyond single factor user id/password. (Wherever possible this should be implemented now)

## Security Requirements (Cont.)

- **Access to personal desktop systems or laptops will be individually controlled. All actions must be traceable to a unique user**

# Security Requirements (Cont.)

- Public:
  - Password required at the time operating system loads; local administrator rights will be disallowed to general users
- Non-Public:
  - Same as public plus:
    - Future/goal:
      - Authentication mechanism beyond single user id/password

## Security Requirements (Cont.)

- **Category 4: Access to systems and applications (beyond public display) will be logged**
  - **Access will be logged and the log record will be retained for a time interval sufficient to meet incident response and legal/regulatory requirements**

# Security Requirements (Cont.)

- Public:
  - Retain system level audit logs; application level audit logs; email transaction logs (from/to, IP address, date/time);
  - Log retention (3 months online, 1 year offline)
- Non-Public:
  - Same as public plus:
    - Network level audit logs (e.g., firewall logs)
    - Log retention (6 months online, 6 years offline)

## Security Requirements (Cont.)

- **Category 5: Data will be secured at rest or in transit commensurate with its sensitivity**
  - Sensitive data will be encrypted wherever it resides

# Security Requirements (Cont.)

- **Public:**
  - **Not applicable**



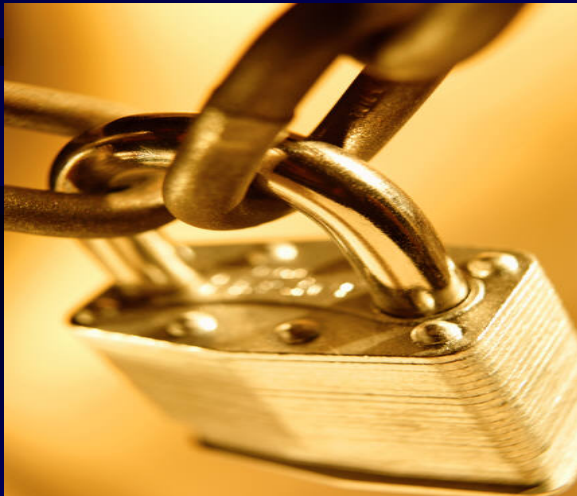
- **Non-Public:**
  - **Future/goal :**
    - **Full disk encryption, individual file/folder encryption**
    - **Professionally administered, physically secured server-class machines** need not be encrypted (at unit discretion).  
Must prevent unauthorized disclosure between user accounts and/or sessions

## Security Requirements (Cont.)

- **Sensitive data will be strongly encrypted when transmitted over local or wide area networks**

# Security Requirements (Cont.)

- Public:
  - Not applicable
- Non-Public:
  - Encrypted transmission means (e.g., ssl, sftp) will be used wherever possible
  - Future/goal: sensitive email will be encrypted



## Security Requirements (Cont.)

- **Category 6: Sensitive data must be sanitized or destroyed prior to system re-use by another entity**
  - Disks (or file systems) that have contained sensitive data must be sanitized or destroyed prior to re-use by another entity, either internal or external to the University



## Security Requirements (Cont.)

- **Category 7: Physical and facility security must be maintained**
  - **Physical and facility security must be in place commensurate with the sensitivity of the data**

# Security Requirements (Cont.)

- Public:
  - Not Applicable
- Non-Public:
  - Physically secured, locked space; employee identity proofing



## Security Requirements (Cont.)

- **Category 8: A development and risk assessment process must be in place commensurate with the sensitivity of the data**
  - **Units developing custom applications must have a documented design, development and test methodology**

# Security Requirement (Cont.)

- Public:
  - Security review at regular intervals during development
  - Documented configuration and change control process
- Non-Public:
  - Same as public



## Security Requirements (Cont.)

**– A risk assessment must be conducted for custom or major-vendor supplied applications prior to introduction as a production service**

- Public: Risk review with business process owner prior to introduction; formal acceptance of residual risk
- Non-public: Same as public

# Security Requirements (Cont.)

- Public:
  - Risk review with business process owner prior to introduction; formal acceptance of residual risk
- Non-Public:
  - Same As Public



## Security Requirements (Cont.)

- **Category 9: Units will maintain local policies in accordance with, and augmenting, University Policy AD20 (Computer and Network Security)**
  - **Units must ensure that appropriate policies and procedures exist in their area commensurate with the value of computing and network resources and the data residing therein**

# Security Requirements (Cont.)

- Public:
  - Unit policies required for data backup, change control and configuration management, acceptable use, network security, device control and configuration
- Non-Public:
  - Same as public plus contract provisions reviewed by Risk Management to share with third parties

## Security Requirements (Cont.)

- **Category 10: Backup and Disaster Recovery measures must be in place commensurate with the value of the computer and network resources, and the data held**
  - **Computer and network resources must have a documented (and tested) backup and recovery plan**

# Security Requirements (Cont.)

- Public:
  - Tested backup and restore capability for both files and full systems
- Non-Public:
  - Same as public plus secure offsite storage

We're All in This Together



The background is a dark blue gradient with several light blue, wavy, horizontal lines that create a sense of movement and depth. The lines are of varying thickness and curve slightly across the frame.

**Questions?**