

**POLICIES AND PROCEDURES
OUACHITA TECHNICAL COLLEGE**

SUBJECT AREA: Information Technology

POLICY/PROCEDURE: Information Technology Security Policy

DATE: 28 November 2006

NUMBER: 6.04

REVISION(S):

In order to continue to protect private information and data, and to comply with the Federal Trade Commission's Safeguard Rule, the Gramm-Leach-Bliley Act (GLBA), and the Family Education Rights and Privacy Act (FERPA), Ouachita Technical College has implemented this Information Technology Security Policy. Objectives of the Policy are

- To ensure the security and confidentiality of nonpublic personal information about students, staff, and faculty, whether in paper, electronic, or another form.
- To protect against any anticipated threats to the security or integrity of such information.
- To guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student, staff, or faculty.

This policy has five components: (1) designating those responsible for coordinating and executing the policy; (2) conducting risk assessments to identify reasonably foreseeable security and privacy risks; (3) ensuring that safeguards are employed to control risks identified and the effectiveness of these safeguards is regularly tested and monitored; (4) overseeing those accessing student information; (5) maintaining and adjusting this policy based on conducted evaluations.

ROLES AND RESPONSIBILITIES

Each member of the campus community is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

Responsibilities range in scope from security controls administration for large systems [e.g. student information system, financial database] to the protection of one's own access password. A particular individual often has more than one role.

The Vice President of Finance and Administration and the Vice President of Student Affairs/Registrar in close cooperation with the Director of Information Technology and the Security Analyst, are responsible for coordinating and executing this policy. However, each division/department is responsible for compliance with privacy and safeguarding rules.

Administrative Officials (individuals with administrative responsibility for campus organizational units [e.g. department chairs, directors, managers] or having functional ownership of data) must:

- Identify the electronic information resources within areas under their control;
- Establish acceptable levels of security risk for resources by assessing factors such as:
 - how sensitive the data is, such as data or information protected by law or privacy,
 - the level of criticality or overall importance to the campus as a whole,
 - how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
 - how likely it is that a resource could be used as a platform for inappropriate acts towards other entities,
- Ensure that requisite security measures are implemented for the resources;

Providers (individuals who design, manage, and operate campus electronic information resources, e.g. project managers, system designers, application programmers, or system administrators) must:

- become knowledgeable regarding relevant security requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
- communicate the purpose and appropriate use for the resources under their control.

Users (individuals who access and use campus electronic information resources) must:

- become knowledgeable about relevant security requirements and guidelines;
- protect the resources under their control, such as passwords, computers, and data they download.

PARTICULAR RISKS

- privacy and security threats associated with the student information system and the financial information system, as well as information processing, storage, transmission, and disposal of student information, and detecting, preventing, and responding to attacks, intrusions, and other system failures;
- privacy and security threats associated with other software containing student information;

- privacy and security threats associated with paper or electronic forms e.g. application for admission, FISAP, transcript request form, change of major form, course rosters;
- privacy and security threats associated with the electronic or paper transfer of information to those providing services to students or staff.

KEY SECURITY ELEMENTS

Logical Security

- computers must have the most recently available and appropriate software security patches;
- adequate authentication and authorization functions must be provided;
- attention must be given not only to large systems but also to smaller computers which, if compromised, could constitute a threat to campus resources, including computers maintained for a small group or for an individual's own use.

Physical Security

Appropriate controls must be employed to protect physical access to resources commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect a user's display screen.

Safeguards Employed to Control Identified Risks

- users with direct access to central databases are limited;
- mission critical servers and databases secured in a lock room to which only the Information Technology (IT) staff have access;
- to detect attempted intrusions, event logs will be inspected periodically;
- routine traffic and protocol monitoring;
- employee training covering privacy and safeguarding requirements and documentation of such training will be performed at the fall in-service each year with statements of acknowledgements to be signed and placed in personnel files;
- procedures that educate new employee's on privacy and safeguarding requirements upon completion of the "payroll packet" will be performed by the Personnel Officer and documented by signature on the statement of acknowledgement;
- periodic review of the College's disaster recovery plan and intrusion detection plan;
- a published annual review of privacy and safeguarding requirements by the program coordinators.

Vice Presidents, directors, and supervisors are ultimately responsible for overseeing employees accessing covered information and ensuring compliance with information security practices.

The Coordinators, working with responsible department/divisions, will annually evaluate the information security program. Adjustments will be made based on risk identification, security audits, other assessment activities, material changes to the College's operations, or other

circumstances that may have an impact on the program.

AUTHENTICATION (Signature):

COPP

President

28 November, 2006
(Date)

6.04

