New River
Community and Technical College

Gramm-Leach-Bliley Act:
Compliance Procedures

Version:	1.0 (December 6, 2023)
Approval Authority:	Dr. David J. Ayersman, Vice President and Chief Information Officer

Executive Summary

This document summarizes New River Community and Technical College's ongoing efforts to comply with the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act (GLBA).

These **GLBA Compliance Procedures** serve as both an internal procedure as well as a concise explanation of the GLBA minimum safeguard requirements.

Additionally, it serves as documentation for New River's continuing control measures and compliance efforts.

Three primary GLBA requirements include:

I. Designate Individual

The name of the individual responsible for New River Community and Technical College's information security program and point of contact for GLBA compliance is the CIO.

Dr. David J. Ayersman
Phone: 304-256-0281
Email: dayersman@newriver.edu
Postal: 280 University Dr, Beaver, WV 25813-8987

II. Perform Risk Assessment

New River began completing the annual NCSR (Nationwide Cybersecurity Review) in 2021 for the year 2020.

The NCSR was last completed on **October 17, 2022,** for the year 2021.

Copies of NCSR results are presented to the President's Cabinet, approved by the President, and available from the CIO.

III. Documented Safeguards

There are eight minimum safeguards that must be addressed to satisfy GLBA requirements. These safeguards and New River's ongoing efforts for compliance are as follows:

1. **Implement and periodically review access controls.**
    a. Annual audits are conducted by New River's internal auditors (Suttle and Stalnaker) and cyber insurance provider (BRIM) to assess ongoing reviews of access controls.
    b. Annual self-assessments using the NCSR are completed by the CIO to enable New River to identify and prioritize improvements to access controls. The CISO and CTO help to determine these priorities and to manage these access controls.
2. **Conduct a periodic inventory of data to note where it is collected, stored, or transmitted.**
    a. New River classifies data into three categories: Low, Moderate, and High Impact (*see Appendix A*).
    b. The use of removable media and personal Cloud storage services for storing Moderate and High Impact data is discouraged.
    c. New River is currently phasing out the use of internal shared drives for storing Moderate and High Impact data and will soon require employees to store this data in Corporate OneDrive folders, that can be managed and recovered by administrators.

3. **Ensure that customer data are encrypted at rest and in transit.**
    a. Customer data stored using Microsoft 365 OneDrive storage or transmitted using Outlook email are encrypted both at rest and in transit (*see Appendix A*).
    b. Archives of email are stored using a Tangent DataCove device that uses 256-bit AES encryption.
4. **Assess applications developed by the organization.**
    a. Few applications are developed internally, but those that have been developed rely on industry best practices for security and access. The CTO supervises this internal development of applications in compliance with established server build standards and controls.
5. **Implement multi-factor authentication (MFA) for anyone accessing customer information on the institution's system.**
    a. Prior to July 2023, MFA was optional for users.
    b. In July 2023, New River began requiring MFA at the SSO portal.
    c. MFA at the desktop for publicly accessible computers is a project currently underway.
    d. MFA for VPN is underway with a hosted provider.
6. **Dispose of customer information securely.**
    a. Data retention policies are automated for departing employees, so that Administrators have 30 days to recover data before it is securely deleted.
    b. The DataCove email archive is automated to ensure that copies of email for all users are maintained in compliance with WVHEPC retention requirements (see https://web.newriver.edu/procedures/email-archive-procedure.pdf).
    c. Employment search and selection records are retained in compliance with record retention guidelines (see New River Procedure #4 - https://www.newriver.edu/wp-content/uploads/2018/04/procedure_4_employment_search_and_selection_8_4_2014.pdf).
    d. The Data Standards and Procedures manual guides compliance with record retention requirements and efforts (see https://web.newriver.edu/procedures/Data-Standards-and-Procedures-Manual.pdf).
    e. Prior to decommissioning end-of-life devices, drives are securely scrubbed of all data by contracted equipment disposal vendors.
7. **Anticipate and evaluate changes to the information system or network.**
    a. The New River infrastructure and network are dynamic, with ongoing changes to improve security and update devices and software. Keeping pace with innovation and decommissioning end-of-life hardware is an ongoing challenge.
    b. Changes are prioritized and implemented as projects and tasks that support the Information Technology Plan, Library Services Plan, Strategic Master Plan, and the Facilities Master Plan. These plans are currently being updated in 2023 and 2024 to reflect the current and near-future needs of the College.

8. **Maintain a log of authorized users' activity and monitor for unauthorized access.**
    a. User and device activity logs are managed and monitored using the Microsoft 365 administrator dashboard.
    b. Network traffic logs are managed and monitored by a third-party vendor using built-in logging functions provided on each device and controllers. Cisco ASA firewalls that currently lack this auditing function will soon be replaced with NGFW devices to enable this data collection and monitoring.

Additionally, GLBA safeguards require that New River address the following three areas:

a. **Employee Training and Management**
    a. New River purchased and began using a solution for cybersecurity and privacy awareness training named **KnowBe4** and it was implemented in Fall 2019 for all employees. Each month all employees receive training with information sent to them by email, and periodically, the system sends email messages to test phishing detection abilities of employees. If a user fails to detect the phishing attempt, they are given remediation training and notifications are sent to the system administrators.
    b. New River also utilizes **Linkedin Learning** to supplement and extend training for privacy awareness with employees and students.

b. **Information Systems, Information Processing, and Disposal**
    a. Each July, New River undergoes an annual internal audit to assess and review IT policies, procedures, and guidelines that address acceptable use guidelines, antivirus standards, patch management updates, hardware/software acquisition, change control, physical security, password requirements and guidelines, portable devices, virtual private networks, wireless networking, remote access, asset disposal, capacity monitoring, data backups and restoration, and disaster recovery. These annual audits validate that existing procedures and measures are adequate to address risks or they identify issues where improvements are needed. Improvements are prioritized and addressed by the Vice President and Chief Information Officer in conjunction with the Data Governance team and the Information Technology Services staff. Changes and improvements are completed and this GLBA Compliance Procedures document is updated to evidence these changes.

c. **Detecting, Preventing, and Responding to Attacks**
    a. The Vice President and Chief Information Officer coordinates with members of the Information Technology Services department and the Data Governance team to evaluate procedures for and methods of detecting, preventing, and responding to attacks or other system failures, existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. Post-incident response efforts guide improvements and Incident Response Plans are updated accordingly.

b. New River adheres to the WVHEPC **Incident Response Plan** to report and respond to threats as they are encountered and identified. Additionally, internal plans, policies, and procedures are relied upon to respond to cyber incidents.
c. Email is scanned at the gateway by a *Barracuda* email security gateway device to detect and block spam, malware, and viruses, and, as a result, users can review any blocked messages safely prior to receiving them.

Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The CIO, on a regular basis, implements safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers. The CIO coordinates with those responsible for third-party service procurement activities to raise awareness of, and to institute methods for, selecting and retaining only those service providers that can maintain appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access.

New River utilizes a **Standard Terms and Conditions** agreement with third-party vendors for all new and renewed contracts for services relative to information privacy requirements entered after **November 2020**. Developed by the CIO, this information is implemented and managed by the CFO.

Program Adjustments

The CIO is responsible for evaluating and adjusting these safeguards based on periodic reviews of risk identification and assessment activities.

Approved by:

CIO (Chief Information Officer)

David J. Ayersman, Vice President and Chief Information Officer

Signature

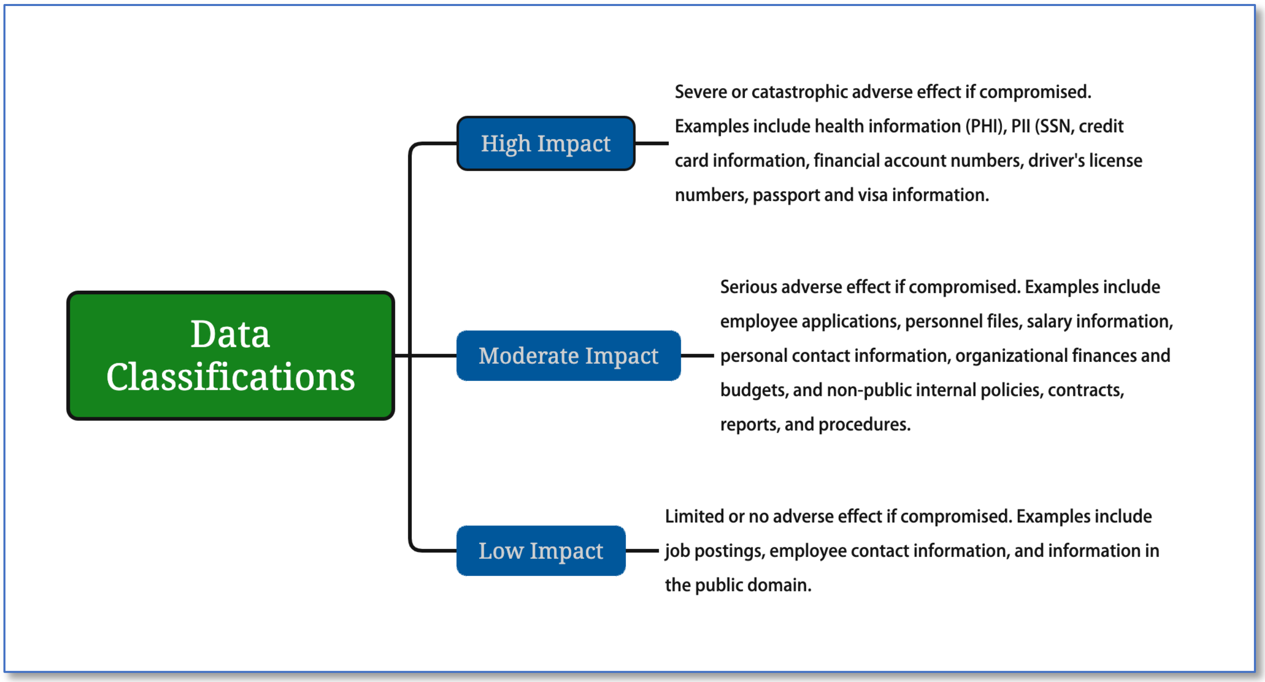
11/23/2023

Date

Appendix A—Data Classification and Storage

A data classification procedure educates users on what type of information is allowed to be stored on the OneDrive, shared drives, and communicated by email. Although all these methods are expected to be *somewhat* secure, none are secure enough for *some types* of personal information.

New River classifies data assets using three levels of impact (see diagram below).



Severe or catastrophic adverse effect if compromised. Examples include health information (PHI), PII (SSN, credit card information, financial account numbers, driver's license numbers, passport and visa information.

Serious adverse effect if compromised. Examples include employee applications, personnel files, salary information, personal contact information, organizational finances and budgets, and non-public internal policies, contracts, reports, and procedures.

Limited or no adverse effect if compromised. Examples include job postings, employee contact information, and information in the public domain.

Office 365 uses encryption to secure data both at rest and in transit, which means that sending within the New River tenant (newriver.edu) is considered secure. If you use Office 365 to share information with anyone outside the New River tenant, we must assume it is no longer secure.

Outlook email is encrypted so that data in transit is secure. Attached files, as well as the email contents, are encrypted so that only the Sender and the Recipient of the information may access it.

Although Office 365 encryption technically does work with some services outside the New River tenant (Outlook.com, Yahoo!, Gmail, and some other email services), it is recommended to use additional security measures when **Highly Sensitive** information is shared outside the New River tenant. Password-protecting PDF versions of the data and sharing the password by a different communication method is recommended.

A recent inventory of New River's data assets revealed that internal shared drives have proven to be a recent vulnerability. In response, New River is phasing out the use of internal shared storage locations and personal cloud storage areas to migrate Moderate and Highly Sensitive data storage to corporate OneDrive folders.

New River's procedure is guided by the following table when determining where to securely store information. The table below shows *Data Classification* in the first column and *Storage Locations* in the additional columns.

Data Classification ↓	**Storage Locations**			
	College Managed Servers (on premise or Cloud)	**Internal Shared Drives** (e.g., T:\, etc.)	**Office 365** (Outlook, OneDrive, or Teams)	**Personal Cloud Storage** (Dropbox, Google, etc)
Public	YES	YES	YES	YES
Sensitive	YES	YES	YES	YES
Highly Sensitive: FERPA	YES	YES	YES	NO
Highly Sensitive: HIPAA	YES	YES	YES	NO
Highly Sensitive: SSN	YES	SOME	SOME	NO
Highly Sensitive: PCI	NO	NO	NO	NO

Additionally, while data on the front of credit cards (Cardholder Data) can be legally stored (only if needed and it must be rendered unreadable through encryption), the PIN or CVV should *never* be stored. Even encrypted information should be deleted when it is no longer needed or as data retention timelines expire.