New River Community and Technical College

GLBA Requirements for Higher Education Institutions

Employee Training and Management

- Awareness and Training
    - Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
    - Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- Media Protection
    - Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.
    - Limit access to CUI on information system media to authorized users.
    - Sanitize or destroy information system media containing CUI before disposal or release for reuse.
- Personnel Security
    - Screen individuals prior to authorizing access to information systems containing CUI.
- Physical Protection
    - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
    - Protect and monitor the physical facility and support infrastructure for those information systems.

Information Systems Design, Storage, Transmission, and Disposal

- Access Control
    - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
    - Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.
- Configuration Management
    - Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware,

and documentation) throughout the respective system development life cycles.
    - Establish and enforce security configuration settings for information technology products employed in organizational information systems.
- Identification and Authentication
    - Identify information system users, processes acting on behalf of users, or devices.
    - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- Maintenance
    - Perform maintenance on organizational information systems.
    - Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- Systems and Communications Protection
    - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

PREVENTION, DETECTION, AND RESPONSE TO THREATS

- Audit and Accountability
    - Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
    - Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
- Configuration Management
    - Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
    - Establish and enforce security configuration settings for information technology products employed in organizational information systems.
- Incident Response
    - Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
    - Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
- Personnel Security
    - Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

- Security Assessment
    - Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
    - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
    - Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
    - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
- Systems and Communications Protection
    - Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- System and Information Integrity
    - Identify, report, and correct information and information system flaws in a timely manner.
    - Provide protection from malicious code at appropriate locations within organizational information systems.
    - Monitor information system security alerts and advisories and take appropriate actions in response.