Information Confidentiality/Security Plan

Summary/Purpose Statement: Defines the plan and policy to protect confidential information for faculty, staff, and students.

Background:

The Gramm-Leach-Bliley 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 ruled that the safeguarding of consumer information wanted by the Act also applies to colleges and universities. Under regulations promulgated in May 2000, colleges and universities are deemed to comply with the Act's privacy provision if they comply with the Family Educational Rights and Privacy Act (FERPA).

General Standards for Safeguarding Customer Information:

To comply with federal requirements to safeguard financial and other confidential information, the University of Mississippi 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 University's main customers are students, a customer is a student, employee, or consumer who has a relationship under which the University provides a financial product or service.

Safeguarding objectives are:

- 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

Called for parts of the security policy and program include:

- Designating an employee to coordinate the information security program. Duties of the Security Coordinator are to look at the program and make modifications needed to comply with all federal and state regulations.
    - The information security program means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, send, dispose of, or otherwise handle, customer information.
- Identifying 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 assessing the sufficiency of safeguards in place to control these risks
- Establishing a risk assessment program 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
- Overseeing service providers by taking steps to select and retain providers that can maintain proper safeguards for customer information
- Contractually calling for service providers to put into effect and maintain the safeguards that are described in this policy
- Periodically evaluating and adjusting the information security program based on the results of testing and monitoring

Information Confidentiality/Security

Justification/Reason

Adequately securing customer information is not only the law but also good business sense. Above all, it is an ethical responsibility to safeguard customer information while in the University's possession. Poorly managed customer data opens doors to identity theft and provides access to sensitive information that could result in loss to customers.

Sensitive Information Collected and Stored

As an educational institution, the University of Mississippi collects, retains, and uses non-public financial/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) with the University
- Transactions with the University's affiliates or others
- Consumer reporting agencies
- State, federal, and other governmental agencies
- Personal information (Social Security number, birth date, grades, and so on)
- Research Sensitive Information

Sharing Information with Affiliates

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

How Information is Protected

Protection of non-public financial/confidential information is of vital importance to the University. Providing for administrative, technical, and physical safeguarding of individual's privacy is an obligation. Employee access to customer information is restricted to those who

have a legitimate business reason for getting such information and those employees are educated about confidentiality and customer privacy. As a part of this commitment, the following Privacy and Safeguarding Sections have been adopted.

Section 1 - Accountability

The University of Mississippi is responsible for maintaining and protecting the customer financial/confidential information under its control. Each functional area of the University possessing this type information will educate its employees and comply with these Sections.

An employee in each functional area is identified as its Information Security Custodian. The custodian is responsible for ensuring that policies and procedures are fulfilled for his/her functional area. The custodian also will maintain an inventory of all protected and document changes that occur to the collection, storage, or disposal of information.

Section 2 - Purpose

The purposes for which customer financial/confidential information is collected will be identified before, or at the time, information is collected. If financial/confidential information is maintained in a functional area of the University, a written statement must be held in the area, stating the information, how it is being used, how long it will be held, and how it will be destroyed ***(see UM Records Retention Policy).*** The Internal Auditing Office will help custodians identify confidential information and state the reason for its collection.

Section 3 - Collection

Student/customer information collected must be limited to purposes identified by the University and must be collected by fair and lawful means. 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.*

Section 4 - Use, Disclosure, and Retention

The University of Mississippi 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 it is called or permitted by law. Customer information may only be retained for the time noted in the University's 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.

Section 5 - Safeguarding

Customer information must have safeguards proper to the information's sensitivity. Each

functional area must review the information it retains and set up the right physical and procedural safeguards for the data.

- Paper data such as copies of checks must be kept in locked rooms and file cabinets.
- Data stored on computers can be protected by password-activated screensavers, using strong passwords of at least eight characters, changing passwords periodically, and not posting passwords near employees' computers, in a notebook, on a desk leaf, or online.
- Computer systems with sensitive data must have a personal firewall installed and operational
- Calls or other requests for customer information should be routed to a designated individual who has been trained about its use, disclosure, and retention.
- Be on the alert for fraudulent attempts to get customer data and report these to the Internal Auditing Office for evaluation.

Data custodians, in conjunction with the Office of Information Technology, provide the training and oversight needed to insure the proper safeguarding of customer information.

Central Data Center Security

The Office of Information Technology department maintains and provides access to policies and procedures that protect against anticipated threats to the security or integrity of electronic customer information and guard against the unauthorized use of such information.

- **Site security.** Physical security of the Central 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.
- **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) and passwords that are changed on a regular basis. Some critical systems feature support accounts which can only be accessed at defined physical locations to deter online attacks or intrusions.
- **Data Security**. Data access above the account level is maintained via a layered firewall implementation which 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.
- **Protection of printed materials.** Printed reports are delivered ONLY to approved locations and personnel, and are never distributed in a way which 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.
- **Offsite system backups.** Intended for use in disaster recovery procedures, offsite data

backups are stored in a vault in another building on campus.

- **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.

Section 6 - Recommended Departmental Safeguards and Responsibilities

The following safeguards and responsibilities are recommended for departments that use internal servers or shadow systems to capture, store, and distribute confidential data.

- Appoint a person to be responsible for data confidentiality and security
- Develop a data security plan based on the type of information got and stored on departmental servers.
- Report issues about the maintenance of confidentiality of customer data to David Drewrey (davidd@olemiss.edu) , the Security Coordinator.
- Maintain a written document that details information security policies and procedures for each relevant area and make it available to the Security Coordinator on request.

Also, departments should follow these guidelines to help safeguard data:

Accounts

- The user of an account is governed by the Appropriate Use Policy (AUP) and must adhere to this policy whether gaining the account on or off-campus. All employees should read and adhere to the AUP.
- The user of an account is responsible and liable for all processes started from the 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. Passwords should be a minimum of 8 characters and changed every ninety (90) days.
- There should be no group accounts.
- Remove unnecessary preconfigured or default accounts that have generic or nonexistent passwords.
- Change the password to default accounts before attaching the system to the network.

Anonymous FTP ---- Anonymous FTP SHOULD NEVER be allowed in Conjunction with Confidential data---

- Place the ftp directory tree in its own restricted directory area.
- Delete all user account information from the ~ftp/etc/passwd file or replace the encrypted password fields with an asterisk.
- Make the ftp/bin and ftp/etc directories execute only. Make sure root owns ~ftp/pub, ~ftp/etc, and ~ftp/bin.
- Make the ~ftp/pub directory read and execute only. If you wish to have a place for anonymous users to leave files, create the directory ~ftp/pub/incoming. This directory is owned by root with permissions 733.

Auditing

- Review logs daily as part of your security plan and question unusual traffic patterns.
- Keep logs secure.

Authentication

- Passwords should be at least eight characters.
- 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 leafs, 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.

Backups

- Make full backups weekly.
- Store a monthly backup offsite.
- Test the restore process.

Equipment Disposal

- When disposing of old computer equipment, hard disks, diskettes, or tapes, make sure the magnetic media is physically destroyed. The IT Helpdesk at 915-5222 can provide instructions on how to permanently erase data on disks or computers prior to salvage.

Firewalls

- Computers and servers must have personal desktop firewall 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 2 or more computers with this level of secure data.

Mail Relay

- The mail relaying feature must be disabled for hosts outside the olemiss.edu domain. If needed, permission can be added for specific outside hosts that need to use campus mail servers.
- For help in closing the mail relay feature on computers, call the Helpdesk at 915-5222.

Patches

- The computer should be configured to check for OS patches daily.
- Be alert for University security announcements that may be about your OS or equipment. It is much easier to stay abreast of patches and use an exploit for which a patch exists than to rebuild a system that has been compromised.

Risk Analysis

- Map the network.
- List your assets.
- Know your vulnerabilities.

SSH (Secure Shell)

- Replace rlogin, rsh, and rcp with ssh.
- Provide secure X connections and secure forwarding of arbitrary TCP connections.

TCP/IP

- Edit the inetd configuration to stop unnecessary TCP/IP services.

- Stay abreast of security issues for 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 equiv entries. Ideally, the .rhost capability should be permanently disabled.

Verify Binaries

Make sure that system files have not been replaced or manipulated by hackers.

Viruses

Computers and servers must have software installed to protect against viruses from the internet or other machines. The software should be configured to automatically check the vendor site daily for updates.

The campus e-mail server has virus protection software that traps viruses before they reach departmental servers and computers. But, it is recommended that virus protection software be installed on all departmental servers and computers, and be used to scan regularly. The Office of Information Technology department recommends using off-the-shelf virus scanning tools such as Norton Utilities or McAfee.

- When a virus is detected, immediately disconnect machines from all networks and contact your systems administrator.
- The systems administrator should contact all users with access to the infected system, explain how to find out if their system is infected, and how to remove the virus.
- If you do not have a systems administrator, call the IT Helpdesk at 915-5222.

Section 7 - 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, if proper. The date, time, and signature of the person changing the data should be logged. Each department/unit is responsible for getting and presenting information when requested by a customer.

Section 8 - Handling Customer Complaints and Suggestions

Students/customers may direct questions about the privacy principles or practices outlined above to the person(s) designated accountable for privacy in each University department/unit or functional area. 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 of supervision.

Section 9 - Information Systems

Information systems include not only network and software design but also information collection, processing, storage, transmission, retrieval, and disposal. Security must be

maintained throughout the life cycle of customer information.

The University of Mississippi maintains centralized control of public and non-public data through various functional areas. These areas maintain their own internal security measures, which are administered by the area's assigned Information Security Custodian.

Physical access to the University's centralized computers is controlled by a card access system to the Central Data Center. Access to this building is restricted to those who have a showed need. All access to the Data Center is granted by the Chief Information Officer.

Information Technology maintains offsite storage of institutional data for disaster recovery purposes. Data tapes are kept in a locked vault inside the building, which is secured with continuous intrusion and fire detection systems.

Transmission of institutional data is routed through the campus network, which is a switched 10/100/1000 Ethernet network. Physical security of the network is provided by locked doors to communication distribution areas. Where possible, data transmission is encrypted. For example, web-based services that use non-public, authenticated data are usually encrypted using SSL.

Institutional data transferred to personal computers and mobile storage devices is the responsibility of the end user, who is responsible for ensuring that the data is securely maintained and properly destroyed.

The University requires that all data be erased, beyond recovery, from computers, hard disks, diskettes, or tapes before they are sold, salvaged, or discarded. Hard drives, diskettes, and other permanent storage media containing confidential data is to be salvaged where they will be destroyed. In all instances physical storage media containing confidential data is not to be transferred outside the University. Departments with computers that are to be sold or salvaged, or other items to be discarded, should contact the IT Helpdesk for instructions on destruction options.

The University of Mississippi maintains an Information Technology security team to respond to problems arising from intrusions, other security violations, and violations of the Appropriate Use Policy. IT has an assigned group to address tries to violate the integrity of the network. IT maintains a log of incidents and resolution of all security violations.

Section 10 - Monitoring and Testing of Security

Periodically, the Information Confidentiality/Security Program will be evaluated and adjusted based on the results of testing and monitoring. Departments will be notified if adjustments call for changes in procedures or access.

Section 11 - Contractors

In the normal course of business, the University of Mississippi selects, and contracts with, proper 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 customer information. Contracts with service providers will include the following provisions:

- Contractor must acknowledge they are aware of this policy and agrees to abide by its data protection guidelines.
- 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 got into 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 got 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

Section 12 - Revisions to Plan

This plan will be evaluated and adjusted in light of relevant circumstances, including changes in the University's business arrangements or operations, or from testing and monitoring the safeguards. Periodic auditing of each functional area's compliance will be done for each internal auditing schedule. Annual risk assessment will be done through the internal auditor's office. Evaluation of the risk of new or changed business arrangements will be done through the legal counsel's office.

Section 13 – Disposal of Confidential Information

Paper records containing confidential information must be **shredded.** Other paper documents may be recycled. Please contact the Physical Plant (7051) for information about shredding of paper records.

Electronic storage media (CD, hard disk, tape, and so on) must be physically destroyed to prevent data recovery. Please contact the Helpdesk (5222) for instructions and destruction options.

Section 14 - Penalties for Violating the Plan

A suspected violation of the University of Mississippi's Information Security Program 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 David Drewrey (davidd@olemiss.edu), the campus Security Coordinator.
- Violations by **staff members** should be reported to their supervisor, then to their department head. The department head will then notify the Director of Human Resources and the campus Security Coordinator, , David Drewrey (davidd@olemiss.edu).
- Violations by **student employees** should be reported to their supervisor, then to their department head. The department head will then notify the Vice Chancellor for Student Life and the campus Security Coordinator, David Drewrey (davidd@olemiss.edu).

Once suspected violations (unauthorized use or disclosure of confidential information) have been reported through proper channels, the Provost, Human Resources Director, or Vice Chancellor for Student Life B or a designee thereof B 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.

University 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. University 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.

Section 15 - Responding to Security Incidents

The University of Mississippi is committed to responding to any data breaches swiftly and in the most ethical manner as defined by existing best practices. In the event of an incident concerning the possible exposure or loss of sensitive institutional or personal data, those who first become aware of the incident must take immediate action to report the incident to the Security Coordinator. The Security Coordinator will work with the Office of Information Technology to determine the facts surrounding the incident and to immediately enact measures to prevent further unauthorized discloser of sensitive data. The Chief Information Officer will work with the University Attorney and the Public Relations office to determine the most appropriate response, including the notification of affected individuals where appropriate.