Information Security Procedure 6.01(a)

Chapter 6: Information Technology

In order to protect personal critical information and data, Rhodes State College will comply with the Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley (GLB) 15 U.S.C. §6801). The following procedures guide the related institutional operations.

I. Risk Assessment and Safeguards

For the purposes of risk assessment and safeguards, the Coordinator must work with all relevant areas of the College to identify potential and actual risks to security and privacy of information. Each Department head, or his/her designee, will conduct an annual data security review, with guidance from the Coordinator. Vice Presidents will be asked to identify any employees in their respective areas that work with covered data and information. In addition, the relevant components of IT will conduct a quarterly review of procedures, incidents, and responses, and will publish all relevant materials except in those cases where publication may likely lead to breaches of security or privacy. Publication of these materials is for the purpose of educating the College community on network security and privacy issues. IT will assure that procedures and responses are appropriately reflective of those widely practiced at other state colleges and community colleges, as measured by four advisory groups: The Educause Security Institute, The Internet2 security working group, the SANS Top Twenty risks list, and the Federal National Institute of Standards and Technology (NIST) Computer Security Resource Center.

In order to protect the security and integrity of the College network and its data, IT will develop and maintain a registry of all computers attached to the College network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine has or has special access to any confidential data covered by relevant external laws or regulations.

IT assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date, and will keep records of patching activity. IT will review its procedures for patches to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly.

IT bears primary responsibility for the identification of internal and external risk assessment, but all members of the College community are involved in risk assessment. IT, working in conjunction with the relevant College offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB.

IT, working in cooperation with relevant College departments, will develop and maintain a data classification procedure, listing those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, development, etc.). IT and the relevant departments will conduct ongoing (at least biannual) audits of activity, and will report any significant questionable activities.

IT will work with the relevant offices (Business Services, Human Resources, the Registrar, and Student Services among others) to develop and maintain a registry of those members of the College community who have access to covered data and information. IT in cooperation with Human Resources and Business Services will work to keep this registry rigorously up to date.

IT will assure the physical security of all servers and terminals which contain or have access to covered data and information. IT will work with other relevant areas of the College to develop guidelines for physical security of any covered servers in locations outside the central server area. The College will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the College to risks.

While the College has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some College employees on the use of social security numbers. Social security numbers are considered protected information under both GLB and the Family Educational Rights and Privacy Act (FERPA).[1] By necessity, student social security numbers still remain in the College student information system.[2] The College will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover College employees as well as subcontractors.

IT will develop a plan to ensure that all central databases are strongly protected from security risks.

It is recommended that relevant offices of the College decide whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees, for example employees handling confidential financial information.

[1] 20 U.S.C. § 1232g

[2] Social Security Numbers are kept both for historical purposes and due to the requirements of 26 U.S.C. § 6050S, the tuition payment credit reporting requirements.

IT will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

The Information Security Coordinator will periodically review the College's disaster recovery program and data-retention policies and present a report to the College leadership.

II. Training and Education

Directors and supervisors are ultimately responsible for ensuring compliance with information security practices, however IT will work in cooperation with Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all College data; custodians of data as identified in the data classification procedure, and those employees who use the data as part of their essential job duties.

III. Violations of Policy and Disciplinary Actions

Rhodes State College employees are expected to comply with this College Policy. Any reporting of non-compliance should be directed to the Office of Human Resources.

Reported violations may result in corrective action up to and including termination as outlined in Disciplinary Action and Due Process Policy 5.5.

Related Policies and / or Procedures:

Information Security Policy 6.01
NIST Requirements Handbook
Disciplinary Action and Due Process Policy 5.5

History:

	Date:	Reason:
Issued:	11/15/2022	Original Issue Date
Revised:	MM/DD/YY	

This policy and / or procedure provides operating principles for Human Resources issues at Rhodes State College. It supersedes any prior policy or procedure covering specific subject. This policy and / or procedure may be suspended, modified or cancelled as determined by the College. This policy and / or procedure does not create a contract of employment, nor is it a condition of employment between the College and its employees.