THE UNIVERSITY OF ALABAMA

# Information Protection Procedure

**Unit:** Office of Information Technology (OIT)
**Effective Date:** 6/1/2020
**Revision Date:** 9/26/2024

**Contact:** Taylor Anderson
**Title:** Chief Information Security Officer

## Purpose

The purpose of this Information Protection Procedure is to assist The University of Alabama community in the electronic protection, storage and usage requirements for all University Information. Based on the classification of the information, users are required to implement appropriate security controls. Having information appropriately classified will assist with protecting information in our systems that utilize classifications.

UA Information Security adopts the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security as the basis for the University-wide set of security standards and guidelines.

## Procedure

### *Classifying Information*

All University data must be classified into one of the three following categories:

- **Public Information**: Information that may be disclosed to the general public without harm.

- **Sensitive Information**: Information that should be kept confidential. Access to this information shall require authorization and legitimate need-to-know. Privacy may be required by law or contract.

- **Restricted Information**: Sensitive information that is highly confidential in nature and carries significant risk from unauthorized access or uninterrupted accessibility is critical to UA operations. Privacy and security controls are typically required by law or contract.

### *Protection of Research Data*

For the protection of human subject research data, refer to the Research and Economic Development Institutional Review Board (IRB) website.

### *Minimum security for all computing devices*

Physical security — Computing devices shall be protected from unauthorized physical access and theft.

Operating systems – Current vendor-supported operating systems are required for all computing devices.

Patching and updates – All computing devices shall have patches and updates applied on a consistent and regular schedule. Computing devices shall have all applicable security updates installed as soon as practicable. This applies to all software running on any computing or network device.

- Critical patches that pose a high risk to the University should be applied immediately, as practical
- High risk patches should be applied within 30 days of receipt
- All other patches should be applied within 90 days of receipt
- Oracle database patches will maintain a quarterly patch schedule for all but critical patches
- Any system that cannot be patched based on the above schedule must document the business reason including a schedule for when patching will occur and communicate to all appropriate University leadership involved (OIT, Business Unit, Application Owners, etc.)

Antivirus and Anti-malware software – Antivirus/Anti-malware software shall be used and kept up-to-date on devices where the use of such software is practical.

Software firewall – Software firewalls shall be enabled and kept up-to-date on devices that have the capability to run software firewalls.

Access control — Devices shall require sign-on or login for users. Users shall be authenticated by means of unique username and passwords/passphrases or by other authentication processes (e.g. two-factor, biometrics or smart cards). In general, only encrypted authentication mechanisms or protocols shall be used. Modern authentication shall be used where technically possible. When passwords/passphrases are used, their construction and management shall comply with the UA password/passphrase procedures detailed below.

Un-authenticated email relays and proxy services – Devices shall not operate as an unauthenticated email relay or proxy services.

Unnecessary software, services, protocols and ports – Software, services, protocols, and ports that are not necessary for the device to perform its function or mission shall be uninstalled and/or disabled.

Encryption of laptop computers used for UA business – All laptop computers used for UA business must be encrypted to protect data from unauthorized disclosure.

## *Minimum security for computing devices that store or transmit sensitive and/or restricted data*

Responsibility for the security of a device covered by this rule and its data shall be assigned to the individual who is designated as its primary user or owner.

Restricted data must be stored on servers located in the UA data center and centrally managed, or within cloud services approved by the Office of Information Technology. Servers that contain either sensitive and/or restricted data will be classified as sensitive and/or restricted servers.

### Servers

In addition to the requirements outlined above for all computing devices, all server-class devices that transmit, process or store restricted and/or sensitive data shall meet the following minimum security requirements:

Physical security — Server-class devices shall be placed within a protected and monitored area with a secure perimeter (e.g. walls, lockable doors, lockable server racks) that protects the system from unauthorized physical access.

Limit network access — Network access to restricted and sensitive systems shall be limited and/or isolated to the least access necessary for the device to perform its function/mission.

Access control — User accounts and users shall have a unique identifier (user ID/login name) that is assigned for their personal use only and not shared. Privileges shall be restricted and controlled in accordance with the principle of least privilege to reduce opportunities for unauthorized access or misuse of the system. Access and privileges shall be authorized by an appropriate authority and reviewed at regular intervals.

Secure login and authentication — Access shall be controlled with secure/encrypted logon procedures such as CAS, Shibboleth, Windows Authentication, or other ticket-based authentication solution (SAML) using 2FA when available.

Protection against brute-force login attacks — Controls shall be put in place to limit failed login attempts. (Back off algorithms)

Session controls — Controls shall be put in place to ensure that inactive sessions shall expire after a defined period of inactivity.

Logging, monitoring and review — System administrator, user activities and system events shall be logged, forwarded to the Enterprise SIEM, and reviewed daily. Logs shall be retained for a period of at least one year or a period deemed practicable by the University department/unit responsible for the security of the device.  Host intrusion monitoring should be performed by our third party Security Operations Center where use of such software is practical.

Identification and management of vulnerabilities — Devices shall be hardened prior to implementation. Hardening guidelines are available at https://oit.ua.edu/security. Security updates shall be applied and unnecessary software and services uninstalled or disabled in order to minimize potential technical vulnerabilities. Vulnerabilities shall be identified and evaluated using a routine process, and appropriate measures shall be taken to remediate significant vulnerabilities.

Change management — A formal process shall be adopted to review, approve, and test configuration changes before the changes are implemented to ensure that the changes do not adversely impact the operation or security of the device.

Encrypted transmission of data — Encrypted protocols or secure channels shall be used to transmit restricted and sensitive data to and from the device. A UA-approved VPN or Cloud service shall be used to access UA resources from outside the UA network or from other isolated networks within UA.

Data containment – Controls need to be implemented that govern and prevent unauthorized transmission of restricted data from systems that are authorized to process restricted data.

Remove restricted and sensitive data when no longer needed — Avoid storing restricted or sensitive data unnecessarily. A process shall be adopted to regularly review archived files and delete files containing restricted or sensitive data when the files are no longer needed. Where possible, automated processes should be used to archive or delete old or unused sensitive data.

Administrator restrictions - Server administrators are required to use standard, least-privileged accounts and only will elevate to administrative privileges when necessary to perform a specific job task. Web surfing from a server to the Internet by administrators is prohibited unless required to perform update or installation tasks and email clients will not be installed on a server-class device.

**Desktops**

In addition to the requirements outlined above for all computing devices, all desktop-class devices that process restricted or sensitive data shall meet the following minimum security requirements:

Physical security — Desktop devices shall be placed in reasonably secure areas, such as lockable offices, and not in publicly assessable areas.

Auto-lock — Desktop devices shall be configured to automatically lock and require a logon after being unattended or inactive for a predefined period of time.

Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.

Protection from drive-by malware — Reasonable methods shall be used to prevent or disable web-browsing capabilities on devices that store or process restricted data. In cases where it is not possible to disable or prevent web browsing, alternative methods — such as application-layer firewalls, proxy servers, and web content filters, and/or application whitelisting— shall be implemented to protect against drive-by attacks and malware.

Remove restricted and sensitive data when no longer needed — Devices shall be configured to automatically delete temporary files, temporary Internet files, clear web browser caches, etc.

- A process shall be adopted to regularly review archived files and delete files containing restricted or sensitive data when the files are no longer needed.
- Restricted data shall not be stored on desktop-class devices unencrypted.

Encrypt restricted data — Restricted data stored on the device shall be stored on encrypted storage devices, or at least in encrypted files or within encrypted volumes.

**Laptops, tablets, and mobile devices**

In addition to the requirements outlined above for all computing devices, all laptop and mobile-class devices that store or process restricted and/or sensitive data shall meet the following minimum security requirements:

Auto-lock — Devices shall be configured to automatically lock and require a logon, pin, or other means of authentication after being unattended or inactive for a predefined period of time.

Protection from theft — Whenever possible, the device should be protected from theft by storing the device in a secure location, and/or anchoring with a security cable, etc. Tracking/location software shall be installed or enabled on the device, if practicable.

Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.

Mobile device management – Devices that process or store restricted information must be under mobile device management where practicable.

Remove restricted and sensitive data when no longer needed — Devices shall be configured to automatically delete temporary files, temporary Internet files, clear web browser caches, etc.

- A process shall be adopted to regularly review archived files and delete files containing restricted or sensitive data when the files are no longer needed.

Encrypt restricted and sensitive data — Restricted and sensitive data stored on the device shall be stored in encrypted files or within encrypted volumes.

## *Password*

### Length

All account passwords / passphrases on systems leveraging myBama IDs will be a *minimum* of 12 characters and a maximum of 32 characters.

- Other account passwords / passphrases not using myBama shall be a minimum of 12 characters.
- System / service accounts will be a minimum of 32 characters in length.

### Lockout

After 10 failed login attempts, accounts should be disabled and locked out for at least 15 minutes where feasible.

### Expiration

Passwords / passphrases shall expire according to the table below:

| Category | Interval | Category | Interval | Category | Interval |
|---|---|---|---|---|---|
| Employee | 365 days | Resource | 90 days | Alumni/ Inactive | 365 days |
| Administrator | 90 days | Temporary | 90 days | Guest | 365 days |
| Student | 365 days | System | None | | |

- The vast majority of UA students, faculty and staff will fall into the category of Employee or Student. Use of multi-factor authentication is considered an allowed compensating control for not expiring passwords / passphrases.
- Information technology personnel with elevated access or higher compliance assurance requirements will be treated as Administrator category.
- When there is a question on which expiration interval applies, the more restrictive interval shall be used.

### History

Password / passphrase history shall be kept to prevent previous passwords / passphrases from re-use to the technical extent possible. Systems should maintain at least 5 previous passwords.

### Caching

Applications or systems that utilize myBama IDs shall not cache or store myBama ID passwords / passphrases, even if hashed or otherwise encrypted without an approved exception.

- Individual devices such as smartphone, tablets, etc. are not subject to this requirement if they are configured to require a pin, biometric, etc. for access to the device.
- Use of a secure, enterprise-grade, password vault approved by UA is acceptable by this standard (e.g. LastPass).

**Rotation**

Windows servers and desktops shall be configured to automatically rotate the Administrator password daily, when the account is enabled (eg. LAPS).

**Complexity**

Passwords / passphrases shall contain at least 1 character from three of the following ASCII character sets: lowercase alphabetic, uppercase alphabetic, numbers, and symbols.

myBama Password Complexity:

- Passwords cannot contain Unicode or international characters.
- Passwords cannot contain any of the following special characters: @ " : ? (“at” sign, quote marks, colon, and question mark).
- Password must not contain myBama username, nor the individual’s first or last name.
- Password may not contain the words bama, roll, or tide.
- Users cannot reuse previous passwords; new passwords must be unique.

System accounts must utilize characters from all *four* of the character sets mentioned.**Sharing**

A password should never be shared. Each user should have their own identification and authentication with the roles or authorization they need to perform their job. In the unlikely event that a password must be shrared, it must be changed by the owner immediately after the shared use.

**Logging**

Systems shall log successful and failed logon attempts and retain such logs for a minimum of 90 calendar days.

**Screen Lock**

A computer screen locking feature is recommended to be enabled and configured to lock the computing device after a period of inactivity not longer than 15 minutes. If enabled, access to the device shall be granted only after a valid password / passphrase is entered or provided.

- Conference rooms may be configured to lock after 60 minutes of inactivity.
- Classroom podium systems will be configured to lock after the maximum time of a standard class in that space.

**Encryption**

All credential usage shall be encrypted while in transit, at rest, and while in storage.

**Multi-factor Authentication (MFA)**

The use of a multi-factor authentication (MFA) system adds an additional layer of security for information systems. Some types of regulated sensitive data access require the use of multi-factor authentication per federal guidelines. Use of multi-factor authentication may be a compensating control for exceptions to the standard. E.g. Duo.

- Where possible, multi-factor authentication must be used for all administrative access.
- All faculty, staff and student VPN access shall use multi-factor authentication.
- Where possible, vendor remote access shall use multi-factor authentication.
- Unless unsupported and a waiver has been signed, access to O365 and Azure resources shall use multi-factor authentication.

## *Account Management*

Involuntary separation of faculty, staff or students, or as dictated by Human Resource, Legal or University of Alabama Police Department: Immediate removal of all accounts

Accounts for Faculty and Staff as a normal separation: Removal of all accounts within 24 hours except for faculty email which will remain active for 90 days

Exceptions to account removal must be approved by the Associate Provost of Academic Affairs for faculty, and Human Resources for Staff

Unused student accounts are suspended if they haven't been accessed in a year

## *International travel and export control*

All laptop and mobile-class devices used for international travel shall meet the minimum security requirements in sections above, "*Minimum security for all computing devices*" and "*Laptops, tablets, and mobile devices*". International travel with restricted data requires the approval from the data steward.

## *Enforcement and implementation*

### Roles and responsibilities

Each University academic and business unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard security rule. The Vice Provost of Information Technology Office is responsible for enforcing this standard security rule.

### Consequences and Sanctions

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment. In the cases where students are involved, such issues will result in the reporting of a Student Code of Conduct violation. Any device that does not meet the minimum security requirements outlined in this standard may be removed from the UA network, disabled, etc., as appropriate until the device can comply with this standard. For certain restricted data, regulatory consequences and sanctions may also be imposed.

### Information Protection Roles

#### Users

The University of Alabama IT resource users (IT resource users include both students, faculty, staff and affiliates) are responsible for protecting the security of all data and IT resources to which they have access. This includes implementing appropriate security measures on personally owned devices which access The University of Alabama

IT resources. In addition, users are required to keep their accounts and passwords secure in compliance with the UA password procedures. Training is required prior to receiving access to certain restricted data under regulatory control (e.g. HIPAA, FERPA, GLBA, PCI, etc).

The University of Alabama employees may grant IT resource guest access to third parties (e.g., visiting scholars). Any University of Alabama employee who grants guest access to IT resources is responsible for the actions of their guest users.

**System Administration**

Every UA-owned IT resource (including virtual resources such as virtual machines and cloud based services) must have a designated system administrator. The UA expectation is that every UA-owned IT resource will be professionally managed by the unit technical support team unless prevailing regulations dictate otherwise.

The system administrator is responsible for proper maintenance of the system, even if the system administrator is not a member of the unit technical support team. This responsibility must be acknowledged and documented. In addition, the machine must be accessible to the unit technical support team for incident management purposes unless legal restrictions will not allow such access.

Negligent management of a UA-owned IT resource resulting in unauthorized user access or a data breach may result in the loss of system administration privileges.

System administration responsibilities for all UA-owned IT resources, including those that are self-administered within academic units and University divisions, include the following:

- Complying with all applicable UA IT policies and procedures
- Performing an annual cyber security self-assessment for the set of IT resources administered
- Working with the unit technical support team to establish the following:
    - Installing and running endpoint security/management agents that have been approved by The University of Alabama Security Team
    - At a minimum, follow the secure configuration recommendations provided for the IT resource
    - Establishing an appropriate backup strategy and performing regular system backups
    - Regularly updating the operating system and other applications installed on the machine
    - Using, where possible and practical, central University of Alabama IT services for system authentication and account management (e.g. LDAP and active directory)

**Network Management**

The Office of Information Technology (OIT) is responsible for planning, implementing, and managing The University of Alabama network, including wireless connections.

The following network appliances cannot be implemented at The University of Alabama without prior written agreement with OIT through a Memorandum of Understanding (MOU):

- Routers
- Switches

- Hubs
- Wireless access points
- Voice over IP (VOIP) infrastructure devices
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Virtual Private Networking (VPN)
- Consumer-grade network technologies
- Taps
- Other networking appliances that may not be included in this list

### Chief Information Security Officer

The Chief Information Security Officer is responsible for creating and maintaining a cybersecurity program and leading The University of Alabama OIT Security team. The purpose of the cybersecurity program is to define an environment to maintain the confidentiality, integrity and availability of UA IT resources and UA data. In addition, the Chief Information Security Officer, or a designee, is responsible for leading the investigation of and response to cyber security incidents as outlined in the University of Alabama Incident Response Plan. The response to any incident will be developed in collaboration with the data steward, Strategic Communications, Legal Counsel and other campus offices as appropriate.

#### Research Protection Reviews

The University of Alabama recognizes the value of research. The Chief Information Security Officer, or a designee, is responsible for reviewing data protection plans and provide suggestions, as necessary, for any improvements or adjustments. In general, all research data shall have a plan that will define access controls commensurate to the risk of unauthorized exposure and sensitivity.

#### Procurement Reviews

The Chief Information Security Officer, or a designee, is responsible for reviewing data protection plans and provide suggestions, as necessary, for any improvements or adjustments during the enrire procurement process. In general, all procurements or renewals shall have a plan that will define access controls commensurate to the risk of unauthorized exposure and sensitivity.

## *Exceptions*

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, the academic dean or division VP can submit the documented request to the Vice Provost of Information Technology and Chief Information Officer.

## *Protection Requirements Based on Classification*

The University of Alabama Information Protection Procedure defines minimum protection requirements for each classification category of information when being used or handled in a specific context (e.g. sensitive information sent in an email message). Please note that these protections are not intended to supersede any regulatory or contractual requirements for handling information.

| **Public Information** | |
|---|---|
| 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 | Information can be readily provided upon request. However, individuals who receive a request must coordinate with Strategic Communications and Legal before providing information. |
| Exchanging with Third Parties, Service Providers, Cloud Services, etc. | No protection requirements |
| Storing or Processing: Server Environment | Systems that connect to the University network must comply with IT Security Practices. |
| Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.) | Systems that connect to the University 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 Information** | |
|---|---|
| Collection and Use | Limited to authorized uses only. |
| | College/Department that collect and/or use Sensitive Information should participate in the information security program by reporting servers to the enterprise information inventory. |
| | In addition, any/all servers that process or store Sensitive Information must meet all requirements associated with applicable laws and/or regulations. |

| | |
|---|---|
| | Sensitive institutional information must be stored and managed in OIT or department data centers. |
| 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 University policies. |
| | All access shall be approved by an appropriate data steward and tracked in a manner sufficiently auditable. |
| | Before granting access to external third parties, contractual agreements which outline responsibilities for security of the information shall be approved through the University Procurement Services process. |
| Disclosure, Public Posting, etc. | Sensitive Information shall not be disclosed without consent of the data steward. |
| | Sensitive Information 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 Information 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 Strategic Communications and Legal. |
| 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 Procurement Services process before exchanging information with the third party / service provider. |
| | UA Box and OneDrive – no special requirements. |
| Storing or Processing: Server Environment | Servers that process and/or store sensitive institutional information must comply with IT Security Practices, as well as applicable laws and regulations. Additionally, sensitive institutional information must be stored and managed in OIT or departmental systems. |
| Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.) | Systems that connect to the University network must comply with IT Security Practices, as well as applicable laws and regulations. |
| | In addition, any/all systems that process or store Sensitive Information must be encrypted and endpoint must require PIN and/or password for access to device. |
| Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.) | Sensitive Information shall only be stored on removable media in an encrypted file format or within an encrypted volume. |
| Electronic Transmission | Sensitive Information 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 Information shall be transmitted only to other University email recipients. |

| | |
|---|---|
| | Sensitive Information may be shared through approved University services. |
| Printing, mailing, fax, etc. | Printed materials that include Sensitive Information 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 Information 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 Information visible and unattended. |
| Disposal | Follow the University Secure Media Destruction process for the secure disposal of discs, CDs, DVDs, tapes and hard drives. |
| | Repurposed for University Use - Multiple pass overwrite. NOT Repurposed for University Use - Physically destroy. |
| | Follow the Destruction of University Records Procedure for printed materials. |

| Restricted Information | |
|---|---|
| Collection and Use | Limited to authorized uses only. |
| | Colleges/Departments that collect and/or use Restricted should participate in the Information Security Program by reporting servers to the Enterprise Information Inventory. |
| | In addition, any/all servers that process or store Restricted Information must meet all requirements associated with applicable laws and/or regulations. |
| | Additionally, Restricted Information must be stored on servers located in the OIT data center and managed by OIT. |
| | SSNs may not be used to identify members of the University 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 Office of the VP of Finance and Operations. |
| 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 University policies. |
| | All access shall be approved by an appropriate data steward and tracked in a manner sufficiently auditable. |
| | Before granting access to external third parties, contractual agreements which outline responsibilities for security of the information shall be approved through the Procurement Services contract process. |
| Disclosure, Public Posting, etc. | Not permitted unless required by law. |
| Electronic Display | Restricted Information 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 Information 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 Strategic Communications and Legal. |
| 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 Procurement Services contract process before exchanging information with the third party / service provider. |
| | UA Box and OneDrive  – Subject to any applicable laws. |

| | |
|---|---|
| Storing or Processing: Server Environment | Servers that process and/or store Restricted institutional Information must comply with IT Security Practices, as well as applicable laws and regulations. Additionally, Restricted Information must be stored on servers located in the OIT data center and managed by OIT. |
| | Storing Credit/Debit card PAN data is not permitted. |
| Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.) | Servers that connect to the University network must comply with IT Security Practices. |
| | In addition, any/all systems that process or store Restricted Information must be encrypted and endpoint must require PIN and/or password for access to device. |
| | Storing Credit/Debit card PAN data is not permitted. |
| | Storing Restricted Information on personally owned devices is not permitted. |
| | Devices storing or processing Restricted Information must be physically secure at all times. |
| | Avoid storing Restricted Information 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 Information stored on removable media shall be encrypted and the media shall be stored in a physically secured environment. Storing Restricted Information on personally-owned media is not permitted. |
| Electronic Transmission | Secure, authenticated connections or secure protocols shall be used for transmission of Restricted Information. |
| Email and other electronic messaging | Not permitted without express authorization or unless required by law. |
| | Messages with Restricted Information shall be transmitted in either an encrypted file format or only through secure, authenticated connections or secure protocols. |
| | Restricted Information may be shared through approved University 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 Information 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 Information 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 Information 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 University Secure Media Destruction process for the secure disposal of discs, CDs, DVDs, tapes and hard drives. |
| | Repurposed for University Use - Multiple pass overwrite. NOT Repurposed for University Use - Physically destroy. |
| | Follow the Destruction of University Records Procedure for printed materials. |
| | Restricted Information that are no longer necessary for University business should be disposed to minimize risk of a data breach. |

## Scope

All University of Alabama information stored, processed, or transmitted must be protected in accordance with this policy. Based on classification; users are required to implement appropriate security controls for the protection of the information.

## Definitions

**Administrator Accounts -** Accounts that have elevated privileges – administrator or privileged access rights.

**Chief Information Security Officer (CISO):** A designated individual responsible for the management of information security for the entire campus.

**Cloud Storage:** Off-campus, third party, hosted services that provide storage of information such as Box, OneDrive, etc. Use of cloud storage for ePHI requires a BAA with the cloud provider.

**Complexity -** The use of a mix of characters to construct a strong password / passphrase that is resistant to guessing and brute-force attacks.

**Computer and network abuse:** The use of resources in a manner inconsistent with the UA policy.

**Data versus Information:** **Data** is defined as the collection of facts and details like text, figures, observations, symbols or simply description of things, event or entity gathered with a view to drawing inferences. It is the raw fact, which should be processed to gain information. **Information** is described as that form of data which is processed, organized, specific and structured, which is presented in the given setting. It assigns meaning and improves the reliability of the data, thus ensuring understandability and reduces uncertainty.

**Employee -** An individual who holds an active faculty or staff assignment based on Human Resource records maintained by UA or its affiliates.  All employment categories are included in this definition.

**Encryption -** Process of encoding data to unreadable ciphertext in such a way  that authorized parties cannot read it but authorized parties can.

**IT Forum** - A UA authorized committee consisting of representatives from the various Colleges/Schools/organizations on campus focusing of IT issues and topics.

**Guest Account** - An account authorized by a UA sponsor for non-employees/students to allow access to limited systems or the Internet.

**Lock-out** – Security feature that temporarily disables an account for a specified period of time.

**myBama ID -** A mnemonic identifier selected by authorized UA users to provide a unique identification mechanism for access to systems and processes.

**Passphrase -** A sequence of words or other text used to control access to a computer system, program or data.  A passphrase is similar to a password in usage, but is generally longer for added security.

**Resource Accounts** – Accounts specifically used for inter-process activities such as program to program communications.

**Screen Lock –** A protective feature that prevents access to device when not in use by the authenticated user.

**Service Accounts –** Generally an account that does not correspond with an actual person that services use to access resources they need to perform their activities.

**Standards –** Established procedure to be followed in carrying out a given operation or in a given situation.

**Student** – FERPA regulations define student as any individual who is or has been in attendance at The University of Alabama and regarding whom the agency or institution maintains education records.

**System Accounts** – Accounts used by servers and other high-level computers/devices which run code not normally associated with a user workstation/handheld device; e.g. file servers, application/database servers, and similar devices.

**Temporary Accounts** – A type of account used for non-permanent situations typically for software testing and debugging prior to being migrated to a production status.