Data Handling Standard
1 PURPOSE & BACKGROUND
The University's Information Security Policy requires controls to manage risks to the confidentiality, integrity and availability of University information. This standard defines the controls required for handling all University managed information in any form. These required controls represent a minimum standard for protection of University information. Additional controls required under applicable laws, regulations or standards governing specific forms of data (e.g. health information, credit cardholder data) may also apply.

The goals of this document are to (1) identify classifications of information handled at the University, and (2) define requirements for handling Sensitive and/or Highly Sensitive Data.

This document is classified University Public. This document may be shared internally and/or externally and is published online at http://getprotected.asu.edu.

2 SCOPE
This standard applies to all information handled by University employees, contractors or vendors. Each individual who creates, uses, processes, stores, transfers, administers and/or destroys University information is responsible and accountable for compliance with this standard.

University information includes but is not limited to information about students, former students, employees, other University affiliates (courtesy affiliates), research data, and intellectual property.

3 DATA CLASSIFICATION LEVELS

3.1 Level 1 – Public
Public refers to information that is publicly available and intended for public use. When used as intended, this information would have no adverse effect on the University's operations, assets, reputation or obligations concerning information privacy or on any individual’s privacy.

3.2 Level 2 – Internal
Internal refers to information that is reserved for private viewing, pending public release, opt-out directory information or internal University communications.

This information is not intended for parties outside the University and its designees. Unauthorized disclosure, compromise or destruction would have little to no adverse effect on the University’s operations, assets, reputation or obligations concerning information privacy.

3.3 Level 3 – Sensitive
Sensitive refers to information intended for limited use within the University by faculty, researchers, staff, students or University affiliates, including information that is regulated or must be protected due to proprietary or privacy concerns; e.g. private student records according to FERPA, personal health information (PHI) according to HIPAA, personally identifying information (PII) according to state and federal laws and industry regulations.

Unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on the University, its students or employees. Violation of statutes, regulations, or other legal obligations, actual or potential financial loss, damage to the University’s reputation and possible legal action could occur.

3.4 Level 4 - Highly Sensitive
Highly Sensitive refers to information involving human health, life, and safety matters or hazardous materials situations. This information is intended for extremely limited use within the
University on a need to know basis. Statutes, regulations, other legal obligations or mandates protect much of this information. Unauthorized disclosure, compromise or destruction would result in severe damage to the University, its students or employees or other individuals providing the information. Physical harm or endangerment, violation of legal obligations, actual or potential financial loss, damage to the University’s reputation and possible legal action could occur.

4 DATA HANDLING

4.1 Public and Internal Information
Confidentiality requirements do not generally apply to public information. Appropriate measures should be taken to ensure the integrity and availability of public information and to ensure the confidentiality, integrity and availability of internal information. These measures include:

• Read/write access controls
• Regular backups
• General workstation and server security practices

4.2 Sensitive and Highly Sensitive Information

4.2.1 Creation and Identification
Records containing Sensitive or Highly Sensitive information should exist only in areas where there is a legitimate and justifiable business need, as authorized by the relevant Data Trustee. When at all possible, Sensitive information should be accessed from its original source, and copies or printed versions of the information should be kept to a minimum. Computers and practices used to handle Sensitive or Highly Sensitive information must comply with ASU's Data Storage Guidelines.

University departments should work to identify and track all University records through their life cycle using Records Retention and Disposition Schedules and other University mechanisms. A first priority in this effort should be the identification of Sensitive information. Departments should make use of centrally provided automated tools to identify existing Sensitive or Highly Sensitive information on local systems.

Records Retention and Disposition Schedules (RRDS) should be created in collaboration with the University Archivist and maintained to document the existence of these materials and the rationale for keeping them and to help ensure their availability during the period for which they are vital as active administrative or historical records. Once the information no longer serves an active administrative or historical function according to its RRDS, it should be disposed of in a timely manner to mitigate the risk of exposure.

4.2.2 Access
Sensitive and Highly Sensitive information requires strict control. Access to Sensitive information shall be granted only to individuals or entities that are authorized by the relevant Data Trustee. Employees should receive annual training on their responsibilities regarding appropriate use and steps they can take to protect Sensitive information. Any other disclosure of Sensitive or Highly Sensitive information requires the written approval of the appropriate Officer of the University or Data Steward, in consultation with the Office of General Counsel as necessary.

Employees with access to Sensitive or Highly Sensitive information should be reviewed on an annual basis to ensure that access to this information is still needed. The list of people who have access to Sensitive or Highly Sensitive information and evidence of annual review of their access shall be made available to the Information Security Office on request.
4.2.3 Use, Transmission and Storage
The following controls are strongly recommended when using, transmitting or storing Sensitive or Highly Sensitive information:

- Do not discuss or display it in an environment where it may be viewed or overheard by unauthorized individuals.

- Do not leave keys or access badges for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.

- When printing, photocopying or faxing, ensure that only authorized personnel will be able to see the output. Sensitive or Highly Sensitive information should not be transmitted to network-connected printing/scanning devices unless on a closed or securely encrypted network.

- Store paper documents in a locked drawer and in a locked room or in another secure location approved by the Data Trustee.

- Properly identify such information as Sensitive or Highly Sensitive to all recipients by labeling it accordingly, providing training to personnel, explicitly mentioning the classification or similar means.

- Encrypt Sensitive or Highly Sensitive information using an industry standard encryption algorithm when (1) placing it on removable media; (2) placing it on a mobile computer (e.g. laptops, PDAs, smart phones); or (3) sending it via electronic mail.

- Do not send Sensitive or Highly Sensitive information via instant message or unsecured file transfer unless it is encrypted.

- Follow an established and documented software development lifecycle when building applications that process Sensitive or Highly Sensitive information.

- Applications that process Sensitive or Highly Sensitive information should comply with the Secure Web Development standard, Web Application Security standard and all other applicable information security standards.

4.2.4 Transport
The following controls are required when transporting Sensitive or Highly Sensitive information:

- When sending paper copies to off-campus locations (e.g. via United States Postal Service, UPS or FedEx), the information must remain secure. Consult with the appropriate Data Trustee for specific handling restrictions.

- When sending the information by campus mail in non-electronic form, the sender should consult with the appropriate Data Trustee for proper handling procedures. Such handling procedures might include using a security envelope with sealed flap inside a second envelope, stamping "Sensitive" or "Highly Sensitive" on the inner and/or outer envelope seal or signing the envelope seal.

- When carrying Sensitive or Highly Sensitive information or devices containing such information, ensure that it is physically secure at all times.

- Do not remove Sensitive or Highly Sensitive information from an approved secure location without prior approval of the Data Trustee.
4.2.5 Destruction

University records should be destroyed only in accordance with the University's Records Storage and Destruction policy (PCS 703). Sensitive or Highly Sensitive information in electronic form should be destroyed in accordance with the University's Surplus Property policy (PCS 1002-01) using industry standard software wiping or degaussing technology; deleting files or reformatting electronic media is not sufficient. Sensitive or Highly Sensitive information on paper should be pulped or crosscut shredded, including all transitory work products such as unused copies, drafts and notes.

Records Retention and Disposition Schedules (RRDS) should be created in collaboration with the University Archivist and maintained to document the existence of these materials and the rationale for keeping them and to help ensure their availability during the period for which they are vital as active administrative or historical records. Once the information no longer serves an active administrative or historical function according to its RRDS, it should be disposed of in a timely manner to mitigate the risk of exposure. With enterprise data, UTO and data trustees that may be impacted by the disposition of data should be consulted.

4.2.6 Breach Disclosure of Sensitive Information

If Sensitive information is breached, a legal public disclosure requirement may be triggered depending on the nature of the information and details of the breach. The party discovering the breach is responsible for notifying the Information Security Office in accordance with ASU’s Incident Response standard. Other parties may be required to be notified as well. The resulting Incident Response team will determine whether public disclosure is required and if so, the specific conditions of any disclosure. Care should be taken to preserve evidence related to the breach, as indicated in ASU’s Incident Response standard.

4.2.7 Breach Disclosure of Highly Sensitive Information

If Highly Sensitive information is breached, the result may pose a hazard to health and safety. The party discovering the breach should notify the following entities in the following order:

- ASU Police (immediately)
- Other parties identified in EHS 206, Emergency Notification
- Information Security Office, in accordance with ASU's Incident Response standard
- Other parties as required

Care should be taken to preserve evidence related to the breach, as indicated in ASU's Incident Response standard.

5 ROLES AND RESPONSIBILITIES

5.1 Data Steward

Data Stewards are senior University officials or their designees with planning and policy-level responsibility for information within their functional areas and management responsibility for defined segments of University information. The Data Steward is the individual or entity identified by law, contract or policy with responsibility for granting access to and ensuring appropriate use of the information. In the case of research information, the principal investigator is ordinarily the Data Steward except when a sponsored project award or gift might specify that the sponsor is the Steward. The responsibilities of the Data Steward include:

- Assigning, training and overseeing Data Trustees
- Overseeing the establishment of data policies in their areas
- Determining legal and regulatory requirements for information in their areas
- Ensuring that Data Trustees implement segregation of duties and rules in applicable areas
Promoting appropriate information use and information quality
Ensuring that he/she does not put his/her information at risk through his/her own actions
Assigning classification standard values to the information for which he/she is responsible
Implementing a Records Retention and Disposition Schedule for information
Working with the Information Security Office, Data Trustees and other authorized individuals on the investigation and mitigation of information security incidents/breaches affecting the integrity, confidentiality or availability of their information.
Performing information security duties as required by other University standards and practices, policies, executive orders, coded memoranda, etc.
Establishing written procedures granting and revoking access privileges

5.2 Data Trustee(s)
Data Trustees are individuals or entities with direct operational responsibility for the management of one or more types of University information. Data Trustee responsibilities include:

- Developing and maintaining information classification according to this standard
- Developing, implementing and managing information access policies
- Ensuring that data quality and data definition standards are developed and implemented
- Interpreting and assuring compliance with Federal, State and University policies and regulations regarding the release of, responsible use of and access to University information
- Coordinating and resolving issues and data definitions of data elements that cross multiple functional units
- Providing communications and education to information users on appropriate use and protection of University information
- Ensuring that access to and protection of information and the file systems that host them are in compliance with all applicable information security policies and the authorized directives of the information authority
- Ensuring that any electronic systems have all appropriate security features installed. This includes operating systems and systems software, database management systems, applications systems, computer hardware, firewalls where appropriate and communications hardware and software being administered by the information custodian/Steward
- Working with the Information Security Office, the Data Steward and other authorized individuals on the investigation and mitigation of information security incidents/breaches affecting the integrity or confidentiality of the information
- Notifying the Information Security Office in a timely manner of any perceived breach or loss of Highly Sensitive or Sensitive information
- Reviewing access requests to and use of the information, determining appropriate access and authorizing or denying the request under their authority
- Ensuring that those with access to the information understand their responsibilities for collecting, using, retaining and disposing of the information only in appropriate ways
- Monitoring usage of the information

5.3 Information User(s)
Information users are individuals who need and use University information as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Information user responsibilities include:

- Ensuring that their own actions do not put the information at risk
- Ensuring that any computer systems they use to create, access or handle the information are in compliance with ASU's Data Handling Standard.
- Notifying the Information Security Office in a timely manner of any perceived breach or loss of Highly Sensitive or Sensitive information.
5.4 Information Security Office
The Information Security Office’s responsibilities include reviewing access to Sensitive and Highly Sensitive information as needed, defining data classifications and invoking Incident Response procedures upon notification of a breach.

6 RESOURCES

6.1 Relevant ASU Resources

- Computer, Internet and Electronic Communications policy (ACD 125)
- Emergency Notification policy (EHS 206)
- Incident Response Standard
- Information Security Policy
- Records Storage and Destruction (PCS 703)
- Surplus Property (PCS 1002-01)
- Secure Web Development Standard
- ASU Data Storage Guidelines
- Web Application Security Standard
- Office of Research Integrity and Assurance – Human Subjects Research

6.2 Relevant Legislation and Regulations

- Federal Educational Rights and Privacy Act (FERPA)
  - Final Regulations
  - Educause resources on FERPA

- Health Insurance Portability and Accountability Act (HIPAA)
  - Understanding HIPAA Privacy (for Covered Entities), US Department of Health & Human Services
  - US Departments of Education and Health & Human Services Joint Guidance on the Application of FERPA and HIPAA to Student Health Records
  - Educause resources on HIPAA

- Health Information Technology for Economic and Clinical Health (HITECH) Act

- Gramm-Leach-Bliley Act (GLBA)
  - Federal Trade Commission (FTC) on GLBA
  - Educause resources on GLBA

- State Security Breach/Notification Laws
  - ARS § 44-7501
  - Commercial Law League of America’s matrix on all states
  - Educause resources on data breach notification

- Payment Card Industry Data Security Standard (PCI DSS)
  - PCI Security Standards Council's summary and supporting documents

- Red Flags Rule Legislation
  - www.ftc.gov
7 STANDARD REVIEW AND REVISION

This standard is subject to review and revision at the direction and approval of the Chief Information Security Officer. To offer suggestions and/or recommendations, contact the Information Security Office at infosec@asu.edu.

Last Review

This standard was reviewed and revised in October 2013. This version supersedes all previous versions.

Interim Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revised by</th>
<th>Nature and purpose of revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/15/2013</td>
<td>Susan Moore</td>
<td>Updates to terminology, etc.</td>
</tr>
</tbody>
</table>
APPENDIX - EXAMPLES OF DATA CLASSIFICATIONS

The following list is not exhaustive or comprehensive. If you have a question about a specific data type and/or are uncertain how it should be classified contact, please contact the Information Security Office.

Public

Public Relations Information includes:
- University Web site content intended for external consumption
- Press releases
- Public events calendars

Public Disclosure Required include:
- Annual disclosure statements
- Other information the University is required by law to disclose

University Research includes:
- Existing data from any public source
- Anonymously recorded data posing no harm to participants as determined by the Institutional Review Board
- Data from public sources on elected officials

Employee Information includes:
- Affiliate ID
- ASURITE UserID (do not list in a public or a large aggregate list, protection of spam)
- Employee title
- Employee public email address
- Employee work location and telephone number
- Employing department
- Employee classification
- Employee gross salary
- Name (first, middle, last) (except when associated with protected information)
- Signature (non-electronic)

Internal

Financial Information includes:
- Financial budget information
- Purchase order information

Student (and former student) Information (Directory Information) includes:
- ASURITE UserID (do not list in a public or a large aggregate list, protection of spam)
- Name
- Major Field of Study
- Participation in officially recognized sports/activities
- Weight and Height of athletic team members
- Dates of Attendance
- Full or Part-time status
- Degrees and awards received
- Campus electronic mail address
- Most recent or previous college/university/agency attended

Student prospects and Applicants
• Information about student prospects and student applicants doesn’t appear in the online directory

Other Affiliates

• Some courtesy affiliates appear in the online directory. Only title, company, and business information will appear.

Other Information includes:
• Non-ASURITE login credentials
• Encrypted or hashed login credentials
• Details of information security vulnerabilities not related to campus law enforcement operations

Sensitive

Identity Validation Keys
• Birth date (full: mm-dd-yy)
• Birth date (partial: mm-dd only)

Personally Identifiable Information (PII)
• Unencrypted ASURITE login credentials
• PINs (Personal Identification Numbers)
• Birth date combined with last four digits of SSN
• Tax ID
• Driver’s license number, state identification card number, and other forms of national or international identification
• Social Security number
• Mother’s maiden name

Employee Information
• Home or mailing address
• Biometric information (e.g.: fingerprint, voice recording, palm print, iris scan, DNA)
• Birthplace (City, State, and if not USA, Country)

Financial Information
• Credit card numbers with cardholder name
• Bank account or debit card information

Health & Insurance Information
• Medical records related to an individual
• Psychological Counseling records related to an individual
• Speech and Hearing records

Law Enforcement Information
• Law Enforcement Records related to an individual
• Vulnerability/security information related to campus law enforcement operations

Library Information
• Registration records related to an individual patron information
• Circulation records related to an individual borrowing particular books and material

Employee Information
• Employee net salary
• Employment history
• Personal telephone numbers
• Personal email address
• Parents and other family members' names
• Emergency contact names and telephone numbers
• Payment history
• Employee evaluations
• Background investigations
• Electronic or digitized signatures
• Private key (digital certificate)
• Ethnicity
• Gender
• Marital status
• Personal characteristics (e.g., hobbies)
• Physical description
• Photograph

University Research
• Research proposals, protocols, and disclosures
• Research data posing no financial, emotional, or criminal harm to participants, with no link to individual identities

Student Information
• Educational records of individual students (Excludes directory information such as name mailing address, preferred telephone listing, e-mail address, major, etc. Refer to specific FERPA information for details about directory information.)
• Student identification - home or mailing address
• Personal telephone numbers
• Personal email address (excludes ASURITE username@asu.edu)
• Ethnicity
• Gender
• Birthplace
• Grades
• Courses taken
• Schedule
• Test Scores
• Advising records
• Educational services received
• Disciplinary actions
• Non-directory student information may not be released except with Office of the Registrar’s approval and only under certain prescribed conditions.

Facilities Information
• Building plans and architectural drawings

Legal Information
• Legal investigations conducted by the University
• Settlements and claims against the University
• Accident reports and investigations

Library Patron Information
• Linking a library user with the specific subject which the library user has requested information or materials.
Purchasing and Accounts Payable Information
• Sealed bids prior to award
• Identifiable information (purchase order) of the supplier/company

University Donor Information
• Name
• Home or mailing address
• Personal telephone numbers
• Personal email address
• Donation if request is for anonymous gift/donation

Highly Sensitive

Secret Legal
• Active legal dispute between ASU and an employee over an HR matter

University Research
• Classified research requiring facility security clearance oversight
• Human subjects research determined by the IRB to pose criminal, financial, or emotional harm
• Research data subject to a federally approved Certificate of Confidentiality
• Research involving vulnerable populations as determined by the IRB
• Vertebrate animal research with designated species
• BSL3, ABSL3, and Select Agent related research
• Misconduct in Research investigations and Conflict of Interest questionnaires and disclosures
• Internal review records of the Office of Research Integrity and Assurance
• Coded private data with links to individual identities in research protocols and disclosures
• Confidential or sponsor-proprietary information
• Export controlled research information, software, deemed exports and equipment
• Space and building door and data access to Select Agent areas (Per CDC and Department of Health and Human Services)