

**The University of Mississippi
Department of Human Resources**

**Plan for Creation and Implementation of Procedures for Safeguarding
Customer Information Under the Gramm-Leach-Bliley Act**

May 23, 2003

Section 1 - Types of Records Maintained

The Department of Human Resources maintains the following customer records: names; Social Security numbers; phone numbers; addresses; ACH direct deposit authorization forms; copies of federal tax forms; and other various University reports and records that may contain any information covered under the GLB Act.

Section 2 - Control of Access to Data

The Department of Human Resources remains locked during all non-business hours. All customer information will be maintained in limited access areas within the Department of Human Resources in order to prevent unauthorized use of the customer information. Human Resources staff are trained to protect sensitive information.

Each functional area in the Department of Human Resources will review the information being retained and establish appropriate physical safeguards for the data. Physical paper data will be kept in areas that are limited only to Human Resources personnel. Computer stored data will be protected by utilizing strong passwords of at least eight characters, by changing passwords periodically and not posting passwords near employees' computers, by encrypting sensitive customer information when it is transmitted electronically over networks, and by recognizing any fraudulent attempt to obtain customer information and reporting it to the Internal Audit Department for evaluation.

Section 3 - Methods of Collection of Data

Information may be collected via U.S or campus mail, fax, when an employee or applicant completes and signs a hard-copy document, voice mail, or computer. Manual and electronic methods are used to process the data collected. Most of the data collected is stored in paper form. Additionally, data is also stored on microfiche, CD's, disks, and tapes or electronically in SAP, PeopleAdmin, and E-forms.

ACH direct deposit forms are collected directly from the customer. The customer is required to provide a blank voided check and must sign and date an authorization form.

Section 4 - Distribution of Data

Human Resources is routinely required to provide information to outside individuals or agencies. Information will be released in order to comply with legal requirements. In those instances, information is distributed to those individuals or agencies who have a legitimate need to know.

Human Resources staff will only release information about an employee to other vendors who provide a signed document from the employee requesting that we release the specified information. Also, social security numbers have been removed from mailings, check stubs, applications for employee identification cards, benefits statements, and printable employment applications.

Section 5 - Methods of Processing

Data may be distributed via mail, fax, email, or other electronic means. Bank account information ACH direct deposits is transmitted over the internet during each payroll. Access to this process is restricted to certain employees in Human Resources who are assigned user ids and passwords. Access to the bank website is password protected and each user is assigned to a certain level of authority.

Section 6 - Methods Used to Protect Data

All paper documents related to employee records shall be filed timely in the appropriate office files.

Only authorized personnel shall have access to employee or other office files as required to complete the scope of their job duties.

All documents that contain employee confidential, non-public information not pertinent to any office file or not needed for official records shall be destroyed through the use of a shredding machine only. No documents containing employee confidential, non-public information shall be disposed of, unshredded, in the normal daily trash cycle.

No employee shall enter false statement or information into an employee's record, either electronic or paper, or misrepresent any communication with an employee. Any such action by an employee will result in disciplinary action and possible job dismissal.

All electronic data contained in the University's Information Systems Network will be protected, secured and safeguarded by the University's Information Technology Office.

Employees will be required to stay current on all Federal and State Laws related to the safeguarding, security, privacy and confidentiality of employee records. Furthermore, each employee will be required to read and sign a statement concerning the safekeeping of customer information.

Section 7 - Methods of Storage of Data

Paper documents are stored in filing cabinets in restricted areas. Customer data is also stored electronically on the SAP system as well as the PeopleAdmin applicant system.

Section 8 - How Data is Used

Data is used by Human Resources to provide information to outside individuals or agencies. Information will be released in order to comply with legal requirements. In those instances, information is distributed to those individuals or agencies who have a legitimate need to know or who have a signed release from the employee.

Section 9 - How Data is Transmitted

Customer data is transmitted internally via updating computer records, written documents, email, telephone and fax.

Customer data is transmitted externally via electronic means, written documents, email, telephone and fax.

Section 10 - Methods Used to Dispose of Data

Paper documents will be shredded. Personal computers retired from service will be stored in a safe place until such time that the hard drive can be reformatted.