UADA Policy 920.1
Data Lifecycle and Management Policy/Procedures

Purpose

The purpose of this policy is to outline the method of categorizing data assets based on risk to the University of Arkansas System, Division of Agriculture (UADA) and establish specific minimum standards for data handling across the UADA system. This includes ensuring that necessary UADA records and documents are adequately protected and maintained and that records no longer needed for organization purposes are discarded appropriately. This policy also ensures that UADA manages data consistently and appropriately and assigns responsibilities and roles that are applied to data governance and to aid employees of UADA in understanding their obligations in retaining and destroying either physical (paper) or electronic documents - including email, text files, digital images, sound and movie files, PDF documents, and all Microsoft Office or other formatted files or paper documents.

Scope

This policy applies to UADA employees, faculty, staff, temporary employees, students, contractors, vendors, volunteers, and other personnel responsible for owning and managing UADA records and documents in either paper or electronic formats. This also applies to all UADA data, and all other individuals and entities granted use of UADA information.

Definitions

Confidential Information: Information concerning UADA research projects, confidential employee information, information concerning the UADA research programs, proprietary information of UADA, sign-on and password codes for access to UADA computer systems, and Protected Health Information.

Data Inventory: A detailed record of the data maintained by UADA.

Data Owner: The data owner is the subject of the data (i.e., the student). If the data is not a subject, the data owner is the creator of the data or legally specified owner of the data.

Data Steward: An individual who has direct responsibility to ensure that a data domain is classified appropriately.

Data User: Individuals who need and use UADA data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals given access to sensitive data have a position of special trust and, as such, are responsible for maintaining the confidentiality, integrity, and availability of that data.

Compensating Control: A data security measure that is designed to satisfy the requirement for some other security measure that is deemed too difficult or impractical to implement and that meets the intent and rigor of the original control.

Institutions: All local and remote offices and program areas, UADA Shared Services, and UADA Administration.

UADA Data: Data, in any form (electronic, physical, or otherwise), including but not limited to data created, used, or stored in pursuit of UADA's mission.

Policy

UADA is committed to a secure information technology (IT) environment supporting its mission. Data management begins with the creation or collection of data and continues through the entire lifecycle, which includes data inventory, data classification, and data protection.

The data inventory process consists of identifying and recording basic information about data in your custody, such as data owner, data format, record category and retention, storage, access, transfer, the purpose of processing, etc.

A data inventory is valuable because it provides information on what data you have, where it's located, and who has access to it. Data Inventory also helps identify information that must be safeguarded under requirements of laws (e.g., FERPA, HIPAA, GLBA), regulations (e.g., GDPR), industry standards, and UADA requirements and policies. A thorough data inventory also helps facilitate data incident investigation and disclosure/breach containment.

To establish the safeguards required for particular types of data, it is necessary to determine the level of risk associated with the data. Data classification assigns such levels and determines the extent to which technical, administrative, and physical controls should be applied to protect the data from theft, alteration, loss of integrity, and/or misuse. Proper data security handling must be implemented commensurate with the sensitivity of the data and the risk to UADA. This ensures appropriate protection from threats to the confidentiality, integrity, and availability of UADA data.

These procedures establish a minimum baseline for data handling on all current and future systems. It may be permissible to substitute a compensating control for a particular item below, provided it meets the rigor and intent of the original control. Compensating controls shall be documented in writing and submitted by the Director of Information Technology for AES and CES (DIT) and to the Associate VP (AVP) for review. If there are any concerns, the DIT and the AVP will engage with subject matter experts as needed. Upon recommendation by the AVP, in concurrence with the DIT, the compensating control will be routed to the Senior Assoc VP for UADA for approval.

Data may be classified as:

- High Risk (Sensitive): if compromised or destroyed in an unauthorized transaction, would have a catastrophic impact on the organization or individuals. For example, financial records, intellectual property, and authentication data.
- Medium Risk (Restricted): intended for internal use only, but if compromised or destroyed, would not have a catastrophic impact on the organization or individuals. For example, emails and documents with no confidential data.
- Low Risk (Public): intended for public use. For example, public website content

The Data Steward(s) shall evaluate and classify data for which he, or she, is responsible according to the definitions in this policy and the standards specified in this policy.

All information shall be kept, in a manner, consistent with appropriate controls and standards commensurate with its data classification and the protections outlined in this policy.

Information shall also be maintained according to the Record Retention Policy and applicable state and federal laws and regulations.

Data may contain elements from multiple classifications (i.e., data sets). The composition of these data sets may result in either a High or Medium Risk data classification. In these cases, protections prescribed by federal law will take precedence.

This policy also defines the UADA record retention and destruction schedule for paper and electronic records. The Electronic and Paper File Retention Guide is approved as the initial maintenance retention and disposal schedule for the physical (paper) and electronic records of UADA. The Chief Financial Officer (CFO) is responsible for the administration of

this policy and the implementation of processes and procedures to ensure that the Electronic and Paper File Retention Guide is implemented within UADA record and document handling processes. General Counsel is authorized to; make modifications to the Electronic and Paper File Retention Guide as needed to ensure that it follows state and federal laws; ensure the appropriate categorization of documents and records on behalf of the UADA; annually review the policy and monitor university compliance with this policy. This policy applies to all physical (paper) and electronic records generated in the course of the UADA operations, including both original documents and reproductions. UADA records must be retained and destroyed according to the defined schedule in either paper or electronic formats.

No one person or unit can be directly responsible for all UADA Records. Therefore, every office or department managing UADA records is responsible for:

- Implementing records management practices consistent with this Policy.
- Educating staff in Records management practices.
- Preserving Records as required under this Policy.
- Properly disposing of Inactive Records at the end of the applicable retention period.
- Protecting Records against misuse, misplacement, damage, destruction, or theft.
- Monitoring compliance with this Policy.

Procedures

Data Stewards

These standards establish a minimum baseline for data inventory and classification across UADA. Each institution shall identify a qualified Data Steward(s) for all data sets controlled by the group or department. For the purpose of these standards, it is the responsibility of the Data Steward to work with Information Technology, Financial Services, and Human Resources to ensure that the data is classified appropriately.

- Each institution area shall provide training for their data stewards to ensure they understand their responsibilities and to enhance the consistent classification of data.
- Each data steward must identify the major system(s) where their data resides, classify those systems according to the classifications defined in this policy, document this classification in an electronic format, upload the document to a designated cloud folder, and implement appropriate controls.
- Data covered by the Family Educational Rights and Privacy Act (FERPA) may contain elements from multiple classifications (i.e., data domains). The composition of these data domains may result in either a moderate or high-risk data classification. In these cases, protections prescribed by federal law will take precedence.
- Data Steward(s) shall review data classification(s) at least annually (365 days).

Data Inventory

The Data Inventory Template (xlsx) should be used to capture all relevant information about your data. Upon completing the data inventory, follow the guidance in the Data Classification section to determine if you have Regulated information in your custody.

Data Stewards are required to review their data inventory periodically and at least bi-annually to determine if there have been any material changes, such as changes to a record category, storage location, or access to data in the custody of that unit.

Data Stewards should submit their completed Data Inventory to the Division Security Team at division-it-security-team@uada.edu and promptly inform the Division Security Team if there are changes to their regulated data inventory.

For assistance with completing or reviewing your data inventory, contact the Division Security Team.

Data Element Classifications

High Risk (Sensitive) data:

Information and technology that is regulated by federal, state, or local legislation, regulations, or industry standards. It may include contractual obligations: access, use, transmission, or management of restricted data as outlined in the applicable regulation.

Examples of High Risk (Sensitive) data are:

- (HIPAA) Protected Health Information and health insurance policy ID numbers
- (HHS 45 CFR part 46) Sensitive identifiable human subject research data.
- (FERPA) - student data including but not limited to grades, exams, rosters, official correspondence, financial aid, scholarship records, enrollment, etc.
- (GDPR) General Data Protection Regulation
- (GLBA) -Student Loan Application Information
- (PCI-DSS) Credit card/E-Commerce data, debit cards
- (DFARS) Data subject to Defense Federal Acquisition Regulation Supplement or (FAR) Federal Acquisition requirements Export controlled information
- (ITAR) International Traffic in Arms Regulations
- (EAR) Export Administration Regulations
- (CUI) Controlled Unclassified Information
- (CTI) Unclassified Controlled Technology Information
- Attorney-client privileged information
- Audit working papers that pertain to highly sensitive audits
- Business process that pertains to security practices
- Detailed building plans and other infrastructure diagrams and data, e.g., Server rooms and floor plans, Building blueprints, HVAC systems, and electrical wiring.
- Donor records and work products (records compiled and maintained by University Advancement)
- Biometric identifiers, including finger and voice prints
- Certain contractual obligations
- Employment file/ HR Data
- Financial account numbers (bank account, investment account, etc.)
- Law Enforcement records- background checks /arrest records
- Personally Identifiable Information (PII), including SSN, passport numbers, visa numbers, other national ID numbers, and driver's license numbers
- Passwords/PINs
- Research Data before publication, governmental research, intellectual property
- Subpoena, National Security inquiry, FISA request, and other court orders
- Tax information (W-2, W-4, 1099, etc.)
- Trade secrets or proprietary information which the University of Arkansas, by choice, contract, or other agreement, identified for confidentiality.
- Other data covered by federal and/or state confidentiality laws

Medium Risk (Restricted) data:

Medium Risk (Restricted) data is information that is not intended to be shared with the public. Medium Risk (Restricted) data should not be disclosed outside of UADA without the permission of the person or group responsible for the data.

Examples: By way of illustration only, examples of Medium Risk (Restricted) data are, but are not limited to:

- Business partner information where no more restrictive confidentiality agreement exists
- Certain contractual obligations not specifically classified as High Risk (Sensitive) data.
- Data related to unpublished research that is not subject to the Common Rule (de-identified data) or not in the High Risk (Sensitive) data Category.
- Embargoed news items
- Information related to university operations, finances, contracts, legal matters, audits, or other activities that are not public in nature
- Internal memoranda, emails, and reports
- Library user records
- Research Data before publication, governmental research, intellectual property
- Technical documents such as system configurations of information systems or processes.
- Other data where the risk to the affected parties reaches the level of harm defined in Medium Risk (Restricted) data

Low Risk (Public) data:

Low Risk (Public) data includes data where unauthorized disclosure or loss poses a low risk or impact to the organization or its affiliates. Public data is information to which the general public may be granted access per UADA policy or standards.

Examples: By way of illustration only, some examples of public data include, but are not limited to:

- Course catalogs and timetables
- Directory information
- Brochures, maps, magazines, newsletters, newspapers, and magazines.
- Institutional statements and other reports filed with federal or state authorities and generally available to the public.
- Press releases
- Public donations
- Schedules of classes

Data Handling and Control Areas

1. Access Controls (incl. Request for Data Access)

   Low Risk (Public) data

   - Access to modify public data must use authentication methods that meet the requirements of this policy, and its associated procedure.

   Medium Risk (Restricted) data

   - Access to view or modify is restricted to authorized individuals.
   - Remote access by the third party for technical support is limited to authenticated and authorized access via secure protocols

   High Risk (Sensitive) data

   - Access is limited to end users and administrators who have been designated by the appropriate Data Steward or similar position.
   - Remote access by a third party for technical support is limited to authenticated and authorized access via secure protocols.
   - Authorization and authentication are required for access.

- Multi-factor authentication is required.
- Confidentiality requirements must be established and disseminated to appropriate parties.
- Data must be encrypted in transit and at rest.

Copying/Printing/Transmission

Low Risk (Public) data

- No restrictions.

Medium Risk (Restricted) data

- Data distribution must be limited to individuals whose role requires access to the data domain and who have the authorization to access the data domain.

High Risk (Sensitive) data

- Data distribution must be limited to as few individuals as feasible whose role requires access to the data domain and who have the authorization to access the data domain.
- Hard copies must not be left unattended and must be stored in a secure location.
- Data must be encrypted in transit and at rest, and all parties must be authenticated.

Network Security

Low Risk (Public) data

- No restrictions.

Medium Risk (Restricted) data

- Defense in depth must be used, with the following controls:
  1. Network firewall protection, including port restriction, protocol restriction, or IP address Access Control Lists (ACL)
  2. Single-factor authentication, such as username/password

High Risk (Sensitive) data

- Defense in depth must be used, including two of the three following controls:
  1. Network firewall protection, including port restriction, protocol restriction, or IP address Access Control Lists (ACL)
  2. Multi-factor authentication, such as username/password
  3. Comprehensive intrusion detection and intrusion prevention, including advanced logging of all attempted access to network resources, or Advanced Threat Protection (ATP)
- Network access to a system or server hosting the data must be limited to the minimum necessary.

IT Data Center Security

Low Risk (Public) data

- No restrictions

Medium Risk (Restricted) data

- Data will be stored in an institution or UADA-System-provided cloud storage service or data center.
- If data are stored on file shares/servers, NAS, or attached storage, encryption is required.

- All devices that access high-risk data must be managed in an institution or UADA-System-approved manner.

High Risk (Sensitive) data

- Data will be stored in an institution or UADA-System-provided cloud storage service or data center.
- If data are stored on file shares/servers, NAS, or attached storage, encryption is required.
- All devices that access high-risk data must be managed in an institution or UADA-System-approved manner.

System Security

Low Risk (Public) data

- No restrictions.

Medium Risk (Restricted) data

- System administrators shall follow any system security procedures established by the institution as well as operating system-specific best practices for system management and security.

High Risk (Sensitive) data

- System administrators shall follow any system security procedures established by the institution as well as operating system-specific best practices for system management and security.
- Protection with a firewall is required.
- Data at rest must be encrypted.

Physical Security

Low Risk (Public) data

- No restrictions.

Medium Risk (Restricted) data

- Hardcopy files must be properly marked and stored in a locked cabinet.
- System must be locked or logged out when unattended.

High Risk (Sensitive) data

- Data must be masked from a casual view to prevent unauthorized access.
- Hardcopy files must be properly marked and stored in a locked cabinet.
- System must be locked or logged out when unattended.
- Storage must be in a secured location.

Data Storage

Low Risk (Public) data

- No restrictions

Medium Risk (Restricted) data

- Data must be stored in an institution or UADA-System-provided cloud storage service or data center.

- Individuals and departments should not select storage providers or technologies without institution or UADA approval.
- Hard copies must not be left unattended and must be stored in a secure location.

High Risk (Sensitive) data

- Data must be stored in an institution or UADA-System-provided cloud storage service or data center.
- Individuals and departments should not select storage providers or technologies without institution or UADA approval.
- If data are stored on an individual workstation or mobile device, encryption is required.
- Hard copies must not be left unattended and must be stored in a secure location.
- All devices that access high-risk data must be managed in an institution or UADA-System-approved manner.

Backup/Disaster Recovery

Low Risk (Public) data

- Regular backup is required, and recovery is periodically tested.
- Backup media must be encrypted and stored in a secure location.

Medium Risk (Restricted) data

- Regular backup is required, and recovery is periodically tested.
- Backup media must be encrypted and stored in a secure location.

High Risk (Sensitive) data

- Regular backup is required, and recovery is periodically tested.
- Backup media must be encrypted and stored in a secure location.

Media Sanitization and Disposal

Low Risk (Public) data

- No restrictions.

Medium Risk (Restricted) data

- Must securely destroy or use bonded disposal service.

High Risk (Sensitive) data

- Must securely destroy or use bonded disposal service.

Workstation and Mobile Devices (incl. personally owned devices)

Low Risk (Public), Medium Risk (Restricted) data

- Password protection and an inactivity auto-lock are required.
- Employees shall remove UADA data from their personally owned devices before the devices are discarded or replaced or before the individual is discharged from employment with the UADA.

High Risk (Sensitive) data

- Password protection and an inactivity auto-lock are required.

- Data considered high risk is not allowed on mobile or personally owned devices. There are no exceptions to this.

Record and Document Destruction

Per applicable state and federal laws and the UADA Data Classification, Handling, and Protection Policy, any documents containing personal or confidential information should be destroyed so that the information cannot be practically read or reconstructed. For physical (paper) documents, personal or confidential data should be destroyed with a cross-cut shredder. For electronic documents, personal or confidential data should be destroyed with the appropriate software for overwriting electronic data, disk degaussing technology, or through other means of physical destruction where the information cannot be practically read or reconstructed. For complete details of what is considered personal or confidential data, please refer to the UADA Data Classification, Handling, and Protection Policy.

Suspension of Record and Document Destruction Schedule

If the organization is served with a subpoena or request for documents, or any employee becomes aware of a governmental investigation or audit concerning the organization or the commencement of any litigation against or concerning UADA, such employee shall inform General Counsel, and any further disposal of documents shall be suspended until the General Counsel determines otherwise. General Counsel shall take such steps as is necessary to promptly inform appropriate staff of any suspension in the further disposal of documents. Upon notice from General Counsel, the email data of the individual(s) in question will be made available for legal holds; automatic email archiving for the individual(s) in question will be turned off, and all the necessary legal holds will be applied to the individual's email. Once the litigation is terminated or settled, General Counsel will notify the appropriate individuals so that the legal hold and archiving can be turned back.

Accountability and Contacts

Violation of this policy may subject the user to sanctions, including the loss of computer and/or network access privileges, disciplinary action, dismissal, and/or legal action. When applicable, UADA will report violations to the appropriate authorities.

The Directors of Information Technology for UADA are charged with the responsibility to review the policy and propose changes as needed periodically.

References

UADA-Data Classification and Protection Chart
UADA Data Classification, Handling, and Protection Policy
The Electronic and Paper File Retention Guide

Revision Dates:

December 12, 2022