

University of Alabama at Birmingham

DATA PROTECTION AND SECURITY POLICY

March 19, 2007

(Replaces policy entitled “Electronic Data Processing Security Policy” dated August 5, 1985)

Introduction

In the course of doing business at UAB, electronic information assets (data) are created and must be protected and maintained in accordance with all applicable federal and state laws and university policies. The intent of this policy is to provide a framework that ensures that electronic data, in all of its forms, are adequately protected. This policy specifically outlines:

- The roles and responsibilities of the UAB community for data protection and security;
- Additional requirements associated with the use and maintenance of systems containing sensitive information.

Scope and Applicability of Policy

Managing and protecting data are responsibilities shared by all members of the UAB community. This policy applies to:

- All individuals (faculty/staff/students/visitors), schools, departments, affiliates, and/or other similar entities within the UAB community, including employees of contracted or outsourced non-UAB entities;
- All UAB data and systems including, but not limited to, centralized institutional systems, departmental/ unit systems, systems created or operated by third party vendors under the direction of UAB, and UAB data in any and all of those systems.

POLICY STATEMENT

General Data Protection

Availability of data to the UAB community is critical to conducting business. All members of the UAB community should learn to protect their individual data and data under their control or use by viewing the online UAB General Data Security training program and periodically reviewing all applicable data security, confidentiality, and acceptable use policies.

Protection of Sensitive Data

When sensitive data are used or stored electronically, additional care must be taken to ensure security and confidentiality.

Sensitive Data Defined

Sensitive data include, but are not limited to:

- Individually identifiable information (Example: name and date of birth – see “Information Disclosure and Confidentiality Policy”)
- Social Security numbers
- Credit card numbers
- Driver’s license numbers
- Proprietary research data
- Privileged legal information
- Data protected by law such as student and patient records

Specific Roles and Responsibilities for Protecting and Maintaining Sensitive Data

The following information is provided for members of the UAB community as a guide in understanding their roles and responsibilities in the protection of sensitive UAB data:

Data Custodians

UAB’s central Information Technology (IT) units are responsible for protecting all sensitive information maintained/stored in the institutional information systems. While it is not recommended that sensitive information be stored outside centrally maintained servers and systems, any UAB department or unit that retains sensitive UAB data on departmental/unit servers, personal computers (desk and laptop), personal digital assistants (PDAs), thumbdrives, or computer disks also will be responsible for protecting and securing those data. In the case of information stored in department/unit systems, the department/unit head is charged with responsibility for data protection and designated as the data custodian.

A minimal list of the Data Custodian’s responsibilities may be found on the UAB IT web site <http://www.uab.edu/it/datasecurity>.

System Administrators

System Administrators are individuals within the central IT units or school/department units with day-to-day responsibility for maintaining information systems. They are responsible for following all data security and protection procedures and practices. (See IT Security Practices at http://www.uab.edu/it/policies/UAB_IT_Security_Practices.doc.) System Administrators are further responsible for reporting any data security breaches or compromises to their immediate supervisor. As required by the Data Custodian or department head, they perform risk assessments and data backups. They also provide secure storage, execute disaster recovery plans, and provide system documentation. System Administrators successfully complete specific security and other IT training as required.

Data Users

Data Users are individuals within a department/unit who access/use UAB information systems and data. The UAB data users are responsible for following the acceptable use policies for the

specific systems in use as well as all other applicable policies. Data users should not reuse or save sensitive data on their desktop or laptop computers without approval and appropriate security safeguards in place. Data users are further charged with reporting to their supervisors or managers any activities that could compromise the protection of UAB data.

Incident Reporting and Response Relative to Data Security

Any breach or compromise of UAB data must be reported immediately, especially when it involves sensitive data. Anyone who becomes aware of a breach or compromise should report the incident to his or her immediate supervisor or manager. Department/unit heads are responsible for reporting breaches to the Data Security Office in the Office of the Vice President for Information Technology. Specific procedures for reporting a suspected or actual breach/compromise of data are maintained on the Data Security web site at <http://www.uab.edu/it/datasecurity/index.html>. Upon receiving the report, the Data Security Office will be responsible for conducting or coordinating the investigation, making or assessing a recommendation for corrective action, reporting the incident to the Incident Response Committee or other administrative units as needed, and maintaining documentation of the incident.

Risk Assessment and Risk Management

Department/unit heads are responsible for assessing (in conjunction with UAB Information Technology) the business processes and technical risks associated with implementing any planned or proposed electronic information system or data collection system. Such risk assessments are required when sensitive data are involved and must be updated periodically. Risk assessments must identify specific procedures to manage risks. Approval for the dissemination of sensitive information will be in accordance with the UAB Information Disclosure and Confidentiality policy.

Other Data Security Policies at UAB

Other data security policies implemented at UAB (campus-wide or locally by/for a specific department, school, or system) may be more restrictive than this UAB-wide policy but may not be less restrictive.

Implementation

Data Custodians located both centrally and within departments/units are responsible for implementation of this policy within their areas of responsibility. The Vice President for Information Technology is responsible for overall procedures related to the implementation of this policy and for providing implementation assistance to Data Custodians.

Policy Violation

A violation of this policy by employees, including faculty, shall result in disciplinary action, up to and including discharge, according to established UAB disciplinary procedures. A violation of this policy by a student constitutes nonacademic misconduct, and the student will be subject to established disciplinary action.

DATA PROTECTION AND SECURITY POLICY

March 19, 2007

Page 4

See also the following:

- “Information Disclosure and Confidentiality Policy” (UAB Policy Reference Manual)
- “UAB Policy for Acceptable Use of Computer and Network Resources” (see “Acceptable Use Policy” on UAB Information Security World Wide Web site)
- “Policy for Connecting Devices to the UAB Voice, Data, and Video Network” (UAB Policy Reference Manual)
- “World Wide Web Pages Policy” (UAB Policy Reference Manual)
- Search Policy (Section 10.3 in the *You & UAB Handbook for Faculty and Staff*)
- Related UAB Information Technology procedures, standards, guidelines, and training materials
- Related UAB/UABHS HIPAA Privacy and Security Standards
- Board of Trustees Rule 105 “Ownership and Preservation of Records and Files.” (The Board of Trustees of The University of Alabama Board Manual)
- Data Custodian Responsibilities (<http://www.uab.edu/it>)