Purpose
ASU's Information Security Policy requires controls to manage risks to the confidentiality, availability, and integrity of University information. This standard defines the controls required for handling all University managed information. These required controls represent a minimum standard for protection of University information. Additional controls required under applicable laws, rules and 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 all data including Sensitive and Highly Sensitive data.

Applicability
This Standard applies to all users of ASU’s computing, internet, and communications resources, including all students, faculty, staff (including student employees), courtesy affiliates, contractors, vendors, consultants, temporary and other workers for ASU and Component Units (Users). This standard applies to all information handled by University employees, and University affiliates, contractors and vendors. Each such entity and individual who creates, collects, records, organizes, stores, adapts, alters, retrieves, uses, processes, has access to, transfers, discloses, 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 prospective, current, and former students, and employees, and other University affiliates, research data, and intellectual property.

Contents
Data Classification Levels
Standard
Roles and Responsibilities
Violation and Enforcement
Resources
Appendix
Standard Revision

Data Classification Levels
See appendix for detailed examples of data in each classification.

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.

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 without specific University authorization, contract, or good reason. Unauthorized disclosure, compromise or destruction would have little to no adverse effect on the University's students, faculty, or staff, or its operations, assets, reputation or obligations concerning information privacy.

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 Family Education Rights and Privacy Act (FERPA), protected health information (PHI) according to Health Insurance Portability and Accountability Act (HIPAA), personal data of data subjects in the European Union according to the Global Data Protection Regulation (GDPR), confidential financial information according to Gramm Leach Bliley Act (GLBA), payment card information protected by the Payment Card Industry (PCI), personally...
identifiable information (PII) according to state and federal laws and industry regulations or control systems related to critical infrastructure, and information regulated by applicable international privacy laws, rules and regulations.

Unauthorized disclosure, compromise, or destruction would directly or indirectly have an adverse impact on the University, its students, faculty, staff or University affiliates. 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.

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, faculty, staff, 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.

Standard

Public and Internal Information

Confidentiality and privacy 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, availability, and integrity of Internal information. These measures include:

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

Sensitive and Highly Sensitive Information

Creation and Identification

The following controls are required when Creating and Identifying Sensitive or Highly Sensitive information:

- Records should exist only in areas where there is a legitimate and justifiable business need, as authorized by the appropriate Data Steward or Deputy Data Steward.
- When at all possible, data should be accessed from its original source, should not transmitted or shared, and copies or printed versions of the information should be kept to a minimum.
- 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.
- 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 accordance with the University’s Records Storage and Destruction policy (PCS 703) 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 to active administrative or historical records. Once the information no longer serves an active administrative or historical function according to its RRDS, it should be destroyed in a timely manner to mitigate the risk of exposure.

Access

The following controls are required when accessing Sensitive or Highly Sensitive information:

- Access shall be granted only to individuals or entities that are authorized by the appropriate Data Steward or Deputy Data Steward.
- Employees should receive annual training on their responsibilities regarding appropriate use and steps they can take to protect Sensitive and Highly Sensitive information.
- Any other use, access to, or disclosure requires the written approval of the appropriate Officer of the University or Data Steward, in consultation with the Office of General Counsel as necessary.
- The list of people and entities with access to this data should be reviewed on an annual basis to ensure that access is still needed. Evidence of an annual review of their access shall be made available to the Information Security Office on request.
Use, Transmission, and Storage

The following controls are strongly recommended when using, transmitting, or storing Sensitive or Highly Sensitive information:

- Consider applicable laws, rules, and regulations may impose additional requirements.
- Do not discuss or display information 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 individuals.
- When printing, photocopying or faxing, ensure that only authorized personnel will be able to see the output. 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 applicable Data Steward or Deputy Data Steward.
- Sensitive identity and financial information such as SSN or bank account information stored in electronic or paper. Documents should be masked or redacted unless there is a business reason to store the information. This includes removing this information from non-production test systems.
- Store source code and documentation of critical control systems related to critical infrastructure in a secure location.
- Share data only with individuals who have completed appropriate training and have access to the level of data being shared. Once access level has been confirmed, clearly identify the data by labeling it as Sensitive or Highly Sensitive. If data needs to be shared with an individual or entity (such as a vendor or contractor) that does not have access, the Data Steward or Deputy Data Steward must approve prior to information being shared.
- Store data in a secure location. Encrypt information at rest, and in transit using an industry standard encryption algorithm.
- All new systems are to be implemented with full-disk encryption. Existing systems accessing the ASU network, or containing this data must also be fully encrypted, or an encryption conversion plan must be filed and accepted by the Information Security Office as InfoSec@asu.edu.
- Do not send 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 this data.
- Applications that process this data should comply with the Secure Web Development Standard, Web Application Security Standard, and all other applicable information security standards.
- When at all possible, information should be accessed from its original source, and electronic copies or printed versions of the information should be kept to a minimum.
- If information must be stored outside its original source, refer to the ASU Data Handling Matrix for appropriate options.
- When contracting with a third party for data use, processing, or storage, the college or departmental unit is responsible to follow the ASU Data Storage Guidelines, as well as ensure, on an annual basis, that security and privacy contract requirements are met, including reviewing key security reports from the vendor.

Transport

The following controls are required when transporting or transmitting 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 Steward or Deputy Data Steward for specific handling restrictions.
- When sending the information by campus mail in non-electronic form, the sender should consult with the appropriate Data Steward or Deputy Data Steward 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, and the devices are encrypted.
- Do not remove from an approved secure location or device without prior approval of the Data Steward or Deputy Data Steward.

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 accordance with the University's Records Storage and Destruction policy (PCS 703) and maintained to document the existence of 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 destroyed in a timely manner to mitigate the risk of exposure. With enterprise data, UTO and the appropriate Data Steward or Deputy Data Steward should be consulted.

**Breach Disclosure of Sensitive Information**

If Sensitive information is, or is suspected of being, breached, disclosed without authorization, or lost, a legal public disclosure requirement may be triggered. The University party discovering any actual, suspected, possible, or potential breach, unauthorized disclosure, or loss of Sensitive information is responsible for timely notification to the Information Security Office in accordance with ASU's [Incident Response Standard](mailto:InfoSec@asu.edu). 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.

**Breach Disclosure of Highly Sensitive Information**

If Highly Sensitive information is or is suspected of being breached, disclosed without authorization, or lost the result may pose a hazard to health and safety. The University party discovering any actual, suspected, possible, or potential breach, unauthorized disclosure, or loss of Highly Sensitive information should notify the following entities in priority order:

- ASU Police (immediately)
- Other parties identified in EHS 206, Emergency Notification
- Information Security Office, in accordance with ASU's [Incident Response Standard](mailto:InfoSec@asu.edu)
- Other parties as required

Care should be taken to preserve evidence related to the breach.

**Roles and Responsibilities**

**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. Each Data Steward is charged by law, contract or policy with responsibility for protecting, granting access to and ensuring appropriate use of a specific category of University 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 research sponsor is the Steward. The responsibilities of each Data Steward include:

- Assigning, training and overseeing one or more Deputy Data Stewards
- Overseeing the establishment of data retention, privacy, security, and other data-related policies in their areas
- Identifying legal and regulatory requirements for information in their areas
- Ensuring that Deputy Data Stewards 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, Deputy Data Stewards and other authorized individuals on the investigation and mitigation of suspected, potential, possible, and actual information security incidents/breaches/disclosures/losses affecting the confidentiality, privacy, availability, or integrity of their information.
- Performing information security and privacy duties as required by other University standards and practices, policies, executive orders, coded memoranda, etc.
- Establishing written procedures granting and revoking access privileges
Deputy Data Steward

Deputy Data Stewards are individuals or entities with direct operational responsibility for the management of one or more types of University information. Deputy Data Stewards’ 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 applicable, laws, rules, regulations, and University policies, standards, and guidance, 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 information are in compliance with all applicable information security and privacy policies and the authorized directives of the information authority
  - 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 confidentiality or integrity 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 with respect to information under their authority
  - Ensuring that those with access to the information understand their responsibilities for collecting, using, sharing, processing, transmitting, storing, retaining and disposing of the information only in appropriate ways
  - Monitoring usage of the information

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 systems they use to create, access, process, transmit, use, store, destroy or handle data comply with ASU’s Data Handling Standard.
- Timely notification to the Information Security Office of any actual, suspected, possible, or potential breach, unauthorized disclosure, or loss of Highly Sensitive or Sensitive information.

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.

Violations and Enforcement

Enforcement may include removal of systems from the ASU network or removal of access privileges to ASU’s computing, Internet and communication resources, until requirements are met. Violations of this Standard may lead to disciplinary actions or contract termination as applicable.

In a circumstance where compliance may not be immediately possible, the ASU academic or business units must confer with the Information Security Office to develop a plan for moving into compliance within a reasonable amount of time.

Resources

Relevant ASU Resources

- IT Policies and Standards
- ASU Merchant Services
- ASU Data Storage Guidelines
- Computer, Internet and Electronic Communications policy (ACD 125)
- Data Governance Guideline
● Emergency Notification policy (EHS 206)
● GDPR Guidance & Training
● General Workstation and Server Security Practices
● Get Protected GDPR Compliance Guidelines and FAQs
● Incident Response Standard
● Information Security Policy
● Office of Research Integrity and Assurance – Human Subjects Research
● Records Storage and Destruction (PCS 703)
● Secure Web Development Standard
● Surplus Property (PCS 1002-01)
● Secure Web Development Standard
● Web Application Security Standard
● GSA Rules and Policies – Protecting PII - Privacy Act

Relevant Legislation and Regulations

● ABOR Policy
  ○ Arizona Board of Regents Policy 9-201 (General Policy)
  ○ Arizona Board of Regents Policy 9-202

● Arizona Revised Statutes
  ○ ARS §15-1823 (Identification numbers; social security numbers)
  ○ ARS §44-1373 (Restricted use of personal identifying information; civil penalty)

● Canada’s Anti-Spam Law (CASL)

● 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

● Children’s Online Privacy Protection Act
  ○ Children’s Online Privacy Protection Rule

● Global Data Protection Regulation for the European Union (GDPR)
  ○ ASU European Union Supplement
  ○ GDPR Regulation

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

● State Security Breach/Notification Laws
  ○ ARS § 18-541 ARS § 18-552
  ○ Educause resources on data breach notification

● Payment Card Industry Data Security Standard (PCI DSS)
  ○ PCI Security Standards Council’s summary and supporting documents
Appendix

Examples of Data Classifications
The following list is a list of examples and is not intended to be exhaustive or comprehensive. Please Note: Privacy laws are changing internationally and within the United States. Please understand your data elements and any applicable laws. The items below are for reference only.

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

Public Disclosures Requirements 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 (Also known as the PeopleSoft EMPLID)
- ASURITE User ID (do not list in a public or a large aggregate list, protection of spam)
- Employee title
- Home or mailing address
- Employee public email address
- Employee work location and telephone number
- Employing department
- Employee classification
- Employee gross salary
- Employment dates
- Name (first, middle, last) (except when associated with protected information)
- Signature (non-electronic)

Access to ASU faculty and staff data and records is governed by ABOR Policy 6-912, ACD 811, SPP 1101, and Arizona law.

Student (and former student) Information
- ASURITE User ID (do not list in a public or a large aggregate list, protection of spam)

Internal
Financial Information includes:
- Financial budget information
● Purchase order information
● Personal, non-ASU email address

Student Prospects and Applicants
● Information about student prospects and student applicants doesn’t appear in the online directory
● Affiliate ID (Also known as the PeopleSoft EMPLID) when stored and/or processed only for ASU Single Sign On (SSO)

Student
● Affiliate ID (Also known as the PeopleSoft EMPLID) when stored and/or processed only for ASU Single Sign On (SSO) unless otherwise protected by a FERPA hold, the GDPR, or similar privacy laws
● Student (and former student) Information - Releasable information per Student Services Manual SSM107-01 unless otherwise protected by a FERPA hold, the GDPR, or similar privacy laws
● Please note due to the sensitivity of some data elements, ASU has classified some as sensitive as noted in later sections of this appendix, such as DOB.
● FERPA is one law that provides direction for educational data of individuals in the USA, Other state and international laws, rules, and regulations could further restrict what personal data may be disclosed.
● Student – Non-directory student information may not be released except with Office of the Registrar’s approval and only under certain prescribed conditions.

Other Affiliates
● Non-ASU directory courtesy affiliate data. Typically, the directory is limited to title, company, and business information unless otherwise protected by the GDPR, or similar privacy law.

Other Information
● 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)
As identified in ARS § 18-551
● The individual’s social security number.
● The individual’s number on a driver license issued pursuant to ARS § 28-3166 or number on a non-operating identification license issued pursuant to ARS § 28-3165.
● The individual’s financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual’s financial account.
● An individual’s username or email address, in combination with a password or security question and answer, that allows access to an online account.
● A private key that is unique to an individual and that is used to authenticate or sign an electronic record.
● An individual’s health insurance identification number.
● Information about an individual’s medical or mental health treatment or diagnosis by a health care professional.
● An individual’s passport number.
● An individual’s taxpayer identification number or an identity protection personal identification number issued by the United States internal revenue service.
● Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account.

Sensitive PII also means any information relating to or about any specific individual or groups of individuals protected from disclosure under the Family Educational Rights and Privacy Act of 1974 (FERPA) or the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or any other applicable Global, Federal, State or local statute, law, rule or regulation.
GDPR (Global Data Protection Regulation) Personal Data - Any information, recorded in any form, relating to a natural person in the European Union, or other jurisdiction with similar privacy laws, that was submitted to ASU (or another entity that submitted it to ASU) while the person was in the European Union, that can identify the person, directly or indirectly, such as a name, date of birth, address (including email address), identification number, location data, online identifier, or factors specific to the person’s physical, physiological, genetic, mental, economic, cultural, or social identity.

GDPR – Special Category Data - GDPR personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of a natural person, and GDPR personal data that is genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or data concerning a natural person’s sex life or sexual orientation.

Financial Information
- Credit card numbers with or without extra data such as cardholder name, security codes, track data
  - When ASU is the Merchant this is sensitive PCI data.
  - When ASU is the customer (internal ASU Purchasing cards) this is sensitive, but not PCI data.
- 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
- Biometric information (e.g., fingerprint, voice recording, palm print, iris scan, DNA)
- Birthplace (City, State, and if not USA, Country)
- 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. Releasable information per Student Services Manual SSM107-01
- **Affiliate ID** (Also known as the PeopleSoft EMPLID) when shared and/or stored for purposes other than ASU Single Sign On (SSO)
- 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
- Control systems related to critical infrastructure including building control systems not already considered highly sensitive. (Electrical power, Gas, Oil Storage, Water Supply, HVAC etc.)

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 (including 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

Critical Control Systems
- Control systems related to critical infrastructure, including building control systems, that maintain life safety or materials that may become hazardous if environment is changed.

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, ABL3, 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)

Export Controlled Research -
- ITAR (import/export defense related technical data or foreign students)

**Standard Revision**

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