**University of Alabama at Birmingham**

**STANDARD FOR RESEARCH DATA SECURITY REQUIREMENTS**

Approved and Implemented: February 22, 2017

Reviewed/Updated: June 28, 2021

**Related Policies, Procedures, and Resources**

* **Data Protection and Security Policy**
* **UAB HIPAA Core Policies**
* **Data Classification Rule**
* **Data Protection Rule**
* **Data Access Policy**
* **Acceptable Use Policy**
* **Data custodian responsibilities**

**1.0 Introduction**

The objective of this standard for research data security requirements is to assist the UAB research community in the protections requirements of data and systems.

**2.0 Scope and Applicability**

All UAB research data stored, processed, or transmitted must be protected in accordance with these standards. Based on the regulatory or contractual requirements of the award; researchers are required to implement appropriate security controls.

Researchers are encouraged to consult with their department IT support, as needed. Many of the protections described herein are provided with UABIT-supported servers and networks, and would not require any additional technical investments by the researchers.

**3.0 Classification of Research Data**

The classification of research data depends on several factors such as type of data, and/or contractual elements and thus may fall into any of the classifications defined herein. Likewise, time of release and collaboration effect the classification of research data. As such, certain unpublished research data may be classified as private or sensitive until such time the research is published.

Likewise, intellectual property that has not been disclosed to or protected by the IIE may need to be classified as sensitive. Additionally, federal laws, rules and regulations (including but not limited to FISMA, HIPAA, FERPA, and Export Controls), sponsor requirements, and UAB policies and guidelines will necessitate a certain classification.

**It is incumbent upon the Researcher to know the type of data, the circumstances governing the data, and classify it accordingly.** Once classified, the Researcher will need to maintain the data using the appropriate UAB system of record or database with the appropriate access and security controls aligning to the classification standard. For example, not all UAB data storage options are recommended for sensitive data.

Research data shall also be maintained in accordance with UAB’s [Record Retention Policy](https://www.uab.edu/policies/content/Pages/UAB-AD-POL-0000708.html) and record retention schedule. For more information about protected research data please refer to the UAB OVPRED.

**3.1 Specific Roles and Responsibilities for Protecting Institutional Data**

3.2 [Data Stewards](#BK1) have administrative control and are officially accountable for a specific information asset. Data Stewards shall:

* assign an appropriate classification to the information;
* govern processes for determining access to information assets; and
* ensure compliance with policies and regulatory requirements related to the information.

**Examples:** VP of Financial Affairs & Administration - financial and HR data; VP of Research & Economic Development - research administration data; Deans and Unit Chairs and data from their respective academic area.

3.3 [Data Custodians](http://www.uab.edu/it/home/component/k2/item/213-data-custodian-responsibilities) safeguard the data on behalf of the Data Steward.

* UAB’s central Information Technology (IT) units shall be responsible for protecting all Institutional Data maintained/stored in the institutional information systems.
* Distributed Information Technology (IT) units shall be responsible for protecting all Institutional Data maintained/stored in unit level information systems.

3.4 UAB Information Security

Members of the UAB Information Security team are responsible for developing and implementing an information security program as well as the supporting data security and protection policies, standards and procedures.

3.5 Information Security Liaison (ISL)

Each unit senior manager will designate at least one ISL who will act as a liaison to the UAB information Security Team. ISLs oversee information security responsibilities for the units and schools, including assisting with security awareness and security incident response.

3.6 System Administrators

System Administrators are individuals within the central IT/HSIS or school/units with day-to-day responsibility for maintaining information systems.

3.7 Data Users

Data Users are individuals authorized to access UAB data and are responsible for protecting the information assets on a daily basis through adherence to UAB policies.

**4.0 Protection Requirements Based on Classification**

The table below defines minimum protection requirements for each category of data when being used or handled in a specific context (e.g. Sensitive Data sent in an email message). Please note that these protections are not intended to supersede any regulatory or contractual requirements for handling data.

|  | **Public Data – Low Risk** |
| --- | --- |
| Collection and Use | No protection requirements |
| Granting Access or Sharing | No protection requirements |
| Disclosure, Public Posting, etc. | No protection requirements |
| Electronic Display | No protection requirements |
| Open Records Requests | Data can be readily provided upon request. However, individuals who receive a request must coordinate with University Relations Office before providing data. |
| Exchanging with Third Parties, Service Providers, Cloud Services, etc. | No protection requirements |
| Storing or Processing: Server Environment | Servers that connect to the UAB network must comply with IT Security Practices. |
| Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.) | Systems that connect to the UAB network must comply with IT Security Practices. |
| Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.) | No protection requirements |
| Electronic Transmission | No protection requirements |
| Email and other electronic messaging | No protection requirements |
| Printing, mailing, fax, etc. | No protection requirements |
| Disposal | No protection requirements |

|  | **Sensitive Data – Moderate Risk** |
| --- | --- |
| Collection and Use | Limited to authorized uses only.  Units/Colleges that collect and/or use Sensitive Data should participate in the Information Security Program by reporting servers to the Enterprise Information Security Office.  In addition, any/all servers that process or store Sensitive Data must meet all requirements associated with applicable laws and/or standards.  Additionally, sensitive institutional data must be stored and managed in unit or higher systems. |
| Granting Access or Sharing | Access shall be limited to authorized University officials or agents with a legitimate academic or business interest and a need to know as outlined by UAB policies.  All access shall be approved by an appropriate data steward and tracked in a manner sufficient to be auditable.  Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved through the UAB contract process. |
| Disclosure, Public Posting, etc. | Sensitive Data shall not be disclosed without consent of the data steward.  Sensitive Data may not be posted publicly.  Directory information can be disclosed without consent. However, per FERPA, individual students can opt out of directory information disclosure. |
| Electronic Display | Only to authorized and authenticated users of a system. |
| Open Records Requests | Sensitive Data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with the University Relations Office. |
| Exchanging with Third Parties, Service Providers, Cloud Services, etc. | A contractual agreement (or MOU if governmental agency) outlining security responsibilities shall be in place and approved through the UAB contract process before exchanging data with the third party / service provider.  UAB Box.com – no special requirements.  UAB O365 – no special requirements. |
| Storing or Processing: Server Environment | Servers that process and/or store sensitive institutional data must comply with IT Security Practices, as well as applicable laws and standards. Additionally, sensitive institutional data must be stored and managed in unit or higher systems. |
| Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.) | Systems that connect to the UAB network must comply with IT Security Practices, as well as applicable laws and standards.  In addition, any/all systems that process or store Sensitive Data must be encrypted volume and endpoint must require PIN and/or password for access to device. |
| Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.) | Sensitive Data shall only be stored on removable media in an encrypted file format or within an encrypted volume. |
| Electronic Transmission | Sensitive Data shall be transmitted in either an encrypted file format or over a secure protocol or connection. |
| Email and other electronic messaging | Messages shall only be sent to authorized individuals with a legitimate need to know.  Messages with Sensitive Data shall be transmitted only to other uab.edu or uabmc.edu email recipients.  Sensitive Data may be shared through approved UAB services. |
| Printing, mailing, fax, etc. | Printed materials that include Sensitive Data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know.  Access to any area where printed records with Sensitive Data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.  Do not leave printed materials that contain Sensitive Data visible and unattended. |
| Disposal | Follow the [UAB Secure Media Destruction process](https://www.uab.edu/it/home/it-reports-and-publications/item/211-what-is-the-process-for-uab-secure-media-destruction) for the secure disposal of discs, CDs, DVDs, tapes and hard drives.  Repurposed for University Use - [Multiple](https://www.uab.edu/it/home/it-reports-and-publications/item/211-what-is-the-process-for-uab-secure-media-destruction) pass overwrite. NOT Repurposed for University Use - Physically destroy.  Follow the [Destruction of University Records Procedure](http://www.uab.edu/policies/content/Pages/UAB-UC-PRO-0000713.aspx) for printed materials.  Refer to the [UAB Records Retention Policy](http://www.uab.edu/policies/content/Pages/UAB-AD-POL-0000708.aspx) and [Records Retention Schedule](https://www.uab.edu/compliance/images/Records_Retention_Schedule_FINAL_20-NOV-2017.pdf) for specific guidance on records retention. |

|  | **Restricted/PHI Data – High Risk** |
| --- | --- |
| Collection and Use | Limited to authorized uses only.  Units/Colleges that collect and/or use Restricted data should participate in the Information Security Program by reporting servers to the Enterprise Information Security Office.  In addition, any/all servers that process or store Restricted Data must meet all requirements associated with applicable laws and/or standards.  Additionally, restricted/PHI data must be stored on servers located in the UAB data center and managed by Central IT.  SSNs may not be used to identify members of the UAB community if there is a reasonable alternative.  SSNs shall not be used as a username or password.  SSNs shall not be collected on unauthenticated individuals.  All credit/debit card uses must be approved by the VP of Financial Affairs and Administration Office. |
| Granting Access or Sharing | Access shall be limited to authorized University officials or agents with a legitimate academic or business interest and a need to know as outlined by UAB policies.  All access shall be approved by an appropriate data steward and tracked in a manner sufficient to be auditable.  Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved through the UAB contract process. |
| Disclosure, Public Posting, etc. | Not permitted unless required by law. |
| Electronic Display | Restricted data shall be displayed only to authorized and authenticated users of a system.  Identifying numbers or account number shall be, at least partially, masked or redacted. |
| Open Records Requests | Restricted data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting Restricted portions of records. Individuals who receive a request must coordinate with the University Relations Office. |
| Exchanging with Third Parties, Service Providers, Cloud Services, etc. | A contractual agreement (or MOU if governmental agency) and/or Business Associate Agreement (BAA) outlining security responsibilities shall be in place and approved through the UAB contract process before exchanging data with the third party / service provider.  UAB Box.com – Subject to any applicable laws.  \*\* ePHI/HIPAA data is subject to Health System approval (transactional storage).  UAB O365 (SharePoint and OneDrive) is subject to approval.  UAB O365 (Teams and Email) is prohibited. |
| Storing or Processing: Server Environment | Servers that process and/or store sensitive institutional data must comply with IT Security Practices, as well as applicable laws and standards.  Additionally, restricted/PHI data must be stored on servers located in the UAB data center and managed by Central IT.  Storing Credit/Debit card PAN data is not permitted. |
| Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.) | Any/all systems that process or store Restricted Data must be encrypted volume and endpoint must require PIN and/or password for access to device.  Storing Credit/Debit card PAN data is not permitted.  Storing Restricted Data on personally-owned devices is not permitted.  Devices storing or processing restricted data must be physically secure at all times.  Avoid storing Restricted Data on portable devices. |
| Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.) | Not permitted unless required by law.  If required by law, Restricted Data stored on removable media shall be encrypted and the media shall be stored in a physically secured environment. Storing restricted data on personally-owned media is not permitted. |
| Electronic Transmission | Secure, authenticated connections or secure protocols shall be used for transmission of Restricted Data. |
| Email and other electronic messaging | Not permitted without express authorization or unless required by law.  Messages with Restricted Data shall be transmitted in either an encrypted file format or only through secure, authenticated connections or secure protocols.  Restricted Data may be shared through approved UAB services.  SSNs may not be shared through email or other electronic messaging.  Credit card data may not be shared through email or other electronic messaging. |
| Printing, mailing, fax, etc. | Printed materials that include Restricted Data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know.  Access to any area where printed records with Restricted Data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.  Do not leave printed materials that contain Restricted Data visible and unattended.  Social Security Numbers shall not be printed on any card required to access services.  New processes requiring the printing of SSN on mailed materials shall not be established unless required by another state agency or a federal agency. |
| Disposal | Follow the [UAB Secure Media Destruction process](https://www.uab.edu/it/home/it-reports-and-publications/item/211-what-is-the-process-for-uab-secure-media-destruction) for the secure disposal of discs, CDs, DVDs, tapes and hard drives.  Repurposed for University Use - [Multiple](https://www.uab.edu/it/home/it-reports-and-publications/item/211-what-is-the-process-for-uab-secure-media-destruction) pass overwrite. NOT Repurposed for University Use - Physically destroy.  Follow the [Destruction of University Records Procedure](http://www.uab.edu/policies/content/Pages/UAB-UC-PRO-0000713.aspx) for printed materials.  Restricted Data that is no longer necessary for University business should be disposed to minimize risk of data breach.  Refer to the [UAB Records Retention Policy](http://www.uab.edu/policies/content/Pages/UAB-AD-POL-0000708.aspx) and [Records Retention Schedule](https://www.uab.edu/compliance/images/Records_Retention_Schedule_FINAL_20-NOV-2017.pdf) for specific guidance on records retention. |

**Change History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Description** | **Approval** | **Date** |
| 1.0 | Final version – approved by President Watts | Dr. Ray Watts | 2/22/2017 |
| 1.1 | Added specific related policies, rules & guidance  Corrected grammatical errors |  | 12/15/2017 |
|  | Reviewed - no changes/updates |  | 6/4/2018 |
|  | Reviewed - no changes/updates |  | 6/3/2019 |
| 2.0 | Added risk levels for data classifications.  Added health system approval for transactional use of UAB Box.com for ePHI/HIPAA  Added UAB O365 specific requirements for sensitive and restricted data. | Dr. Curt Carver | 6/28/2021 |