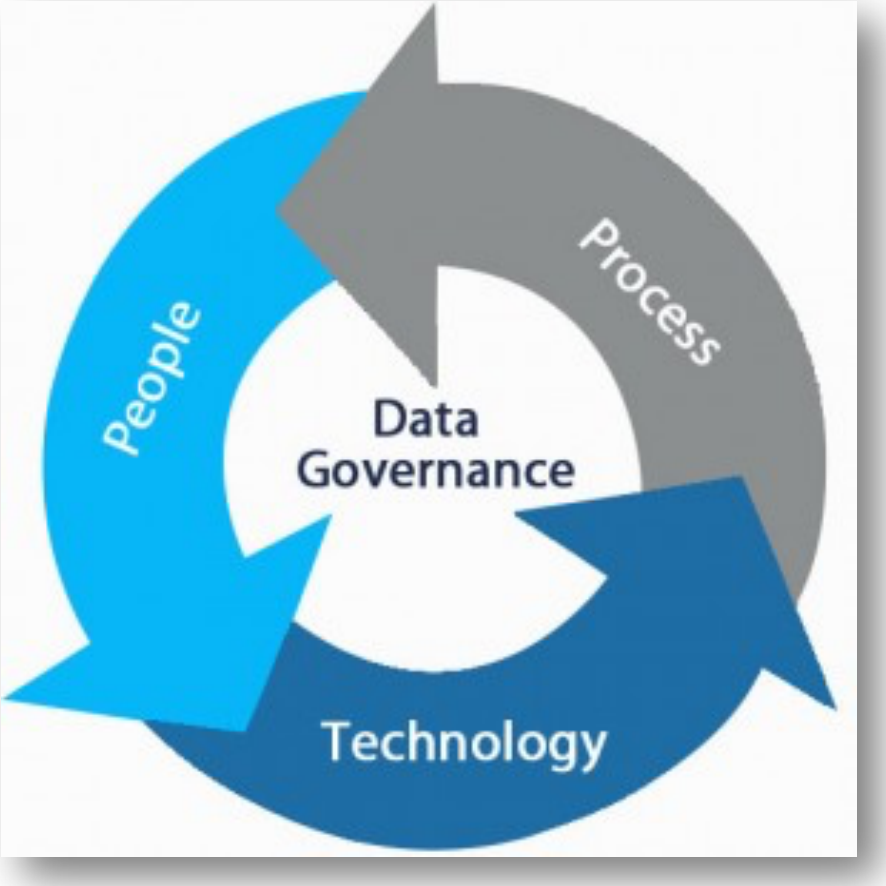
New River
Community and Technical College

Data Governance Plan

2021 through 2025



We are drowning in information and starving for knowledge.
– Rutherford D. Rogers

Resulting from several years of effort, this plan was created by David Ayersman, Dara Fann, Jason Garris, Steve Garlow, and Steve Lacek and completed in 2021. It will be shared with the President's Cabinet for approval and then shared with and implemented by all employees who have some level of data governance responsibility.

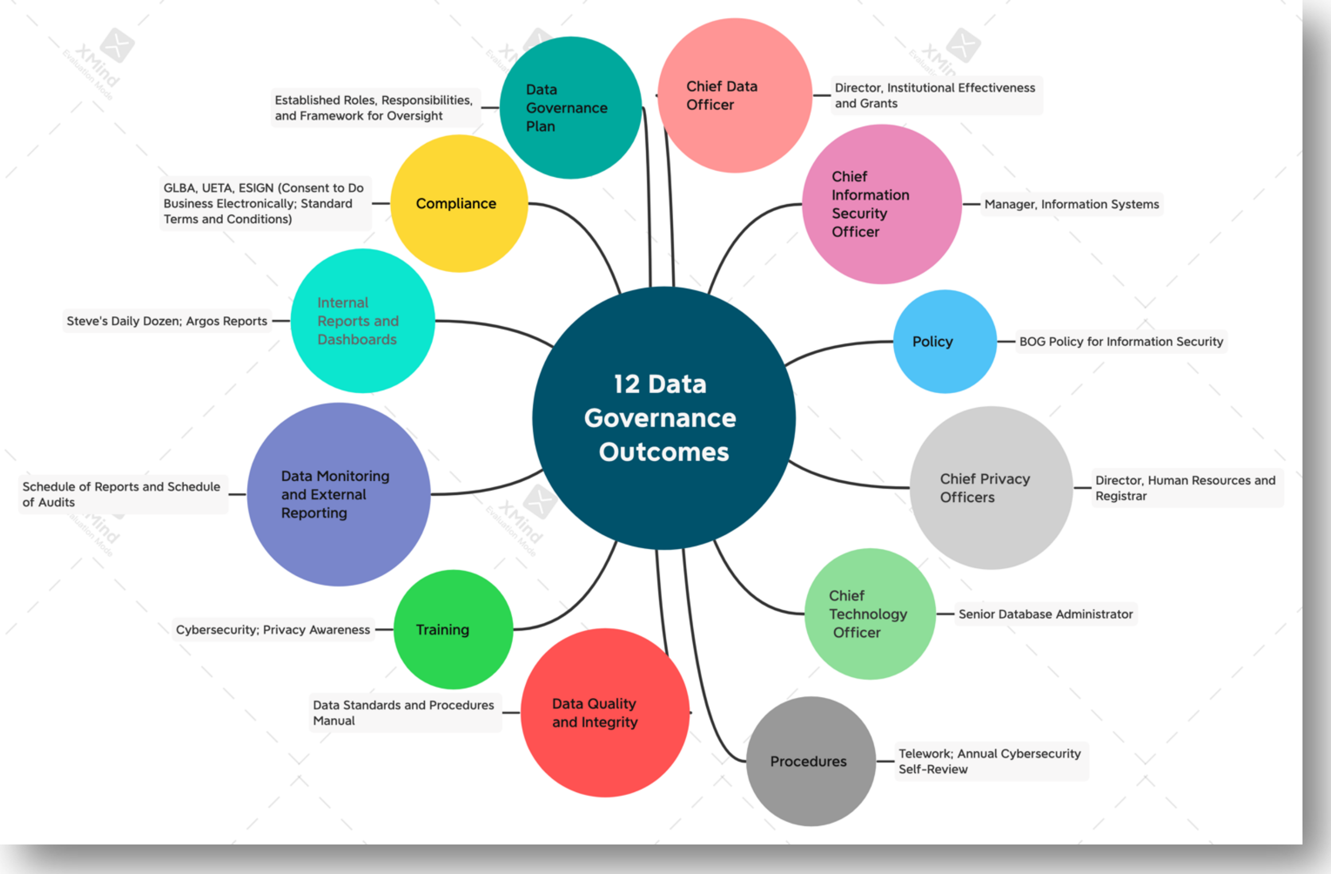
Table of Contents

EXECUTIVE SUMMARY

Creating this **Data Governance Plan** required tremendous effort from multiple individuals spanning more than several years. It is a testament to the fortitude of these individuals that despite numerous challenges, they endured to self-educate on rapidly developing compliance requirements while learning about best practices and drawing from their own personal experiences acquired as they fulfilled their day-to-day responsibilities—to create this plan. We thank them.

Businesses that implement data governance programs benefit by improving customer satisfaction, increasing operational efficiencies, maximizing revenues and creating competitive advantages. By creating this plan, New River has established clear assignments of responsibility for data governance, as well as a framework for managing it, new policies, new procedures, new reports, new dashboards, and new schedules for audits and reports. New training has also been developed and assigned, which improves our security while satisfying compliance requirements.

Developing this plan has had many positive outcomes, but the following graphic highlights 12 tangible results achieved from creating this plan:


12 Data Governance Outcomes
Data Governance Plan
Established Roles, Responsibilities, and Framework for Oversight
Chief Data Officer
Director, Institutional Effectiveness and Grants
Compliance
GLBA, UETA, ESIGN (Consent to Do Business Electronically; Standard Terms and Conditions)
Chief Information Security Officer
Manager, Information Systems
Internal Reports and Dashboards
Steve's Daily Dozen; Argos Reports
Policy
BOG Policy for Information Security
Data Monitoring and External Reporting
Schedule of Reports and Schedule of Audits
Chief Privacy Officers
Director, Human Resources and Registrar
Training
Cybersecurity; Privacy Awareness
Chief Technology Officer
Senior Database Administrator
Data Quality and Integrity
Data Standards and Procedures Manual
Procedures
Telework; Annual Cybersecurity Self-Review

With no budget for this initiative and striving to maximize efficiencies, we capitalized on existing resources by simply identifying the personnel already responsible for the very important tasks and responsibilities associated with data governance. This plan ensures that New River is compliant with federal, state, and local requirements.

BACKGROUND AND OVERVIEW

In 2014, New River received an action plan from Ellucian as a free consultation intended to strengthen our data governance structure. That plan recommended we procure services from Ellucian to assist us with creating a data governance structure to formalize our procedures for identifying responsibilities and developing procedures related to how we manage our data as a resource. While this purchase was not possible at the time, we did use the information to create internal groups of users responsible for data governance. And a few of these users banded together after the Ellucian Action Plan ended in 2016 to continue these efforts.

These continued efforts began with a small group of Data Stewards (composed of only Dara Fann, Steve Lacek, and Dave Ayersman) to do some initial research and planning during the summer of 2018. Since then, much has been accomplished and many more individuals have contributed to this effort. One result of these combined efforts is this plan for data governance.

There are many constraints that impacted this initiative. Assumptions we made from the outset of planning were that:

(1) we have no additional budget or personnel for this initiative,
(2) our timeline is self-created and somewhat flexible although we will strive to complete this project as a high priority, and
(3) the overall initiative will be broken into smaller and more manageable tasks that will require buy-in and support from multiple personnel (and supervisors).

Through the creation of a data governance structure, we will identify data **owners** and **stewards** to be responsible for specific systems as well as internal procedures (working collaboratively with the **Chief Data Officer**, the Retention and Records Committee and others) to create a formal understanding of how the College manages its data resources. Existing personnel with these responsibilities will be clearly identified and will obtain expertise and information from external sources, such as the **Data Governance Institute** and **Linkedin Learning**.

The Data Governance Institute (DGI) is an excellent source of in-depth, vendor-neutral best practices and guidance for data governance. The framework they provide is used throughout the world as a basis for data governance programs. The DGI Data Governance Framework is designed to assist organizations and we learned from it and applied it to our own plan. The following is a quote from their site:

> *All organizations need to be able to make decisions about how to manage data, realize value from it, minimize cost and complexity, manage risk, and ensure compliance with ever-growing legal, regulatory, and other requirements. Management and staff need to*

> *make good decisions – decisions that stick. They need to reach consensus on how to "decide how to decide." They need to create rules, ensure that the rules are being followed, and to deal with noncompliance, ambiguities, and issues. In short, they need to do more than manage data; they need a governance system that sets the rules of engagement for management activities. Small organizations, or ones with simple data environments, may be able to succeed in these goals through an informal system of governance. They may not even be aware of when they are switching between making management decisions and broader governance decisions. On the other hand, larger organizations, or ones with more complex data or compliance environments, generally find that they need to step back and agree upon a more formal system of governance.*

MILESTONES AND TIMELINE

Early in our planning process for creating this plan, we utilized a *Planning and Roadmap Tool* to develop both high-level and detailed tasks that comprised the overall initiative. We then created this table (see below) of key milestones and a timeline to complete these milestones to guide our planning. This information provides an effective high-level overview of this data governance initiative.

Milestones	Who/Status	Timeline
Identify Data Governance Requirements	Stewards	05/2018
Research Data Governance Topics and Locate Supporting Information	Stewards	05/2018
Identify Current State and Complete Gap Analysis	Stewards	05/2018
Develop Responsibilities by Role	Stewards	06/2018
Create and Complete **Data Governance Training**	Stewards	06/2018
Create a Project Communication Plan	Stewards	09/2018
Establish "**Daily Dozen**" criteria for monitoring institutional health	CDO	08/2019
Cybersecurity Awareness Training *(using KnowBe4)*	CIO and CISO	01/2020
Information Security Policy	Board Approved	10/2020
Standard Terms and Conditions *(to establish privacy and security compliance with vendors)*	Cabinet Approved	11/2020
Privacy Awareness Training *(using Linkedin Learning)*	CIO and CISO	11/2020
GLBA Compliance Procedures	CIO	04/2021
Telework Policy and **Memorandum of Agreement**	Pending Cabinet Approval	04/2021
Monitor Data Governance Efforts *(Calendar for Audits and Reports for both HEPC/IPEDS and Routine Reporting)*	CDO and CTO	05/2021
Create Schedule for **Data Reporting Requirements** *(see Section 7 - Monitoring)*	CDO and CTO	07/2021
Data Governance Plan	Pending Approval	07/2021
Data Standards and Procedures Manual	Pending Approval	08/2021
Consent to Do Business Electronically	Pending Approval	08/2021
Information Security Procedures *(define procedures for managing the lifecycle of data, security of that data, and establishing methods for auditing these procedures to maintain quality)*	CIO and CISO	12/2021

Dashboards, **reports** and other solutions to enhance leadership's view of key indicators of institutional health *(define the key indicators, keep it simple; make it securely accessible; model it after a proven solution)*	CTO, CDO, and Owners	12/2021
Develop a dynamic **Business Data Glossary** *(to provide Data Definitions for Banner and then other enterprise systems)*	CTO and Owners	12/2021

*NOTE: From the table above, the items that have been completed are color-coded as **white** while those still underway are **yellow**.*

This plan connects related organizational initiatives and obligations as appropriate. For example, BRIM provides the College an insurance policy that has recently been modified to include coverage for cyber information security and privacy. There are clear expectations for the College to address a number of issues in this area while providing documentation and evidence of completion (evidence of confidentiality agreements, privacy awareness training, etc.). An effective *Information Security Procedure* will encompass much of this and we simply haven't yet created such a procedure for the College. This procedure (and others) will be created as components of this data governance initiative. Once completed, it is our hope that having these procedures in place will allow for additional procedures, standards, and guides for meeting the needs of an increasingly technology-savvy workforce. But clearly, we see establishing parameters for data security and management as foundational and as a prerequisite to this type of more detailed refinement.

The Plan

1. Vision, Mission, and Purpose

This data governance initiative is an enterprise-wide initiative representing multiple opinions and perspectives integrated into an overall common vision. It strives to identify a desired state (vision), provide a logical value (mission), and describe how efforts will combine to result in an improved alignment of goals and strategies (purpose).

1.1 Vision

New River is dedicated to creating a data governance program to establish agreed upon standards and procedures for inputting, processing, verifying, retrieving, archiving, and restoring data with clearly defined and shared responsibilities among stakeholders.

1.2 Mission

This data governance program will help New River successfully manage and maintain data resources, ensuring the integrity, reliability, availability, and compliance of organizational data and information resources.

1.3 Purpose

The purpose of this plan is to provide clarity for data governance responsibilities by defining expectations, roles, responsibilities, and a framework for accountability related to data governance. Standards and procedures for data governance must be created to protect data assets. Data Owners and Data Stewards must be identified and charged with clear responsibilities to manage these assets. Data standards must be established with accompanying procedures for monitoring and managing them to ensure they are followed. Compliance requirements must be understood and satisfied. IT goals and strategies must be aligned with business goals and strategies to achieve this. This plan aligns business and IT goals, and strategies, as follows:

Business Goals	a. Standardize data entry procedures. b. Improve quality and validity of data.
Business Strategies	c. Establish procedures and guidelines to ensure integrity of data. d. Ensure compliance with federal, state, and local requirements.
IT Goals	e. Leverage technology to automate and streamline processes. f. Generate a high degree of user confidence in the organization's data.
IT Strategies	g. Use data to provide insight to business decision making. h. Ensure data is of high quality through consistent processes for data auditing, data escalation, and data monitoring.

2. Guiding Principles

We focused on the following guiding principles for this data governance plan: **ownership**, **integrity**, **quality**, **access**, **security**, **privacy**, and **literacy**.

2.1 Data Ownership

Data ***ownership*** refers to defining the various levels of responsibility relating to a particular data set. If ownership is not assigned or well-known to users, then it is less likely that data standards can be maintained (since no one is responsible for ensuring the quality of the data).

2.2 Data Integrity

Data ***integrity*** refers to the reliability of the information based on its accuracy, validity, and consistency across its lifecycle. Underlying issues related to data *integrity* include definitions, entry errors, terminology, formats, procedures, and timeliness.

2.3 Data Provenance and Quality

Data ***quality*** refers to the reliability of the information to serve its intended purpose of supporting the planning, decision making, and operations of the enterprise. An understanding of primary, secondary, and shadow data sets is necessary to discern the validity of information and the impact of data errors. An understanding of integrations of data sets is helpful too, since data is routinely fed from one system (primary data source) to another (secondary data source) and knowing the origin of the data (data ***provenance***) is critical to understanding and ensuring its quality.

2.4 Data Access

Data ***access*** refers to a user's ability to locate and retrieve data stored within a database or repository. Depending on the data, the source, and the user's level of access, the data may be protected behind a network firewall or freely available through the Internet. The principle of "least privilege" works by allowing only enough access to perform required job functions, so user roles and access privileges to data are matched with job functions.

2.5 Data Security

Data ***security*** refers to protective digital privacy measures that have been applied to the data to prevent unauthorized access. Data security also protects against corruption and examples of data security measures include requiring the use of authentication for access, the use of encryption for storage and transmission, and proven procedures for data backups and recovery.

2.6 Data Privacy

Data ***privacy*** refers to protecting the information of individuals (students and employees). Data privacy efforts should ensure compliance with privacy laws and regulations while managing the risks associated with personal data confidentiality to protect this data from unauthorized access.

2.7 Data Literacy

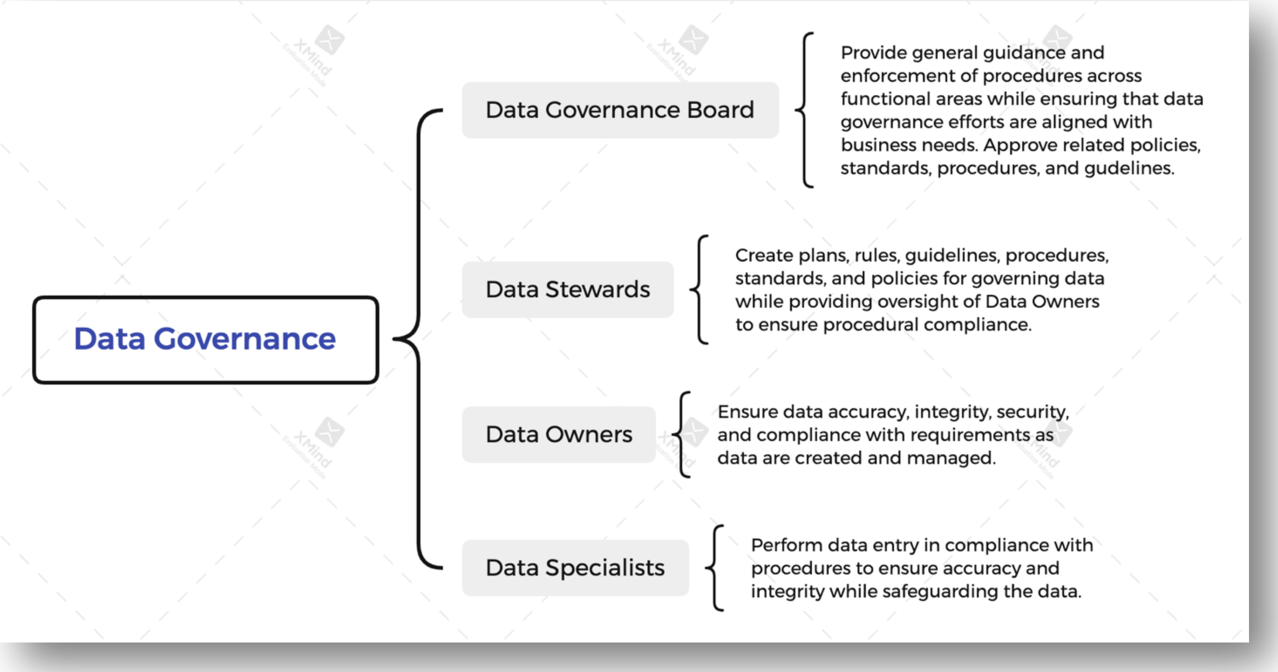
Data ***literacy*** is the ability to derive meaningful information from data. Complex data analysis requires some knowledge of math and statistics and often specialists are employed to perform this function for an organization. The Chief Data Officer fills this role and is responsible for the interpretation and meaning of data while Programmers and Database Administrators have responsibility for accessing data, compiling reports, and providing data to meet requested criteria. Some basic level of data literacy is expected of all employees (e.g., to identify malicious emails and take appropriate action), while a higher level of data literacy is expected of some key positions charged with making data-informed decisions.

3. Establishing Roles and Responsibilities

Data governance is a college-wide initiative with executive-level support and enforcement. Managing data well requires the effort of many individuals working collaboratively toward a clearly defined goal using agreed upon procedures with checks and balances for compliance.

In most small companies, individuals often serve in more than a single role. This plan exemplifies this since some Data **Owners** have no subordinate staff (and must also serve as Data **Specialists**) while some Data **Stewards** are also Data **Owners** with responsibilities of both roles. Additionally, four of the Data **Stewards** are also members of the Data **Governance Board** since they serve on the President's Cabinet. To be clear, the roles and responsibilities assigned through this plan are not new responsibilities. It is merely a reflection of existing responsibilities with data governance roles more clearly overlaid and defined.

The following diagram clearly defines the roles and responsibilities used at New River for governing data:


Data Governance
Data Governance Board
Provide general guidance and enforcement of procedures across functional areas while ensuring that data governance efforts are aligned with business needs. Approve related policies, standards, procedures, and gudelines.
Data Stewards
Create plans, rules, guidelines, procedures, standards, and policies for governing data while providing oversight of Data Owners to ensure procedural compliance.
Data Owners
Ensure data accuracy, integrity, security, and compliance with requirements as data are created and managed.
Data Specialists
Perform data entry in compliance with procedures to ensure accuracy and integrity while safeguarding the data.

3.1 Data Specialists and Data Owners

Ownership means being held accountable for such things as data integrity, security, and compliance requirements. **Data Owners** have this responsibility. They are accountable to an authoritative body (**Data Stewards**) who has an enterprise perspective. Most Data Owners supervise employees who are tasked with data entry **(Data Specialists**), so ownership includes oversight of these personnel to ensure that data integrity is maintained by all persons involved.

3.2 Data Stewards

Data Stewards have enterprise authority and are responsible for planning data governance efforts while creating the rules and processes for governing data. They establish standards, procedures, and develop policies to define how data governance should be managed. They ensure that Data Owners and Data Specialists follow these rules and processes. They operate under the guidance and approval of the President's Cabinet, which serves as the **Data Governance Board**.

Data Stewards are leaders in their respective areas, and they work collaboratively as a group to establish a coherent enterprise-wide solution for data governance.

To clarify these responsibilities for data governance, this plan identifies internal titles for each of the **Data Stewards** to better reflect their areas of responsibility. These areas of responsibility are not *new* assignments, but instead a recognition of *existing* responsibilities for aspects of data governance. This plan identifies the following internal titles for the **Data Stewards**:

1. Chief Data Officer (CDO)—Director, Institutional Effectiveness and Grants
2. Chief Privacy Officer (CPO)—Registrar and Director, Human Resources
3. Chief Information Security Officer (CISO)—Manager, Information Systems
4. Chief Information Officer (CIO)—Vice President, Information Technology Services
5. Chief Technology Officer (CTO)—Database Administrator Senior
6. Chief Technology Officer Assistant—Systems Programmer

A **Chief Data Officer** (CDO) must be able to understand both the technical points of data management, as well as the business drivers and needs regarding data. The CDO establishes data procedures and standards while working closely with IT to implement them. The CDO is the go-to person for data-related issues within the company and is essentially the overall manager of the data governance initiative – while working closely with others in functional areas and in IT.

This plan identifies the Director of Institutional Effectiveness and Grants as the **Chief Data Officer** (CDO).

In 2019, Dr. Copenhaver modified the reporting structure for the CDO, and this position now reports directly to the President. The **Chief Data Officer** role is an evolving one with some literature suggesting it should be a C-level executive position. At New River this means being a member of the President's Cabinet and Dr. Copenhaver has added this position to the Cabinet.

> *To truly appreciate the increasing need for the CDO's role, one must first understand that **90% of the world's data was created in the past two years alone** (Forbes, 2018).*

A **Chief Privacy Officer** (CPO is responsible for managing risks related to information privacy laws and regulations. For New River, both the Registrar and the Director of Human Resources serve as **Chief Privacy Officers**. The CPO develops and implements policies designed to protect employee and student data from unauthorized access.

While *privacy* is concerned with protecting the information of individuals (students and employees), *security* is concerned with protecting College-owned data. This plan designates the Manager of Information Systems as the **Chief Information Security Officer** (CISO). The CISO is responsible for ensuring the protection of proprietary data and intellectual property by managing overall security needs. Through collaboration with others, the CISO develops security policies and protection procedures. The CISO oversees the introduction of new technologies, manages cybersecurity and privacy awareness training and education programs, and provides leadership and guidance for other employees, students, and customers.

A **Chief Information Officer** (CIO) is the most senior executive in an organization who has responsibility for information technology and computer systems. The CIO analyzes how various technologies benefit the company or improve an existing business process and then integrates a system to realize that benefit or improvement. The CIO is responsible for strategy and implementation of technology to support enterprise goals and develops related plans, policies, and procedures. The Vice President of Information Technology Systems is identified as the **Chief Information Officer**.

A **Chief Technology Officer** (CTO) is responsible for overseeing the effectiveness of technology resources within an organization. Their duties include communicating across functional areas to assist with improving and automating procedures while ensuring that enterprise data assets are effectively managed. The CTO explores new technologies and works to align resources with agency needs. The Database Administrator Senior is designated as the **Chief Technology Officer**.

3.3 Data Governance Board (President's Cabinet)

This plan establishes the President's Cabinet as the **Data Governance Board,** and this group helps communicate the value of data governance throughout the College by supporting its enforcement. This group of cabinet-level personnel will ensure that the data governance program is aligned with business needs and that goals and policies are enforced.

While Data Stewards as a group work independently, they rely on the **Data Governance Board** for guidance, approval, and enforcement across functional areas.

Data Governance Board (President's Cabinet)	
Core Objectives:	Support enforcement of data governance efforts while ensuring these efforts are aligned with business needs.
Responsibilities:	Periodically review data governance issues and processes using reports and audits to ensure that institutional needs are addressed and that procedures are being enforced.
Frequency of Meetings:	Meets monthly, particularly during Fall and Spring terms. Data governance topics are reviewed as needed with periodic updates from Data Stewards.

3.4 Asset and Data Management

New River data assets are managed by personnel serving in the roles previously described. The following table details this assigned responsibility to show which data assets are managed by each Data Owner (in bold) with supporting **Data Specialists** for each data asset (using a snapshot of employee assignments from **July 2021**).

Organizational Area	Data Specialists and Data Owners (*in bold*)	Data Set
Academic Services – Student Records	**Registrar** and Records Officers	**Banner** (course definitions, term schedules, academic programs) and **DropGuard** (attendance)
Academic Services – Scheduling and Accounts	Vice President of Academic Affairs (tbd) **Dean** (Patriquin) Administrative Assistant (Rahal) Supervisor, Student Accounts (Borders) Student Services Specialist (Lewis) Administrative Assistant (Miller)	**Banner** (course schedules, instructor assignments) Student Accounts
Admissions	**Enrollment Services Director** (Evans) Student Program Advisor (Dalton)	**Banner** (admissions) and **Comevo** (online orientation)
Finance	**Vice President of Finance** (Shields) Accounting Manager (Roark) Accountant Senior (Kuhn) Director of Purchasing (Jackson) Director of Physical Plants (Runion) Senior Business Office Administrator (Matherly)	**Banner** (finance and budget) Payroll Inventory Purchasing Vehicle Logs, Maintenance Requests, Access Logs Clery Act Reporting Online Bookstore
Financial Aid	**Director of Financial Aid** (Harmon) Financial Aid Manager (Ritchie) Financial Aid Counselor (Fry and Feijo)	**Banner** (financial aid) Counseling
Institutional Advancement and Communications	**Executive Director of Institutional Advancement** (Green) Administrative Associate (Taber) Director of Communications (Canterbury) Recruitment Specialist (Honaker and Saunders)	**Blackbaud** (donor and alumni) and **Quicken** (foundation budget and scholarships) **Banner** (Prospective Students)
Human Resources	**Director of Human Resources** (Adkins) Temporary Staff (Parker) HR Assistant (Gill and Williams)	**Banner** and **NeoGov** (employee information)
Information Technology Services	**Manager of Information Systems** (tbd) **Librarian** (Coston) **Help Desk Manager** (Davis)	**Active Directory** (authentication source, account creation, email) **ILL Requests** **ID Cards and Trouble tickets**
Workforce	**Dean** (Sampson Program Specialist (Kincaid)	**Banner** (course schedules and instructor assignments)
Student Success	**Dean** (Hoeman) Instructional Specialist (Rhodes) Retention Specialist (Young)	TANF tracking; **DropGuard**; Student Success Center (usage and testing)

4. Training, Compliance, and Procedures for Data Governance

4.1 Training

Training is needed not just for the broad topic of data governance, but also for specific areas within data governance. For example, BRIM (the West Virginia Board of Risk and Insurance Management) requires us to document that we train employees on Privacy and

Security Awareness. These topics (and other requirements from BRIM) are components of our overall data governance plan, and we identify, provide, and manage training related to these requirements as part of this initiative. New River purchased a solution for cybersecurity and privacy awareness training named **KnowBe4** and it was implemented in Fall 2019 for all employees.

We created a playlist for Data Governance in **Linkedin Learning** and are using it to increase expertise for those involved in managing this responsibility (Board, Stewards, and Owners). To determine who has completed the training, we run a report named *Privacy Awareness* in the Reports section of Linkedin Learning.

The following information is from one of the training sessions in Linkedin Learning:

> *Managing data is concerned with the use of data to make good business decisions while data governance is the degree to which we use disciplined behavior across our entire organization in how we manage our data. At a high level, data governance is simply data that is managed well.*

The **Linkedin Learning** playlist we've created for Data Governance contains the following information:

1. Course: Learning Data Governance (41m 4s)
    a. Video: Data Governance Definition and Basics (2m 32s)
    b. Video: Data Governance Focus Areas (3m 37s)
    c. Video: Data Quality and Governance (4m 29s)

4.2 Compliance with Laws, Policies, Procedures, and Rules

Compulsory reporting to multiple external agencies requires New River to comply with established laws, rules, and policies that govern and guide our data management. This compliance is an ever-evolving requirement as cybersecurity, data privacy, and data governance are rapidly increasing in complexity with new compliance requirements being introduced frequently.

The compliance requirements and standards that currently apply to New River which are addressed by this plan are:

PCI DSS—**Payment Card Industry Data Security Standards** govern credit card transactions. Compliance with PCI DSS isn't required by federal law, but compliance shields New River from liability in the event of a data breach.

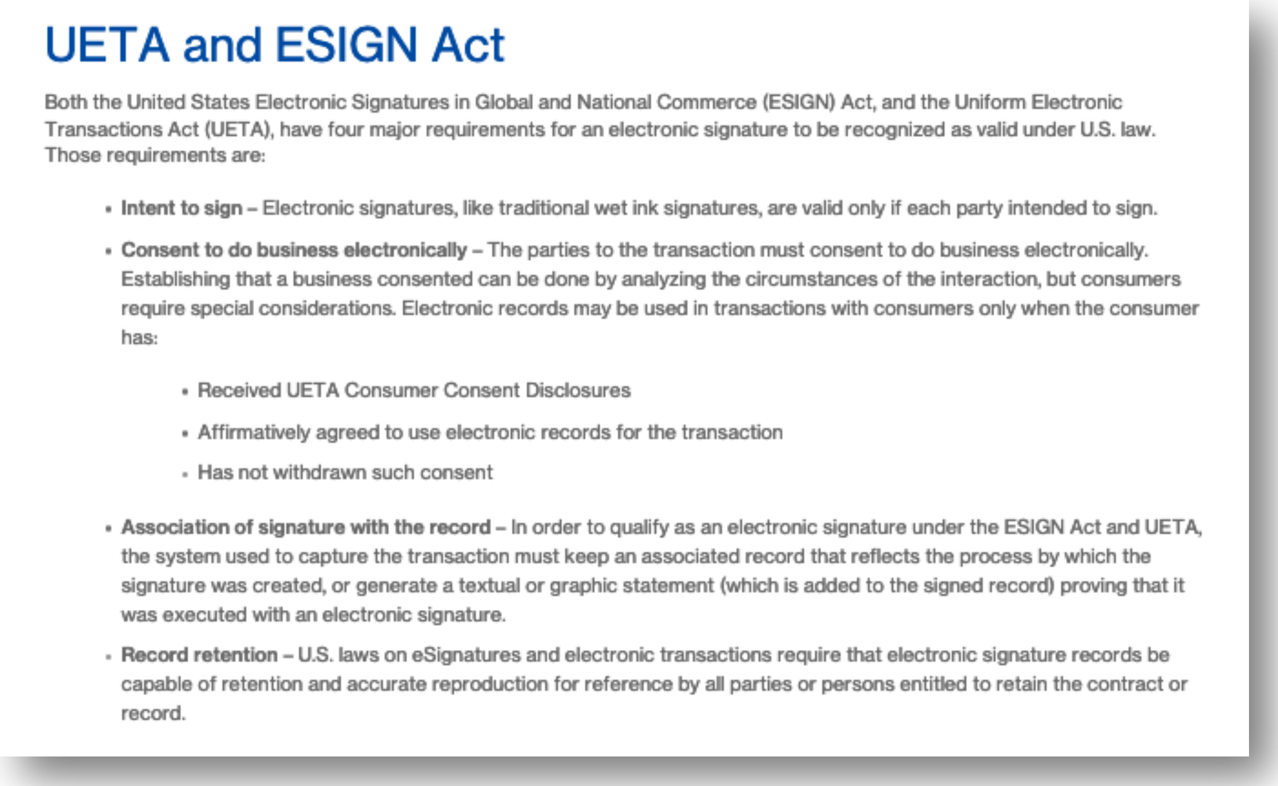
GLBA—The **Gramm-Leach Bliley Act** requires New River to explain information-sharing practices we use to inform customers (students) about how we safeguard their information.

GDPR—The **General Data Protection Regulation** is a legal framework that sets guidelines for the collection and processing of information on European Union (EU) subjects. This may apply to transactions with EU companies or individuals.

NACHA—The **National Automated Clearing House Association** manages the administration, development, and governance of the ACH framework, which is the electronic system used to facilitate financial transactions in the United States by credit and debit card.

FERPA—The **Family Educational Rights and Privacy Act** is a federal privacy law that gives parents certain protections regarding their children's educational records (such as grades, transcripts, disciplinary records, class schedules, and family information).

UETA—The **Uniform Electronic Transactions Act** and the **ESIGN Act** are two U.S. regulatory acts established to guide businesses regarding how to conduct business electronically. These two acts work together to ensure that eSignatures receive the same legal recognition as electronic signatures. However, there are differences between the two. The ESIGN Act is a federal law, which means that every state must comply. Whereas the UETA is adopted on a state-by-state basis. West Virginia is one of 47 states that have accepted the guidelines laid out in the UETA, so New River must comply with both. The West Virginia Secretary of State's Office passed on March 18, 2008, the Use of Digital Signatures, State Certificate Authority and State Repository bill (SB 349, Section 64-9-15).



UETA and ESIGN Act

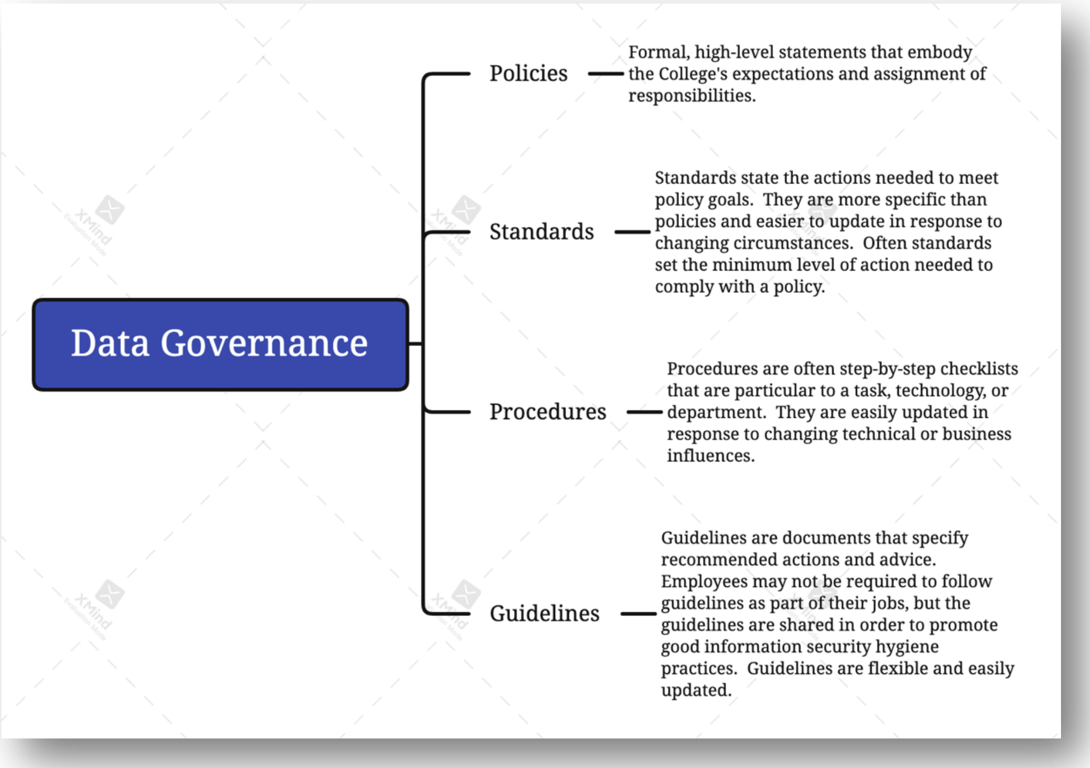
Both the United States Electronic Signatures in Global and National Commerce (ESIGN) Act, and the Uniform Electronic Transactions Act (UETA), have four major requirements for an electronic signature to be recognized as valid under U.S. law. Those requirements are:

- **Intent to sign** – Electronic signatures, like traditional wet ink signatures, are valid only if each party intended to sign.
- **Consent to do business electronically** – The parties to the transaction must consent to do business electronically. Establishing that a business consented can be done by analyzing the circumstances of the interaction, but consumers require special considerations. Electronic records may be used in transactions with consumers only when the consumer has:
  - Received UETA Consumer Consent Disclosures
  - Affirmatively agreed to use electronic records for the transaction
  - Has not withdrawn such consent
- **Association of signature with the record** – In order to qualify as an electronic signature under the ESIGN Act and UETA, the system used to capture the transaction must keep an associated record that reflects the process by which the signature was created, or generate a textual or graphic statement (which is added to the signed record) proving that it was executed with an electronic signature.
- **Record retention** – U.S. laws on eSignatures and electronic transactions require that electronic signature records be capable of retention and accurate reproduction for reference by all parties or persons entitled to retain the contract or record.

4.3 Policies and Procedures for Data Governance

Laws and compliance requirements often drive policy, standards, procedures, and guidelines, which provide the framework for managing data governance.

1. A **policy** clearly states *what* the high-level management of your organization expects from its employees (it may also address *who* is responsible and *why* the policy is required).
2. **Standards** establish quality control and effectiveness measures.
3. A **procedure** is a detailed description of *how* the instructions in the policy are to be carried out.
4. A **guideline** is a statement about what to do, or not to do, in a specific situation.



Formal, high-level statements that embody the College's expectations and assignment of responsibilities.

Standards state the actions needed to meet policy goals. They are more specific than policies and easier to update in response to changing circumstances. Often standards set the minimum level of action needed to comply with a policy.

Procedures are often step-by-step checklists that are particular to a task, technology, or department. They are easily updated in response to changing technical or business influences.

Guidelines are documents that specify recommended actions and advice. Employees may not be required to follow guidelines as part of their jobs, but the guidelines are shared in order to promote good information security hygiene practices. Guidelines are flexible and easily updated.

Policies state the high-level institutional goals around expected information security behaviors and outcomes, and other documents are used to state thresholds of acceptable behavior, step-by-step processes to follow, or recommended (but not required) actions to take. The hierarchy for institutional governance documents is typically:

- **Policies**: The highest level of a governance document. Policies typically have general applicability, and they rarely change (or are hard to change). They are leadership's high-level statement of information security goals and expectations.
- **Standards**: Standards state the actions needed to meet policy goals. They are more specific than policies and easier to update in response to changing circumstances. Often standards set the minimum level of action needed to comply with a policy.

- **Procedures**: Procedures are often step-by-step checklists that are particular to a task, technology, or department. They are easily updated in response to changing technical or business influences.
- **Guidelines**: Guidelines are documents that specify recommended actions and advice. Institutional employees may not be required to follow guidelines as part of their jobs, but the guidelines are shared in order to promote good information security hygiene practices. Guidelines are flexible and easily updated.

Prior to creating this data governance plan, New River developed several internal policies and procedures related to data governance that are still in use (see below).

Procedure	Topic and Objective (with Links)	Owner
Computer Use Policy	Provides acceptable use information for college-owned computer and network resources (***February 24, 2020***). https://web.newriver.edu/procedures/computer-use-policy.pdf	*CIO*
Operating Rule #16:	Serves to ensure proper and ethical expectations for computer use expectations (***February 2, 2012***). https://www.newriver.edu/wp-content/uploads/2018/04/or_16_computer_use.pdf	*CIO*
Confidentiality Agreement	Enables employees to accept responsibility for managing and protecting confidential information (***December 2018***). https://www.newriver.edu/wp-content/uploads/2018/12/Confidentiality-agreement-12-2018.docx	*CPO HR*
Email Retention Procedure	Describes procedures for retaining and accessing emails (***June 21, 2011***). https://web.newriver.edu/procedures/email-archive-procedure.pdf	*CISO and CIO*
Procedure #42: Records Retention	Explains requirements and procedures for retaining records (***July 1, 2016***). http://intranet.newriver.edu/images/publicdocs/HR/procedures/Procedure_42-Records_Retention.pdf	*CDO*
Procedure #22: Social Media	Provides guidelines and information specifically for social media as it pertains to employees and student groups acting on behalf of the college (***March 18, 2014***). https://www.newriver.edu/wp-content/uploads/2018/04/Procedure_22_Social_Media_Procedure_Revised_3-18-2014.pdf	*Director, Communications*
Procedure #24: Email	Establishes New River email as the official method of communication (***November 8, 2013***). https://www.newriver.edu/wp-content/uploads/2018/04/procedure_24_email_communication_8_2014.pdf	*Director, Communications*

Procedure #17: Website Maintenance	Establishes expectations for web content managers to maintain the accuracy of their online information that represents New River (***March 1, 2011***).	Director, Communications

The following policies and procedures were developed in conjunction with or as a result of creating this data governance plan:

Policy or Procedure	Topic and Objective (with Links)	Owner
Data Standards and Procedures Manual	Establishes origin of data, identifies data entry personnel, provides procedural steps for cleaning data, and decreases the amount of duplicate and incomplete data within enterprise systems. (***July 22, 2021***). **TBD**	CTO and CIO
Standard Terms and Conditions for Information Privacy and Security with Vendors	Establishes compliance requirements for information privacy with vendors (***October 19, 2020***). https://web.newriver.edu/procedures/Standard-Terms-and-Conditions.pdf	CIO
Business Data Glossary	Establishes guidelines for classifying institutional data. **TBD**	CIO and CTO
ID Card Procedures	Assigns responsibilities and provides procedural information related to the New River ID Card system (***July 25, 2021***). https://web.newriver.edu/procedures/ID-Card-Procedures.pdf	CIO
Information Security Procedures	Includes procedures for responding to cybersecurity incidents, evidence of confidentiality agreements, completion of privacy and security awareness training, and privacy policy information. Need to include laptop encryption efforts and email encryption details (VPN, Barracuda, Microsoft Security Essentials, etc.). **Draft**: (coming soon)	CIO and CISO
Telework Procedure	Addresses employee expectations regarding a modern workforce capable of securely applying technology to enable work from alternate locations. Awaiting approval of the President's Cabinet. **Draft** (https://web.newriver.edu/procedures/Telework-Procedure.pdf)	CIO and CHRO
Consent to Do Business Electronically	Allows students to grant consent to do business electronically (***July 16, 2021***). https://web.newriver.edu/procedures/Consent-To-Do-Business.pdf	CPO and CIO
BOG 6.1: Information Security Policy	Establishes responsibilities and authority for data governance (***October 01, 2020***). https://www.newriver.edu/wp-content/uploads/2021/01/BOG_6.1_Information_Security_signed.pdf	CIO

5. Projects and Services

5.1 Project Standards and Guidelines

Resource limitations are obstacles to overcome before engaging in new data projects and initiatives. The following criteria should serve as **standards** to guide and prioritize new data project or initiative decisions:

1. ***New projects must fit the current data architecture.***

A **data architecture** is composed of models, policies, rules, and standards that govern which **data** is collected, how it is stored, arranged, integrated, and put to use in **data** systems and in organizations. Starting a new data project without leveraging this architecture requires extensively more resources and may not be readily possible. Operating outside the existing data architecture also tends to create shadow systems that may become security vulnerabilities if not effectively managed.

2. ***New projects should increase revenue or decrease costs.***

Identifying new data project or initiative requests that serve to increase revenue or decrease costs will ensure the long-term viability of sustaining the project and may justify the initial investment of resources.

3. ***New projects or services should fit into the current organizational structure.***

If a new data project or service request requires additional personnel, then project outcomes must warrant the increased ongoing institutional costs. If existing personnel will not be charged with security and management of the data, then these vulnerabilities must be justified in the bigger perspective of managing institutional risks.

5.2 Data Value

It is difficult to establish the value of data simply because so many business processes routinely can't be done without it. Data has become essential. Imagine the value of the college as a whole and then imagine that value if the college were to lose all of its data assets. What would it cost to "start over" or recover from this loss and how long would it take? How tragic would the loss of this data turn out to be? Without question, data assets are of great value to the College. Understanding the value of these data assets and taking steps to protect them is a core purpose of this plan.

Data assets are used to support universal executive drivers such as:

- **Increase revenue—**With a focus on performance improvements and continued innovation, data assets are used to inform decision making so processes can be improved. Some examples include (a) improved business cycle times through automation and efficiencies for data access, and (b) simplifying user access to data and using it to personalize services to increase student engagement and improve student retention.
- **Manage costs—**Costs can be decreased or even avoided. Some examples include improved resource and process efficiencies, digital instead of manual processes,

automation, simplification, and enhanced analytics capabilities. Telework can be leveraged to create flexible work environments that remove location-specific limitations for students and employees.

- **Manage risk—**Identify the risks New River faces by NOT doing data governance. Some examples include regulatory and data privacy fines, risk of bad decisions, loss of competitive position, loss of students, loss of eligibility for financial aid distributions, or loss of accreditation to offer degrees and programs. Effectively managing these risks will ensure operational continuity.

6. INTERNAL MANAGEMENT AND CONTROL ACTIVITIES

6.1 Oversight and Supervision

Metrics and reports have been established by **Data Stewards** to serve as checks and balances regarding data integrity. These metrics measure the performance of a specific process or data asset to illuminate data integrity issues and to provide a greater degree of data ownership for **Data Owners**. These metrics identify integrity issues that might require additional training or closer supervision of **Data Specialists** who may unknowingly be compromising data integrity.

Data Stewards coordinate with others (Board Members, Owners, and Specialists) to ensure that accountabilities are defined in a manner that introduces checks and balances between business and technology teams as well as between those who create and collect information, those who manage it, those who use it, and those who introduce standards and compliance requirements.

These reports assist Data Owners and Data Specialists with identifying data integrity issues. These reports are automated so that Data Owners and other key individuals receive the information in a predictable and timely fashion. Data Stewards provide oversight to ensure that integrity issues are being resolved. The Data Governance Board serves to settle any disputes or to address any issues not being resolved.

Reports to Data Owners are weekly or some other periodic schedule for routine data decisions. Reports to the Data Governance Board are annual or ad hoc for issue resolution.

Metrics and Frequency	Objective	Metrics Owner
Banner Security Review *(30 days)*	• Ensure users with access are current with appropriate privileges.	• CTO
Current Employee List *(30 days)*	• Identify current employees and revoke access for non-employees.	• CPO - HR
Duplicate PIDM Report *(Weekly)*	• Identifies duplicate PIDM's assigned in Banner.	• CTO
Enrollment Reports *(Weekly)*	• Provides snapshot of enrollment information.	• CDO
Name Changes *(Weekly)*	• Audit report of any name changes.	• CTO
Automated Data Integrity Report *(Weekly)*	• Reveals missing or erroneous data in student admissions records.	• CTO

6.2 Issue Resolution

Each level of data governance authority has responsibility for identifying and resolving any issues that arise which might compromise or devalue New River data assets (as shown below):

Strategic Level (Board)	• Data investments, access, literacy, and security
Tactical Level (Stewards)	• Data definitions, usage concerns, and security
Operational Level (Owners and Specialists)	• Data quality, accuracy, and integrity

7. External Agency Reports and Monitoring

7.1 Audits for Data Integrity and Compliance

Audits serve to revise and fine-tune ongoing practices, processes, and procedures for the management and handling of data within the organization. These audits should review the organization's security controls, compliance requirements, and internal processes.

New River conducts an annual internal audit with Suttle and Stalnaker. This audit addresses (1) General Controls, (2) Banner Application Review, and (3) agreements and contracts for IT services.

Auditor Name:	**Suttle and Stalnaker** (internal auditors)
Email:	epopp@suttlecpas.com
Phone:	304-343-4126
Frequency of Data Audits:	Annual in July.
Scope of Data Audit:	Organizational structure, policies, procedures, and standards. Physical and environmental conditions and procedures. IT contracts and agreements. Banner application review. GLBA compliance.
Goals and Objectives:	Identify issues to New River and BOG that need addressed for compliance.

New River has cybersecurity insurance through BRIM. Annual audits are conducted to ensure compliance. For network security, New River conducts an annual network penetration audit to identify security vulnerabilities so that corrective actions may be taken.

Auditor Name	**BRIM Insurance with Cybersecurity Incident Coverage**
New River Contact:	Robert A. Runion
Email	rrunion@newriver.edu
Phone	304-929-5026
Frequency of Data Audits	Annual in July.

Scope of Data Audit	Cybersecurity and Privacy Awareness Training
Goals and Objectives	Validate policies, procedures, security, training, and vulnerability testing.

7.2 Data Monitoring and Reporting

Continuous monitoring of our data assets helps to ensure the highest levels of data integrity within our enterprise systems. One value of reporting is that it requires interaction with the data, which provides opportunities for validating the data as the report is created and reviewed. Every interaction with data is an opportunity to verify its accuracy, consistency, and other attributes which help to continually improve its overall *integrity* and *quality*. The following table depicts routine reporting information for New River:

Data Set	Data Importance	Data Change Frequency	Report Recipient	Report Frequency	Reporter
Daily Dozen	Moderate	High	Cabinet + Financial Aid and Enrollment Directors	Daily	CDO
IPEDS Fall Collection	High	Moderate	US Department of Education	Annually	CDO
• Institutional Characteristics					
• Completions					
• 12-month Enrollment					
IPEDS Winter Collection	High	Moderate	US Department of Education	Annually	CDO
• Student Financial Aid					
• Graduation Rates					
• 200% Graduation Rates					
• Outcome Measures					
IPEDS Spring Collection	High	Moderate	US Department of Education	Annually	CDO
• Fall Enrollment					
• Finance					Chief Financial Officer
• Human Resources					Director of HR
• Academic Libraries					Library Services
HEPC August 1 File Submission	High	Moderate	WVHEPC	Annually	CDO
HEPC September 1 File Submission					
HEPC September 15 File Submission					
HEPC October 1 File Submission					
HEPC October 15 File Submission					
HEPC Fall Final					
Higher Education Reauthorization Filing					
Update Students with Disabilities information					
HEPC January File Submission					
HEPC June File Submission					
HEPC July File Submission					
Financial Aid Audit	High	Moderate	Suttle & Stalnaker	Annually	Director of Financial Aid
• Banner Applications Review					CIO
• General Controls					CIO
• Network Overview					CISO
• Cybersecurity and Privacy Awareness Training	High	Low	BRIM	Annually	CIO and CISO
NCSR	High	High	DHS	Annual	CIO
HLC Institutional Update	High	Moderate	Higher Learning Commission	Annually	CDO
Academic Program Reviews	High	Moderate	Board of Governors, WVCTCS	Various	Academic Affairs
Student Data Integrity	Moderate	High	Admissions and Registrar's Office	Weekly	IT
Applicant Data Integrity	Moderate	High	Admissions	Various	IT
Charges and Fee Summary	Moderate	High	Finance + CDO	Daily	IT
Paid/Unpaid/CHold List	Moderate	High	Finance	Daily	IT
New and Cancelled Courses	Low	High	Various	Daily	IT
Cleary Act Reporting	High	Moderate	Department of Education	Annually	Director of Facilities and Campus Safety

8. Communication Planning to Maintain Initiative

All those involved in data governance (Specialists, Owners, Stewards, and Board members) have a responsibility for continuously promoting the value of data to the organization by advocating for ways to educate the organization and its data stakeholders on the benefit of data management.

The following table depicts the type of change to data governance plans, policies, and procedures and how these changes are expected to be communicated:

Type of change	**Method of communication**	**Responsibility**
Process Change	College-wide or targeted email to those impacted and newsletter updates as appropriate.	Data Stewards and Board
New Data Policy	College-wide email and posting on web site.	Data Stewards and Board
Plan updates, reports, audit findings, and training updates.	Informational announcements in cabinet meetings	Data Stewards

It is important to realize, that despite years of effort to create this Data Governance Plan with accompanying policies, procedures, and related information, it will need to continuously evolve to maintain relevance with rapidly changing technologies and other dynamic environmental conditions as well as everchanging compliance requirements.

To address this, we plan annual reviews of this information by **Data Stewards** with approval from the **Data Governance Board** each **July**. These reviews should update key aspects of the plan to address:

1. any changes in last approved dates for policies and procedures,
2. an updated schedule of reporting (if changes are needed),
3. any changes to roles or responsibilities for data governance, and
4. progress updates on training completion.

REFERENCES, NOTES, AND SUPPORTING INFORMATION

We located, learned from, and relied upon many resources to create this plan. We've listed the most helpful.

Data Governance Framework
http://www.datagovernance.com/the-dgi-framework/

Data Governance Institute
http://www.datagovernance.com

Educause—Data Governance
https://library.educause.edu/topics/information-systems-and-services/data-governance

Educause—The Safeguards Rule Audit Objective is Here!
https://er.educause.edu/blogs/2019/7/the-safeguards-rule-audit-objective-is-here

Educause: Asset and Data Management
https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/asset-and-data-management

Educause: Information Security Guide: Effective Practices and Solutions for Higher Education
https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide

Hechinger Report
https://tuitiontracker.org/fitness/school.html?unitid=447582

How to Use the DGI Data Governance Framework to Configure Your Program
http://www.datagovernance.com/wp-content/uploads/2014/11/wp_how_to_use_the_dgi_data_governance_framework.pdf

Information Security Guide: Effective Practices and Solutions for Higher Education
https://spaces.internet2.edu/display/2014infosecurityguide/Home

Infogix Data Governance Resource Center
https://datagov.infogix.com

Malicious Domain Blocking and Reporting (MDBR)
https://mdbr.cisecurity.org

National Center for Education Statistics (NCES) and Integrated Postsecondary Education Data System (IPEDS)
https://nces.ed.gov/collegenavigator/

https://nces.ed.gov/collegenavigator/?q=new+river+community&s=WV&zc=25813&zd=0&of=3&id=447582

NIST 800-171
Federal Guideline for Controlled Unclassified Information

NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

Records Retention Procedure for New River CTC (July 1, 2016)
http://intranet.newriver.edu/images/publicdocs/HR/procedures/Procedure_42-Records_Retention.pdf

Security Policy Templates
https://www.sans.org/information-security-policy/

Standards, Guidelines, and Procedures (Security Policies article from EDUCAUSE)
https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies

The NCSR Team
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
NCSR@cisecurity.org
518-516-6154 or 518-516-6116

West Virginia Legislature, House Bill 4261 (Establishes state-level data governance manager)

West Virginia Legislature, Code 46A-2A-102 (Notice of breach of security of computerized personal information)
http://www.wvlegislature.gov/WVCODE/Code.cfm?chap=46a&art=2A

Why Companies are Turning to Chief Data Officers to Generate More Value Out of Data
https://www.forbes.com/sites/kimberlywhitler/2018/07/28/why-companies-are-turning-to-chief-data-officers-to-generate-more-value-out-of-data/#6ab7a69a4b6a

http://www.legis.state.wv.us/Bill_Status/bills_text.cfm?billdoc=hb4261%20intr.htm&yr=2016&sesstype=RS&i=4261