Information Confidentiality/Security

Summary/Purpose: This policy sets standards for how confidential information maintained by the University of Mississippi (UM) is to be protected. Adequately securing customer information is not only the law but also good business sense. Poorly managed customer data opens doors to identity theft and provides access to sensitive information that could result in loss to customers.

Background

The Gramm-Leach-Bliley (GLB) Act enacted Nov. 19, 1999, not only reforms the financial services industry but also calls for the safeguarding of customer financial information and describes the need for administrative, technical, and physical safeguards for such information. Because higher education institutions participate in financial activities such as making Federal Perkins Loans, the Federal Trade Commission has ruled that the safeguarding of consumer information specified by the Act also applies to colleges and universities. To comply with federal requirements to safeguard financial and other confidential information, UM must adhere to general standards and develop, put into effect, and maintain a comprehensive, written policy that contains administrative, technical, and physical safeguards for maintaining the confidentiality of non-public customer information. Although the UM’s primary customers are students, in this context, a customer is defined to be a student, employee, or consumer who has a relationship under which UM provides a financial product or service.

Confidential Information Collected and Stored

As an educational institution, UM collects, retains, and uses non-public financial and confidential information about individual customers, as allowed by law, to provide services. Non-public financial/confidential information is collected from sources such as:

- Applications for admission and other forms
- Financial transactions (checks, credit cards, and electronic funds transfers)
- Protected health information (PHI), which is legally protected by the Federal Health Insurance Portability Accountability Act (HIPAA)
- Transactions with UM affiliates
- Consumer reporting agencies
- State, federal, and other governmental agencies
- Personal information (social security numbers, birth date, grades, and so on)

In addition, UM collects, retains and uses non-public sensitive and confidential data and software to conduct research. UM is required to prevent the intentional and unintentional export of research information in compliance with United States export control laws and regulations. Export controls are United States federal government laws and regulations that restrict the release of items, information and software to restricted foreign countries, persons and entities (including universities). Researchers who work
with export-controlled information are subject to additional security requirements, e.g., the physical location where data is stored. For more information, contact the Office of Research and Sponsored Programs (ORSP).

The security standards defined here apply to all types of sensitive and confidential information whether stored physically on the UM campus or hosted elsewhere.

**General Standards for Safeguarding Customer Information**

Overall safeguarding objectives are as follows:

- Ensure the security and confidentiality of customer information in offices and data storage areas.
- Identify and protect against anticipated threats to the security or integrity of confidential customer information.
- Prevent the unauthorized access to, or use of, confidential customer information.

To meet these objectives, UM department heads who oversee activities that involve access to or the storage of non-public customer information are required to put in place information security programs that include the following components:

- Designate an employee to develop and coordinate a departmental information security program that establishes the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, send, dispose of, or otherwise handle, customer information.
- Identify reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, change, destruction, or compromise of such information, and assess the sufficiency of safeguards in place to control these risks. This includes listing all assets and their vulnerabilities.
- Establish risk assessment programs for the following areas:
  - Employee training and management
  - Information systems, including network and software design, also information processing, storage, transmission, and disposal
  - Detection, prevention, and response to attacks, intrusions, or systems failures
- Select vendor partners and service providers that can maintain proper safeguards for customer information. Contractually require service providers to put into effect and maintain such safeguards.
- Periodically evaluate and adjust the departmental information security program based on the results of testing and monitoring.

The Office of Information Technology (IT) and the IT Helpdesk are available to respond to specific security questions and to assist with training. The campus Security Coordinator, David Drewrey, is available to help establish and evaluate information security programs.
Detailed Standards for Safeguarding Customer Information

1. Sharing Information with Affiliates

To provide services, UM may disclose non-public financial/confidential information about a customer with business affiliates and other third parties. UM does not, and will not, disclose non-public financial/confidential information about customers, or former customers, to anyone, except as permitted by law.

2. Employee Access to Confidential Information

Employee access to customer information is restricted to those who have a legitimate business reason for getting such information and are educated about confidentiality and customer privacy. See the Privacy in the Electronic Environment Policy for full details.

3. Accountability

Department heads are ultimately responsible for ensuring that information technology services deployed by that department meet the security requirements outlined in this policy.

4. Purpose

Departments may not collect or store non-public financial/confidential information without having a legitimate purpose. Departments may collect only the information needed to perform a specific task. *Example: A department may not collect a driver’s license number without having a written policy addressing the specific purpose and use of this information.* The Internal Auditing Office is available to help departments identify confidential information and document reasons for its collection. See the Records Retention Policy for additional details.

5. Use, Disclosure, and Retention

UM will secure and manage private, non-public customer information according to all applicable state and federal laws about its use, disclosure, and retention. Customer information may only be used or disclosed for the purpose for which it was collected, unless the customer consents to its use for another purpose, or when the data is requested as permitted by law. Customer information may only be retained for the time noted in the Records Retention Policy. If the information is to be used for another purpose, consent must be obtained from the customer before use. When getting first permission or revised consent, the customer will be informed how long the information will be retained and how it will be destroyed.

6. Safeguarding
• Paper data such as copies of checks must be kept in locked rooms and physically secured file cabinets.
• Calls or other requests for customer information must be routed to a designated individual who has been trained about its use, disclosure, and retention.
• Attempts to gain fraudulent or unauthorized access to customer information must be reported to the Internal Auditing Office for evaluation.

7. Disposal of Confidential Information

Paper records containing confidential information must be confetti shredded. Contact the Physical Plant Department for information about shredding of paper records. Computer equipment and electronic storage media (CDs, DVDs, hard disks, tapes, and so on) must be physically destroyed or reformatted / securely erased with IT oversight to prevent recovery of data.

8. Customer Access to Confidential Data

On request, customers will be informed of the existence, use, and disclosure of their information and will be given access to it with proper identification. Customers may verify the accuracy and completeness of their information, and may request that it be amended. Any changes to customer data should be logged either through automated mechanisms or through manual processes. Each department/unit is responsible for getting and presenting information when requested by a customer.

9. Customer Complaints and Suggestions

Students/customers may direct questions about the privacy principles or practices outlined above to department heads or their designees. Each department/unit is responsible for dealing with customer complaints and suggestions. If a customer is not satisfied with the resolution provided by the department/unit, he/she should be referred to department’s next level of supervision.

10. Monitoring and Testing of Security

Each department is responsible for actively testing and monitoring its security practices and periodically evaluating and adjusting its information security program based on the results of testing and monitoring. In addition, all servers and storage devices that contain sensitive information must be registered so they can be periodically scanned for vulnerabilities. To register a server or workstation, login to my.olemiss.edu and select the Employees => Tools and Resources to get to the Campus Server Registry.

11. Contractors

In the normal course of business, UM selects and contracts with external service providers. When choosing a service provider that will have access to customer information, the evaluation process will include the provider’s ability to safeguard
Contracts with service providers will include the following provisions:

- Explicit acknowledgment that the contract allows the contractor access to confidential information
- A specific definition of the confidential information being provided
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose outlined in the contract
- A guarantee from the contractor that it will ensure compliance with the protective conditions outlined in the contract
- A guarantee from the contractor that it will protect the confidential information it gets according to commercially acceptable standards and no less rigorously than it protects its own customers’ confidential information
- A provision allowing returning or destroying all confidential information obtained by the contractor, on finishing the contract
- A stipulation allowing injunctive relief, without posting bond, to prevent or remedy breach of the contract’s or contractor’s confidentiality obligations
- A stipulation that a violation of the contract's protective conditions amounts to a material breach of contract and entitles the University to immediately end the contract without penalty
- A provision allowing auditing of the contractor’s compliance with the contract’s safeguard requirements
- A provision ensuring that the contract’s protective requirements will survive ending the agreement


Accounts
- Individual account usage is governed by the IT Appropriate Use Policy.
- Each user is responsible and liable for all processes started from his/her account; therefore, the user should secure his/her computer when leaving the office for any length of time.
- All accounts should be secured using a password. There should be no shared accounts.
- Unnecessary preconfigured or default accounts that have generic passwords should be removed.
- The password to default accounts should be changed before attaching the system to the network.

Auditing
- Review logs daily and question unusual traffic patterns.
- Keep logs secure.

Authentication
- Passwords should be at least eight characters and changed every ninety days.
Strong passwords are difficult to guess and contain alpha, numeric, and shift characters. Do not use words that can be found in the dictionary or identify anything of a personal nature (name, birthday, social security number, and so on).

- Do not write passwords in notebooks or on desk leaves, or store them online.
- Do not share passwords with anyone.
- Passwords should be resistant to computer programs that check previously used passwords or easily compromised passwords.
- **Passwords should never be stored or entered in clear text form.**

**Backups**

- Make full backups weekly.
- Store backup media offsite at an appropriate interval.
- Sensitive data should not be stored on externally hosted systems, including cloud-based storage systems, without a contract that is fully vetted for compliance with University policies. **Reference: See the section below on “Permitted and Restricted Uses of Data”**
- Test the restore process.

**Firewalls**

- A personal desktop firewall must be installed on any computer system that either has access to or has confidential data stored.
- A hardware firewall is also recommended in any instances where there are two or more computers with confidential data.

**Information Security**

- Institutional data transferred to personal computers, mobile devices, or shadow systems is the responsibility of the end user, who must ensure that the data is securely maintained and properly destroyed. The University provides Secure Document Exchange via portal for sharing sensitive data within the University.
- Any sensitive data stored on mobile devices should, at a minimum, be encrypted with AES encryption tools or equivalent.

**Logging In**

- Ensure that all connections to other servers have end-to-end security.
- Use Virtual Private Network (VPN) protection where appropriate.
- Replace rlogin, rsh, and rcp with ssh or equivalent.
- Replace ftp with sftp or equivalent.
- Provide secure X connections and secure tunneling of arbitrary TCP connections.

**Patches and Application Updates**

- Desktop computers and personal devices should be configured to apply application updates and operating system (OS) patches daily.
- Patches should be applied to servers on a regular basis as frequently as is feasible.
- Be alert for UM security announcements. It is much easier to stay abreast of patches and apply protection than to rebuild a system that has been compromised.
**SMTP Mail Servers**
- The operation of mail servers without authorization by the Security Coordinator is not allowed.
- Additional security requirements, e.g., restrictions on mail relaying, may be imposed for those who are permitted to run mail servers.

**TCP/IP**
- Disable unnecessary TCP/IP services.
- Stay abreast of security issues for any TCP/IP services that you run.

**Time Synchronization**
- Keep your time synchronized with a reliable NTP server. This is critical to accurately compare event logs with other servers, which is needed when investigating attacks.

**Trust Relationships**
- Avoid using ~/.rhost and /etc/hosts equivalent entries on Linux or other Unix based operating systems. Ideally, the .rhost capability should be permanently disabled.

**Verify Binaries**
- Make sure that system files have not been replaced or manipulated by hackers.
- Install only digitally signed applications, from a reputable source, signed by a third party certificate authority.
- When suspicious of faulty system activity that could be the result of hackers or malicious software, run a system file check utility or consider re-installing the operating system software. Once complete, restore user content from a secure backup source.

**Viruses**
- UM-owned computers and servers must have software installed to protect against viruses from the Internet or other machines. The software should be configured to perform daily checking for updates and preferably configured in an active scan or real time scan mode.
- Contact the IT Helpdesk for information on campus-wide site licensing for anti-virus software.
- When a virus is detected, immediately disconnect the infected machine(s) from all networks and contact your systems administrator.
- In cases where a systems administrator manages multiple machines, he/she should contact all users with access to the infected system, explain how to find out if related systems are infected, and how to remove the virus.
- See the Anti-Virus Protection for UM Computers Policy for additional information.

13. Data Center Security Practices
Access Security

- Software and access security of all computing resources is maintained with a multi-tiered system of constructed user accounts (i.e., system operators are granted certain privileges, administrators other privileges, and so on).
- All passwords are changed regularly.
- Access to certain critical systems maintenance and administrative interfaces is restricted to defined physical locations to prevent online attacks or intrusions.

Information Security

- Data access above the account level is maintained via a layered firewall implementation that employs various filtering and authentication techniques in conjunction with virtual private networks.
- All confidential data transmitted between central administrative and academic systems, including backups, traverses a physically isolated secure network within the facility.
- Monitoring of data access activity is accomplished via a centralized log server.
- Sensitive data should not be stored on externally hosted systems, including cloud-based storage systems, without a contract that is fully vetted for compliance with relevant UM policies. **Reference: See the section below on “Permitted and Restricted Uses of Data”**

Network Security

- Transmission of institutional data is routed through the campus network, which is a switched /100/1000/10000 Ethernet network.
- Locked doors to communication distribution areas provide physical security of the network.
- Where possible, data transmission is encrypted. For example, web-based services that use non-public, authenticated data are usually encrypted using SSL.

Offsite Backups

- Intended for use in disaster recovery procedures, offsite data backups are stored in a vault in another building on campus that is secured with continuous intrusion and fire detection systems.

Protected Access Documentation

- Online documentation and procedural sections for operations staff are maintained in the building but are not accessible from anywhere else on the Internet.

Protection of Printed Materials

- Printed reports are delivered only to approved locations and personnel, and are never distributed in a way that would allow unauthorized access to sensitive client information. Undelivered printed reports are shredded.

Protection of Stored Magnetic Media

- Access to stored magnetic media is restricted to authorized users only.
- Magnetic media are wiped clean of stored information before they are discarded.

**Site Security**
- Physical security of the Data Center is maintained by an extensive anti-pass-back, fully monitored security system, which provides door-level information on all movement in the area and restricts access to authorized personnel.
- Cameras and video monitors allow staff to verify the identity of those requesting access to the area. The monitors and door security are functional twenty-four hours a day, seven days a week.

**Permitted & Restricted Uses of Data**

**Email is not an acceptable medium for transmitting or receiving confidential data.**

<table>
<thead>
<tr>
<th>DATA TYPE</th>
<th>Storage Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IT Managed Computers, Servers, and Storage Devices Residing in Data Center and Approved 3rd Party Services</td>
</tr>
<tr>
<td>Instructional Data</td>
<td>Must be protected by user</td>
</tr>
<tr>
<td>Student Educational Records (FERPA)</td>
<td>✔️</td>
</tr>
<tr>
<td>Protected Health Information (ePHI-HIPAA)</td>
<td>✔️</td>
</tr>
<tr>
<td>Mississippi State Law Notice-Triggering Information *</td>
<td>✔️</td>
</tr>
<tr>
<td>Gramm Leach Bliley (GLBA) student loans application information</td>
<td>✔️</td>
</tr>
<tr>
<td>Payment Card Information (PCI)</td>
<td>✔️</td>
</tr>
<tr>
<td>Sensitive Identifiable Human Subject Research **</td>
<td>✔️</td>
</tr>
<tr>
<td>Export Controlled Research (ITAR, EAR)</td>
<td>✔️</td>
</tr>
<tr>
<td>All Other Non-Sensitive Data</td>
<td>✔️</td>
</tr>
</tbody>
</table>

✔️ Permitted  ✗ Not Permitted  🟢 Permitted Only with Prior Approval and Server Registry Entry
** - Mississippi Data Breach Notification Law “Notice-Triggering Information”
   An individual's first name or first initial and last name in combination with any one or more of the following data elements:
   o Social security number;
   o Driver's license number or state identification card number
   o An account number or credit or debit card

** requires IRB Approval in addition to IT approval.
1 – Refers to systems such as SAP, Sigma ProSAM, Blackboard, Touchnet, etc. that are managed by professional IT staff with the highest security levels.
2 - Box and Google offer a certain level of protection, but each user is responsible for the management of shared access settings to prevent exposure of sensitive data.
3 - Refers to non-mobile, university-issued computers and storage devices connected to the campus network outside of Data Center or within Data Center but not behind most restrictive Data Center firewalls.
4 - Includes university-issued laptops and mobile devices. Mobile devices should not be used for temporary or permanent storage of sensitive data, although, as part of normal usage, data may be cached when it is viewed from these devices. User is responsible for securing mobile devices to ensure that transient sensitive data is not exposed.

See Section 11 (Contractors) for related requirements for externally hosted services.

**Penalties**

A suspected violation of this policy should be reported through proper administrative channels.

- Violations by **faculty members** should be reported to the proper Department Chair, then to the Dean, then to the Provost, who will notify the Security Coordinator.
- Violations by **staff members** should be reported to the supervisor, then to the department head. The department head will then notify the Director of Human Resources and the campus Security Coordinator.
- Violations by **student employees** should be reported to the supervisor, then to the department head. The department head will then notify the Vice Chancellor for Student Affairs and the campus Security Coordinator.

Once suspected violations have been reported through proper channels, the Provost, Human Resources Director, or Vice Chancellor for Student Affairs, the Security Coordinator will make a preliminary investigation into the infraction and specific incident(s). If the preliminary investigation shows just cause for disciplinary action, the case will be reviewed by proper judicial bodies and proper action(s) will be taken. If the preliminary investigation finds just cause for criminal prosecution, the case also will be investigated by the University Police Department.

UM employees found to have violated this policy may be subject to disciplinary action up to, and including, ending of their employment and/or criminal prosecution. UM students
found to have violated this policy may be subject to disciplinary action up to, and including, termination of their employment, expulsion, and/or criminal prosecution.