PIERPONT COMMUNITY & TECHNICAL COLLEGE
BOARD OF GOVERNORS

IT and Data Reporting Committee Meeting

Wednesday, April 23, 2025
11:00 AM

Pierpont's Advanced Technology Center (ATC)
500 Galliher Drive
Fairmont, WV 26554
Room 201A

AGENDA

I. Call to Order

II. *Approval of Minutes – March 25, 2025 ***Tab 1***

III. IT Updates

A. Caperton Center
   i. Library Computer Lab Refreshed
   ii. Room 307 Media Refreshed

B. VM Server

C. VR Room

D. Windows 11

IV. Institutional Effectiveness Plan ***Tab 2***

V. Data Management Plan ***Tab 3***

VI. Data Policies

A. Data Access Policy ***Tab 4***

B. Data Integrity ***Tab 5***

C. Data Governance Policy ***Tab 6***

D. External Data Reporting and Approval Policy ***Tab 7***

**Denotes possible action item*

VII. HLC Updates

A. Criteria 5

VIII. Adjournment

Tab

1

PIERPONT COMMUNITY & TECHNICAL COLLEGE
BOARD OF GOVERNORS

IT and Data Reporting Committee Meeting

Tuesday, March 25, 2025
1:00 PM

Pierpont's Advanced Technology Center (ATC)
500 Galliher Drive
Fairmont, WV 26554
Room 216A

MINUTES

Notice of Meeting

A meeting of the Pierpont Community & Technical College (Pierpont) Board of Governors IT and Data Reporting Committee was held on March 25, 2025, beginning at 1:00 PM. The meeting was conducted in person at the Advanced Technology Center in Fairmont, WV. Advanced announcement of this meeting was posted on the WV Secretary of State's Meeting Notices Webpage.

Committee Members Present: Vickie Findley, Anthony Hinton, and Nathan Weese

Committee Members Absent: Jessica Killon and Jeffrey Powell

Other Board Members Present: Thomas Cole, Christine Miller, Juanita Nickerson, and Joanne Seasholtz

Others Present: Members of the President's Cabinet, faculty, staff, and others

I. Call to Order

Nathan Weese called the meeting to order at 1:00 PM.

II. Approval of Minutes – February 18, 2025

Anthony Hinton moved to approve the February 18 meeting minutes. Vickie Findley seconded the motion. All agreed. Motion carried.

III. IT Updates

A. Aviation Wireless Expansion/Upgrade

JT Bowers reported that improving wireless internet access at the Aviation Center has become a priority, as both students and staff have experienced ongoing connectivity issues. It was noted that approximately $20,000 could be redirected from the already approved IT budget to help address the issue. The proposed plan would involve the installation of five or six additional access points in key areas.

B. Information Technology Budget Deficit Review

JT Bowers provided an update on the ongoing review of the Information Technology budget, which is currently facing a deficit of approximately a quarter million dollars, as previously discussed during the last meeting and at President's Council. He is performing a thorough, line-by-line analysis of the budget to identify areas where savings can be made. As part of this review, all contracts are being evaluated prior to renewal to determine if better pricing or alternative products are available. One cost-saving measure already implemented was the transition from SCCM to ME, resulting in a savings of $10,000. Additionally, Microsoft licenses were reduced during last year's renewal cycle.

JT is also reviewing the college's current phone system and exploring a U.S.-based alternative that could offer comparable service at one-third to one-half of the current cost, potentially saving $10,000 to $15,000 annually. He anticipates completing the full budget review within the next month or two

IV. HLC Updates

Olivia Boltz reviewed the HLC Status Update Report (**Attachment A**) and provided an overview of ongoing efforts in preparation for the upcoming accreditation review. She noted the development of an institutional effectiveness and data management plan to support Criteria 3 and 4, along with a continued review and development of college policies. The committee will meet next month to review these plans. Additionally, an institutional reporting calendar is being created, and the HLC working group has recommended the development of a communication plan to effectively share HLC-related information with students and employees and across all campuses.

It was noted the potential need for support from the Marketing Department, particularly to help enhance the language of the HLC report—adding polish and assisting with storytelling, as has been done at other institutions. Finally, training and development opportunities are being planned for students and employees in preparation for the upcoming HLC visit.

V. Adjournment

There being no further business, Anthony Hinton moved to adjourn the meeting. Vickie Findley seconded the motion. All agreed. Motion carried.

Respectfully submitted by Amanda N. Hawkinberry

Attachment A

Office of Institutional Effectiveness and Research
Pierpont Community & Technical College
North Central WV Advanced Technology Center
500 Galliher Drive, Fairmont, WV 26554

HLC Status Update

As we continue preparations for our HLC Assurance Visit in September 2026, we pleased to report steady progress in addressing the areas of concern outlined in our most recent review. Below is a summary of recent activity across several key components:

- Criterion 2.C (Board Governance) and 3.C (Sufficiency of Faculty and Staff) are in the final stages of drafting and internal review. These drafts reflect changes made since our last assurance visit, including information and timelines regarding our strategic planning process, information regarding Board member training, and the ongoing progress in staffing and resource alignment.

- Criterion 4.B (now 3.E. Assessment of Student Learning) is currently under development. A dedicated committee has been formed, led by Olivia Boltz and AVP Nancy Parks, with participation from leadership across student services and academic affairs. The committee's work focuses on:
  - Clarifying the distinction between co-curricular and extra-curricular activities,
  - Documenting co-curricular components across all academic degree programs and institutional initiatives,
  - Establishing assessment processes to track impact and engagement.
  - Meeting with program coordinators to collect co-curricular planning and reporting templates.

In addition to these efforts, I have been developing both an Institutional Effectiveness Plan and a Data Management Plan to support our argument regarding institutional effectiveness—particularly as it relates to Criterion 3 (Teaching and Learning for Student Success) and 4 (Sustainability: Institutional Effectiveness, Resources and Planning). This includes reviewing and developing institutional policies that strengthen our approach to data integrity, data governance, and evidence-based decision-making.

To promote transparency and consistency across all departments and campuses, we are also developing an Institutional Reporting Calendar. This calendar will serve as a centralized timeline for major reporting requirements—internal, external, and accreditation-related—to ensure alignment, reduce redundancy, and promote data-informed planning at all levels of the institution.

Finally, as recommended by our HLC Working Group, we are also working on a communications plan to raise awareness about HLC and our ongoing accreditation work across all campuses and among our student body. Ensuring that our entire college community understands the purpose and process of accreditation is a critical part of institutional readiness and engagement.

We remain on track with our internal timeline and will continue to update the Board as we reach key milestones in this process.

Tab

2

Institutional Effectiveness Plan

Improving Institutional Effectiveness

Pierpont Community and Technical College

TABLE OF CONTENTS

INTRODUCTION

Institutional effectiveness is the foundation of continuous improvement at Pierpont Community & Technical College (Pierpont). It ensures that the college's programs, services, and operations are systematically assessed to support student success and institutional growth. Through data-driven evaluation and strategic planning, institutional effectiveness fosters a culture of accountability, innovation, and informed decision-making.

The Institutional Effectiveness Plan provides a structured approach to assessing how well Pierpont meets its mission, vision, and strategic goals. It outlines the processes by which the college measures performance, evaluates outcomes, and implements improvements across all areas of the institution. This ongoing cycle of planning, implementation, evaluation, and enhancement is designed to align with the 2024-2026 Strategic Alignment Plan, ensuring that institutional priorities remain responsive to student needs and community expectations.

By integrating institutional effectiveness into all aspects of academic programming, student services, and operational management, Pierpont strengthens its commitment to continuous improvement, accreditation compliance, and student achievement. This plan serves as a guide for faculty, staff, and leadership in making evidence-based decisions that drive meaningful progress and long-term success.

1. INSTITUTIONAL EFFECTIVENESS OVERVIEW

Pierpont Community & Technical College (Pierpont) is committed to advancing student learning, enhancing institutional quality, and continually improving programs and services. The establishment of an institutional effectiveness plan provides a structured framework to help the college achieve its mission, vision, and strategic goals.

At Pierpont, the Office of Institutional Effectiveness is responsible for assessing programmatic, unit, and operational goals comprehensively, systematically, and reliably. This structured assessment process objectively demonstrates how Pierpont fulfills its mission. Overseen by key institutional leaders—including the President, academic and administrative leadership, and the Director of Institutional Effectiveness—this process ensures that all assessment activities are intentionally designed, implemented, and monitored to foster continuous improvement. The primary goal of this plan is to cultivate a campus-wide culture of assessment that drives meaningful enhancements across all areas of the institution.

This document serves as a guide for implementing the cyclical institutional effectiveness assessment process at Pierpont. The college is committed to collecting and analyzing evidence that demonstrates goal attainment and informs decision-making. Assessment outcomes play a crucial role in shaping institutional planning, resource allocation, and strategic initiatives. Guided by the 2024-2026 Strategic Alignment Plan, Pierpont is strengthening institutional assessment processes with a strong emphasis on student success, academic innovation, and community engagement.

Pierpont's strategic plan is built on four key pillars:

1. People – Increase enrollment, retention, and graduation rates while fostering an inclusive, supportive environment.
2. Programs – Strengthen academic and career pathways, integrate innovative technologies (VR/AI), and enhance experiential learning.

3. Partners – Expand employer advisory committees, collaborate with educational and community-based organizations, and develop a Community Ambassador Program.
4. Performance – Monitor key performance indicators related to enrollment, financial health, accreditation, and institutional growth.

In alignment with this strategic framework, this plan underscores the importance of institutional effectiveness in supporting student achievement and continuous improvement. The college has developed an institutional effectiveness cycle to enhance student success and promote a shared, data-informed understanding of progress toward strategic goals.

Institutional Effectiveness Cycle:

1. Planning – Aligning goals and objectives with institutional priorities.
2. Implementation – Executing initiatives and strategic actions.
3. Evaluation – Collecting and analyzing data to assess outcomes.
4. Improvement – Using findings to drive enhancements and ensure continuous growth.

Ongoing Assessment & Accreditation:

The Office of Institutional Effectiveness plays a critical role in ensuring compliance with accreditation standards set by the Higher Learning Commission (HLC) and aligning institutional priorities with the West Virginia Community and Technical College System (WVCTCS) Master Plan. This plan remains a dynamic document, updated regularly to reflect strategic goals, accreditation requirements, and institutional performance metrics.

By implementing a data-informed culture of continuous improvement, Pierpont reinforces its commitment to "Education That Works", ensuring that all students, faculty, and stakeholders benefit from a high-quality, responsive, and impactful educational experience.

2. PURPOSE AND PRINCIPLES

Purpose

The Institutional Effectiveness Plan at Pierpont Community & Technical College (Pierpont) provides a structured framework to assess and enhance student learning, institutional quality, and operational effectiveness. This plan ensures that Pierpont systematically evaluates its programs, services, and performance metrics to align with its mission, vision, and 2024-2026 Strategic Alignment Plan.

Institutional effectiveness at Pierpont is a continuous cycle of planning, implementation, evaluation, and improvement, fostering a data-informed culture of assessment and accountability that drives meaningful enhancements across all areas of the institution.

Mission Statement

Pierpont Community & Technical College's mission is "to provide accessible, responsive, and comprehensive education" that empowers individuals and strengthens communities. Through high-quality instruction, workforce development, and strategic partnerships, Pierpont prepares students for success in an evolving economy.

Vision Statement

Pierpont aims to "empower individuals and strengthen communities through exceptional training and educational pathways" and create a dynamic and innovative learning environment that fosters academic excellence, career readiness, and community impact. The college is committed to being a leader in education and workforce training, ensuring that students and stakeholders have access to education that works.

Principles of Institutional Effectiveness

Pierpont's approach to institutional effectiveness is grounded in the following principles:

1. Mission-Driven Assessment – Institutional effectiveness efforts are directly aligned with Pierpont's mission, vision, and strategic goals, ensuring that all evaluation processes contribute to student success and institutional growth.

2. Data-Informed Decision Making – The college is committed to collecting, analyzing, and utilizing data to guide institutional planning, resource allocation, and program improvements.
3. Continuous Improvement – Pierpont follows a cyclical assessment process that ensures ongoing enhancements through systematic review and adaptation.
4. Transparency and Accountability – Institutional effectiveness efforts involve stakeholder engagement, including faculty, staff, students, and external partners, to ensure shared understanding and commitment to improvement.
5. Accreditation and Compliance – The plan supports Pierpont’s commitment to meeting and exceeding accreditation standards set by the Higher Learning Commission (HLC) and aligning with the West Virginia Community and Technical College System (WVCTCS).
6. Integration with Strategic Planning – Institutional effectiveness is not a standalone process but an integral component of the 2024-2026 Strategic Alignment Plan, ensuring alignment with the college’s long-term vision.

Institutional Effectiveness Mission Statement:

The mission of the Office of Institutional Effectiveness and Research is to provide accurate and timely information and expertise to support research, assessment, accreditation, strategic planning and the decision-making processes of Pierpont Community and Technical College. The office collects, coordinates, and analyzes data about and for the college and disseminates information to the administrators, faculty, staff, students, and external constituents

3. INSTITUTIONAL ASSESSMENT FRAMEWORK

Purpose of Assessment at Pierpont

The Institutional Effectiveness Plan at Pierpont Community & Technical College (Pierpont) serves as a guide for documenting and evaluating assessment efforts across the institution. It ensures that assessment processes are systematic, outcome-driven, and deeply integrated into all aspects of college operations. The goal of this plan is to enhance student learning, institutional performance, and strategic decision-making, supporting Pierpont's mission of providing accessible, responsive, and comprehensive education that empowers individuals and strengthens communities.

While Pierpont has historically conducted assessment across academic and student services areas, this plan consolidates these efforts into a comprehensive institutional effectiveness model, ensuring that all units participate in structured, cyclical assessment processes. This integration aligns with the 2024-2026 Strategic Alignment Plan, reinforcing Pierpont's commitment to continuous improvement, accountability, and data-informed decision-making.

Assessment Practices and Implementation

The primary goal of institutional assessment at Pierpont is to evaluate student learning, institutional operations, and strategic outcomes to improve educational quality and institutional performance. This process ensures that assessment outcomes actively inform resource allocation, budgeting decisions, and strategic planning.

While Pierpont has existing structures for assessment, this plan strengthens efforts to:

- Ensure systematic and consistent documentation of assessment across all instructional and non-instructional units.
- Standardize assessment processes to align with institutional priorities and accreditation expectations.
- Utilize assessment data to drive improvements in student learning, faculty development, operational efficiency, and community engagement.

- Strengthen connections between assessment results and institutional planning, ensuring that findings directly impact program review, curriculum development, and student success initiatives.
- Pierpont will continuously evaluate and refine its assessment processes to ensure they remain responsive to the needs of students, faculty, staff, and external stakeholders.

Core Components of Institutional Assessment at Pierpont

To ensure a comprehensive and effective approach to assessment, Pierpont's Institutional Effectiveness Plan includes the following core components:

1. Academic Assessment
    a. Course Learning Outcomes (CLO) assessment
    b. Program Learning Outcomes (PLO) assessment and program review
2. General Education Learning Outcomes Assessment
3. Co-Curricular Activities Assessment
4. Administrative Unit (Non-Instructional) Review
5. Establishment of Institutional Key Performance Indicators (KPIs)
6. Closing the Assessment Loop and Sharing Results

Assessment findings will be regularly reviewed and communicated to faculty, staff, and leadership, ensuring that results drive meaningful institutional improvements.

By embedding structured assessment practices into college-wide operations, Pierpont strengthens its capacity for continuous growth, accreditation compliance, and institutional excellence—ensuring that all stakeholders benefit from Education That Works.

4. INSTITUTIONAL EFFECTIVENESS AND DATA GOVERNANCE COMMITTEES

Strategic Planning Committee

The Strategic Planning Committee at Pierpont Community & Technical College is responsible for guiding the institutional planning process, ensuring that strategic goals and initiatives align with the college's mission, vision, and 2024-2026 Strategic Alignment Plan. The committee assists the President and senior leadership in setting institutional priorities, identifying long-term strategies, and evaluating services, policies, and procedures to foster continuous improvement.

The committee is composed of faculty, staff, and administrators representing various departments and functional areas of the college. Members collaborate to:

- Develop goals and objectives that support institutional effectiveness and student success.
- Monitor progress on strategic initiatives and make data-informed recommendations for improvement.
- Ensure alignment between the Strategic Plan, accreditation requirements, and institutional priorities.

This committee plays a critical role in shaping the future of Pierpont by fostering a culture of accountability, innovation, and strategic decision-making.

Data and Institutional Effectiveness Committee

The Data and Institutional Effectiveness Committee provides oversight and guidance for data-driven decision-making across the institution. The committee is responsible for ensuring that institutional data is accurate, accessible, and effectively used to support assessment, planning, accreditation, and reporting.

The committee is composed of representatives from academic affairs, student services, institutional research, finance, and administrative units, working collaboratively to:

- Establish key performance indicators (KPIs) and benchmarks for assessing institutional effectiveness.
- Review and analyze student success metrics, enrollment trends, retention rates, and program performance.
- Ensure compliance with state, federal, and accreditation data reporting requirements.
- Promote data literacy across campus, empowering faculty, and staff to use data effectively in their decision-making processes.

By fostering a culture of evidence-based assessment, this committee ensures that Pierpont remains responsive to institutional needs and committed to continuous improvement.

5. INSTITUTIONAL DATA MANAGEMENT AND USAGE

Purpose of Data Management

Pierpont Community & Technical College is committed to using accurate, reliable, and secure data to support institutional effectiveness, strategic planning, assessment, and decision-making. The college's data governance framework ensures that institutional data is collected, analyzed, and disseminated in a way that promotes continuous improvement, compliance, and accountability.

This section outlines how data is managed across the institution, ensuring that faculty, staff, and administrators have access to timely, high-quality data that informs student success initiatives, program evaluation, and resource allocation.

Institutional Data Usage & Governance

Institutional data at Pierpont is utilized across various departments and operational units to support:

- Strategic Planning – Tracking progress on institutional goals outlined in the 2024-2026 Strategic Alignment Plan.
- Institutional Assessment – Evaluating program effectiveness, student success, and operational efficiency.
- Accreditation & Compliance – Ensuring alignment with Higher Learning Commission (HLC) standards, WVHEPC reporting requirements, and federal regulations.
- Student Success & Retention – Monitoring enrollment trends, course completion rates, persistence, and graduation rates to inform interventions and support services.
- Financial & Resource Planning – Using financial, enrollment, and workforce data to guide budgetary and operational decisions.
- Workforce & Community Engagement – Assessing workforce training program outcomes and employer partnerships.

The Office of Institutional Effectiveness and Research, in collaboration with the Data and Institutional Effectiveness Committee, oversees data governance policies, reporting, and analytics to ensure alignment with institutional priorities.

Key Data Sources & Systems

Pierpont collects and manages data from multiple sources, including:

- Student Information System (SIS) – Banner (enrollment, demographics, course performance).
- Customer Relationship Management (CRM) - Salesforce
- Learning Management System (LMS) – Assessment of student engagement and learning outcomes.
- Institutional Surveys & Evaluations – Student satisfaction, faculty/staff engagement, and employer feedback.
- Power BI & R – Dashboards for real-time data visualization and predictive analytics.
- IPEDS & WVHEPC Reports – Compliance and benchmarking with peer institutions.

Each system plays a role in ensuring data-driven decision-making across academic, administrative, and operational areas.

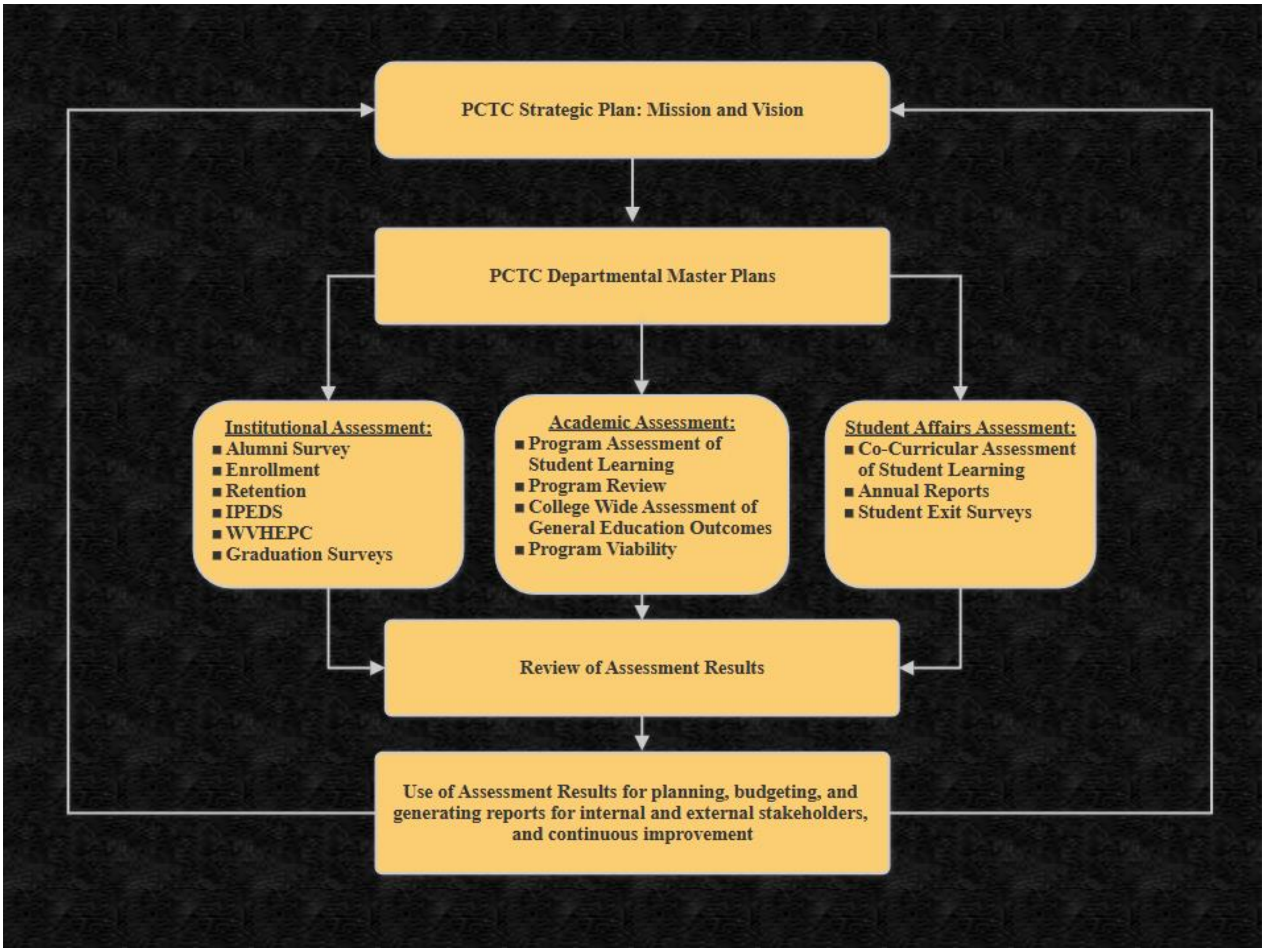
Data Governance & Compliance

To protect data integrity and security, Pierpont follows institutional, state, and federal policies related to data governance, including:

- FERPA (Family Educational Rights and Privacy Act) – Ensuring student data privacy.
- HLC & WVHEPC Reporting Requirements – Compliance with accreditation and state standards.
- Data Security Protocols – Secure storage, restricted access, and cybersecurity measures.
- Institutional Data Access Policies – Guidelines on how faculty, staff, and administrators access and use data.

Pierpont is committed to transparency and responsible data stewardship, ensuring that institutional data is used ethically and effectively to support student learning, institutional accountability, and operational excellence.

6. INSTITUTIONAL EFFECTIVENESS MODEL


PCTC Strategic Plan: Mission and Vision
PCTC Departmental Master Plans
Institutional Assessment:
■ Alumni Survey
■ Enrollment
■ Retention
■ IPEDS
■ WVHEPC
■ Graduation Surveys
Academic Assessment:
■ Program Assessment of Student Learning
■ Program Review
■ College Wide Assessment of General Education Outcomes
■ Program Viability
Student Affairs Assessment:
■ Co-Curricular Assessment of Student Learning
■ Annual Reports
■ Student Exit Surveys
Review of Assessment Results
Use of Assessment Results for planning, budgeting, and generating reports for internal and external stakeholders, and continuous improvement

7. INSTITUTIONAL EFFECTIVENESS GOALS

Goal 1: Support the Implementation, Assessment, and Continuous Improvement of the Strategic Plan

- Maintain and regularly update the 2024-2026 Strategic Alignment Plan to reflect progress and evolving institutional priorities.
- Provide accurate, timely data to assess performance on Strategic Plan goals and key performance indicators (KPIs).
- Assist with preparing mid-year and annual institutional effectiveness reports to track progress on strategic objectives.
- Work with West Virginia Community & Technical College System (WVCTCS) and accrediting agencies to submit required reports and documentation related to institutional effectiveness and performance metrics.
- Utilize assessment results to inform continuous improvement initiatives across academic, administrative, and student support services.

Goal 2: Ensure Timely and Accurate Data Reporting for Internal and External Stakeholders

- Serve as the primary data coordinator for compliance reporting to WVCTCS, the Higher Learning Commission (HLC), and federal agencies (IPEDS, NCES, etc.).
- Maintain and disseminate institutional performance dashboards using Power BI to support data-informed decision-making across campus.
- Provide accurate job placement and workforce outcome data for graduates of career-technical programs to meet workforce and employer engagement goals.

- Ensure accurate data collection and reporting for accreditation self-studies, program reviews, and institutional research projects.

Goal 3: Strengthen Data Collection, Assessment, and Decision-Making in Academic, Administrative, and Student Services Units

- Assist Academic Affairs in coordinating academic program reviews, ensuring that faculty have the data needed for curriculum assessment and improvement.
- Support faculty and staff in designing, conducting, and analyzing student learning assessments, surveys, and program evaluations.
- Facilitate the collection and analysis of co-curricular assessment data, ensuring alignment with student learning and institutional effectiveness goals.
- Conduct institutional research surveys to document successes, challenges, and areas for improvement in academic programs, student services, and operational functions.
- Provide training and support to faculty, staff, and administrators on the use of data in decision-making, strategic planning, and continuous improvement efforts.
- Coordinate, supervise, and assist with the academic and co-curricular assessment of student learning

APPENDIX

Tab

3

Data Management Plan

Pierpont Community and Technical College

TABLE OF CONTENTS

PURPOSE AND SCOPE

Effective data management is critical to Pierpont Community & Technical College's mission and strategic goals. Managing institutional data ensures that decision-makers at all levels have reliable information to drive institutional effectiveness, enhance student success, and guide strategic planning. In higher education, colleges handle vast data ranging from student records to financial and research information, and proper management of this data underpins informed decisions, regulatory compliance, academic excellence, and operational efficiency. Pierpont's own planning documents emphasize that "the importance of regular collection and analysis of data cannot be overstated," assuming data is readily available and accessible to inform ongoing discussions of institutional priorities. In short, robust data management enables the college to measure progress, identify improvement opportunities, and allocate resources in alignment with its strategic plan and student success objectives.

Scope – Data Types Covered: This Data Management Plan encompasses all institutional data across the college. Key data categories in scope include:

- Student Records: Admissions data, enrollment information, academic transcripts, grades, and graduation records (primarily from the Banner student information system).
- Academic Data: Course and program information, learning outcomes, assessment results, and learning management system data (e.g. Blackboard analytics on student performance).
- Financial Data: Budget and accounting records, tuition and fee data, financial aid information, and other fiscal records.
- Human Resources Data: Employee records, payroll, HR benefits, and staffing information.
- Research & Institutional Effectiveness Data: Data from institutional research, surveys, program reviews, and any faculty/staff research data that falls under college management.
- Other Operational Data: Additional data from departments such as facilities, advancement/alumni engagement, or other administrative units as applicable.

By defining the scope in this way, Pierpont ensures that all critical data assets – from student-centric to administrative – are covered under a common management and governance framework.

1. DATA GOVERNANCE AND OVERSIGHT

Pierpont will establish a clear data governance structure to oversee the quality, integrity, and use of institutional data. A cross-functional Data Governance Committee (DGC) will be responsible for setting data policies and standards, ensuring data is accurate and secure, and resolving any data ownership or quality issues. This committee will oversee the quality, integrity, security, and usability of data collected and stored by the college. The DGC will report to senior leadership (e.g. the President or Cabinet) and include representatives from each major division of the college. This shared governance approach brings together key stakeholders to collaboratively manage data resources, reflecting the college's culture of informed decision-making and accountability. The committee may be co-chaired by leaders from Information Technology (IT) and Institutional Effectiveness (IE) to balance technical and academic perspectives in data oversight.

Roles and Responsibilities: Clear roles are defined for departments and individuals involved in data management to ensure accountability:

- Information Technology (IT) Department: Maintains the technical infrastructure for data systems (servers, databases, integrations) and is responsible for data security measures and system administration. IT ensures reliable storage, backups, and uptime for critical data systems and supports the development of reporting tools.
- Office of Institutional Effectiveness (or Institutional Research): Coordinates data governance efforts and analysis. This office acts as a steward for data quality and consistency, synthesizing data from different systems and ensuring that reports/analyses align with strategic planning needs. They also often serve as a point of contact for data requests and official reporting.
- Academic Affairs (Provost/Deans/Registrar): Oversees academic data integrity. The Registrar's office and academic deans ensure that student academic records, course data, and assessment results are recorded accurately and used appropriately for accreditation and continuous improvement. Academic Affairs representatives work to define data definitions/standards for academic programs and outcomes.

- Student Services (Enrollment Management and Student Affairs): Manages student-related data throughout the student life cycle. This includes admissions and recruitment data (often via the CRM), advising and support services data, and retention/engagement metrics. They ensure student records in Banner and other systems are updated and coordinate with IE for analysis on student success indicators.
- Finance Department: Responsible for financial and budgetary data governance. The finance team ensures accuracy of financial records (accounts, budgeting systems, financial aid disbursements) and controls access to sensitive financial information. They provide data for audits and financial reporting, aligning financial data management with institutional policies.
- Human Resources (HR): Ensures proper management of employee data. HR maintains confidential faculty and staff records and is responsible for compliance in handling personal identifiable information of employees. They coordinate with IT on permissions for HR systems and with IE if employee data is needed for institutional reporting (in aggregate form).

These stakeholders work together through the Data Governance Committee to set policies (such as data definitions, data quality standards, and usage guidelines) and to address any cross-departmental data issues. For example, the committee might establish common definitions for data elements across campus and serve as a single point of contact for approving data requests and resolving data discrepancies. By involving a broad set of offices, Pierpont ensures shared responsibility for data governance, which aligns with best practices in higher education governance and fosters buy-in from all areas of the college.

2. DATA COLLECTION, STORAGE AND SECURITY

Data Collection Protocols: Pierpont collects and updates data through its core enterprise systems, with defined protocols to ensure data accuracy and completeness. The primary systems include Ellucian Banner (Student Information System), Salesforce Education Cloud (Constituent Relationship Management system), and Blackboard (Learning Management System):

- Banner (Student Information System): Banner serves as the system of record for student data – including admissions information, course registrations, grades, transcripts, and demographic details. Data entry into Banner is performed by authorized offices (e.g. admissions, registrar, financial aid) following standardized procedures. Key student record updates (enrollment status, grades, etc.) are entered in real-time by staff. Regular data extracts or integrations are configured to pull relevant data from Banner into the college's reporting databases. For instance, enrollment and academic progress data from Banner are periodically exported (e.g. nightly or weekly) to a data warehouse or directly into analytics tools for broader use. Data validation checks are in place to catch input errors (such as impossible grade values or invalid student IDs) to maintain Banner data integrity.
- Salesforce (CRM for Recruitment/Engagement): Pierpont has implemented Salesforce Education Data Architecture (EDA) as its CRM to track prospect and student engagement. This system collects data on communications with prospective students, applicant information, and can also support retention efforts by tracking student contacts and interventions. Data from Salesforce (such as inquiry records, communication logs, event attendance, and other engagement metrics) is integrated with student information from Banner to provide a more complete view of the student lifecycle. Protocols ensure that new inquiry or applicant data flows from Salesforce into Banner when a prospect becomes an enrolled student, and vice versa, some Banner data (like student ID or enrollment status) may sync back to Salesforce to update records. The IT department manages these integrations via secure APIs or batch processes, ensuring that the CRM and SIS data remain consistent.

- Blackboard (Learning Management System): Blackboard is used to deliver courses and track academic performance data such as course grades, assignment submissions, and student participation. Data collection from Blackboard includes capturing grades for each term, course completion statuses, and learning analytics (e.g. login frequency, content access) that can serve as early indicators of student engagement. Instructors input grades and feedback into Blackboard, and this data can be extracted via reporting tools or direct database queries. Pierpont's data protocol includes pulling Blackboard data (such as end-of-term grade distributions or midterm progress reports) into the institutional data repository. For example, reports on course pass/fail rates or students flagged as at-risk (via Blackboard's early alert features) are collected each semester to support student success initiatives.

All these systems are connected through an overarching data architecture. The Office of Information Technology coordinates data integration efforts so that data from Banner, Salesforce, and Blackboard can be compiled for analysis and reporting. Where possible, automated interfaces connect these systems – for instance, the college's new CRM and the IT department's PowerBI data dashboard work in tandem to facilitate data collection from various sources and provide a centralized source of institutional information for end users. In cases where real-time integration is not available, scheduled batch uploads and manual data import processes are defined (with clear procedures for file formats and timing) to ensure data from all departments is captured routinely. Consistent data definitions (e.g. what constitutes an "enrolled student" or an "active program") are used across these systems to ensure that when data is merged, it aligns correctly.

Data Storage Locations: Collected data is stored in secure, centralized repositories managed by IT. Banner and Salesforce operate on enterprise databases that are hosted on secure servers (either on-premises data center servers or within a trusted cloud environment). Blackboard data resides in the learning management system's database, which is also secured and managed by either the college or the vendor. To support reporting and analytics, Pierpont utilizes a database for dedicated reporting where snapshots of Banner/Salesforce/Blackboard data are aggregated. This centralized data storage acts as the "single source of truth" for institutional reporting, minimizing reliance on disparate spreadsheets or local files. Access to these storage systems is tightly controlled (see Access & Usage Policies below) and managed by database administrators. In addition, unstructured data (like survey results or ad-hoc datasets) are stored in approved locations on the college network with appropriate protections.

Security Measures: Protecting the security and privacy of Pierpont's data is paramount. The college employs multiple layers of security for data storage and transfer:

- Encryption: All sensitive institutional data is encrypted both in transit and at rest. When data moves between systems (for example, transferring student data from Banner to the data warehouse or from Salesforce to Banner), it is sent over encrypted connections (SSL/TLS) to prevent eavesdropping. Databases and backups are encrypted at rest, so that if storage media were compromised, the data would remain unreadable without proper keys.
- Backups and Recovery: Nightly backups of all critical databases (student information, CRM data, learning management data, etc.) are performed and securely stored. Backup files are kept in encrypted form and in geographically separate storage (such as an off-site server or cloud backup service) to protect against data loss scenarios like hardware failure or disasters. The IT department tests data restoration procedures periodically to ensure backups are reliable and that the college can quickly recover data in the event of data corruption, accidental deletion, or other emergencies.
- Access Control: Strict access controls are in place to ensure only authorized personnel can view or modify data. Each system (Banner, Salesforce, Blackboard, and the data warehouse) uses role-based permissions and individual user accounts. Users are granted the minimum level of access necessary for their job (principle of least privilege). For example, a financial aid officer can view and update financial aid records in Banner but cannot access HR salary data; an instructor can enter grades for their courses in Blackboard but cannot see students outside their classes. Administrative access to databases is limited to a few database administrators in IT, and any direct queries or data extracts from backend systems require approvals. Multi-factor authentication is enabled for remote or high-privilege access to further secure against unauthorized login.

- Network and Physical Security: The servers hosting institutional data are protected behind firewalls and intrusion detection systems monitored by IT. Regular security audits and vulnerability assessments are conducted to patch any weaknesses. Physical servers (if on campus) reside in locked data centers with access restricted to IT staff. If using cloud-hosted systems (like a vendor-managed cloud for Banner or Salesforce), the vendors are vetted for robust security certifications and compliance. Additionally, the college requires secure configurations and follows best practices recommended by those vendors.
- Data Retention and Disposal: As part of security, Pierpont also defines retention periods for various data types. Data is retained as long as needed for educational or business purposes and legal compliance, after which secure disposal methods (such as shredding of physical documents or certified digital deletion) are used. Ensuring that outdated personal data is not kept longer than necessary mitigates risk. All disposal of records follows protocols to prevent any recovery of sensitive information.

Through these collection protocols and security measures, Pierpont ensures that data from all sources is not only gathered efficiently but also stored safely. The college's approach aligns with best practices in protecting sensitive information from unauthorized access or breaches while maintaining high availability and integrity of data for those who need it.

Regular security training is provided to staff who handle data, so they understand procedures like how to properly transmit data, store files securely, and recognize potential security threats (phishing, etc.). In summary, data is collected systematically from key systems, housed in secure centralized storage, and guarded by robust security controls at all times.

3. DATA ACCESS AND USAGE POLICIES

Access to institutional data at Pierpont is governed by well-defined policies that ensure data is used ethically and only by appropriate personnel. The college employs role-based access control (RBAC), meaning an individual's job role determines what data they can view or edit. This ensures confidentiality of sensitive information while allowing community members to access the data they need to perform their duties. All users must authenticate (log in) through approved systems, and access privileges are reviewed periodically to adjust for job changes or detect any excessive rights. The "need-to-know" principle is enforced: users see only the information required for their role, preventing unnecessary exposure of student or institutional data.

Role-Based Access for Internal Users: Different groups of college personnel have access to different subsets of data, as outlined below:

- Faculty: Faculty members have access to academic information for the students and courses they teach or advise. For example, an instructor can access class rosters, student profiles relevant to their classes, and input or view grades for their courses. Academic advisors (often faculty or professional advisors) can view the records of students assigned to them, including transcripts, degree audits, and flags for at-risk students, in order to provide guidance. Faculty do not have access to data outside their purview (e.g. a professor cannot browse all student records or financial details) – this protects student privacy. When faculty need additional data (such as aggregate data on course outcomes for assessment), they request it through the Institutional Effectiveness office or the data governance process rather than accessing raw data themselves.
- Staff: Staff access is tailored to their departmental functions. Student services staff (admissions officers, registrars, financial aid counselors, etc.) have access to the student data necessary for their operations. For instance, admissions staff use Salesforce CRM data and relevant Banner fields to track applicants; the Registrar's team accesses academic records to manage registration and transcripts; financial aid staff access financial need, award, and payment data in Banner. Advisors and student support staff can see holistic student information (academic and some personal data) to

coordinate interventions. In the Finance department, staff can access financial ledgers, budget systems, and student billing information as needed for accounting and audits. HR staff have exclusive access to HR databases for employee information, which is segregated from student databases. Importantly, each staff member is trained to only use data within the scope of their job – e.g. an HR employee would not query student records, and a student services employee would not open HR files. Cross-departmental staff access (e.g. a grant manager needing both financial and student data) is granted only if approved by the data owners and in line with policy.

- Administrators: Administrators (department heads, deans, vice presidents, and other executives) often require a broader view of data across the institution for planning and oversight. Rather than unrestricted access to raw databases, administrators are typically given access to aggregated reports and dashboards (for example, via Power BI) that compile key metrics. Through these tools, an administrator can review trends in enrollment, retention, budget utilization, etc., without needing direct access to every underlying record. If detailed data is needed, the request goes through proper channels. Certain senior administrators – such as the Registrar, CIO, or Director of Institutional Research – by virtue of their role as data stewards, may have more extensive data access in order to fulfill reporting duties. Even so, their use of data is bound by confidentiality rules and ethical guidelines. All administrators with access to student or employee personally identifiable information (PII) are expected to handle it with the same care and compliance as any other staff member.

Internal Data Sharing: Within the college, sharing of data across departments is done carefully and only as appropriate. Departments do not freely exchange raw data; instead, if one department needs information maintained by another, they will go through an approved data request process. For example, if Academic Affairs needs data on alumni employment outcomes (which might be collected by an Advancement office), a request is made to the data owner or the Data Governance Committee. That request is evaluated to ensure the data is used for a legitimate educational or operational purpose and that any privacy concerns are addressed (such as removing names if individual identities aren’t needed). By channeling inter-department data sharing through Institutional Effectiveness or the data governance framework, Pierpont ensures that data remains consistent (everyone uses the same official figures) and that usage is tracked. This process also prevents duplicate or conflicting data sources from proliferating. In practice, data stewards from relevant offices may prepare a report or grant limited access to a specific dataset for the requesting party. All internal sharing abides by the rule that the receiving party must handle the data under the same security and privacy standards as the originating department.

External Data Sharing: Pierpont maintains strict policies for sharing institutional data with external stakeholders. External requests can come from entities like state and federal education agencies, accreditors, research partners, or the general public (e.g. via Freedom of Information requests or mandated disclosures). The college designates specific offices (primarily Institutional Effectiveness/Research, the Registrar, or the Office of the President, depending on the nature of the data) to handle official data disclosures. Any data released outside the institution must be approved by the appropriate authority and comply with privacy laws and college policies. Personally identifiable student or employee information is not shared externally unless required by law (for example, reporting certain data to government education departments) and even then it is transmitted securely. Typically, external reports use aggregate data – for instance, overall graduation rates or total enrollment figures are provided to the public or state board, rather than individual student records. If Pierpont enters into a research collaboration or partnership that involves data sharing, a formal data sharing agreement or memorandum of understanding is put in place. This agreement will stipulate how the data can be used, how it will be protected, and require that the external party uphold confidentiality (often including that any published analysis will not identify individuals). Before releasing any dataset externally, the Data Governance Committee (or a data steward) reviews it to remove or mask any sensitive personal identifiers unless disclosure of such detail is authorized. Additionally, the college tracks what data was shared, with whom, and for what purpose, creating an audit trail for accountability.

Usage Policies and Ethics: All faculty, staff, and administrators are expected to use institutional data ethically and in accordance with training and guidelines. Pierpont's data usage policy (communicated via annual trainings and the employee handbook) emphasizes that data access is a privilege and must be used only for legitimate educational interests or job functions. Misuse of data – such as accessing records out of curiosity, altering data without authorization, or sharing confidential information inappropriately – is prohibited and could result in disciplinary action. Users must also adhere to data privacy principles: for example, if an employee is given access to student social security numbers for a task, they cannot disclose that information to others or use it for any non-official purpose. The college fosters a culture where data-driven decision making is encouraged, but always with respect for student and employee privacy and data accuracy. By establishing these role-based access rules and usage policies, Pierpont protects data from unauthorized exposure while empowering faculty and staff to leverage data for improving outcomes. This careful control of “who sees what” is a cornerstone of data governance that keeps the institution’s data assets secure and trustworthy.

4. DATA REPORTING AND ANALYTICS

Pierpont Community & Technical College leverages data reporting and analytics to translate raw data into actionable insights. A central part of this strategy is the use of Microsoft Power BI for dashboards and reports that aggregate data from Banner, Salesforce, Blackboard, and other sources. The college's institutional data dashboard (developed by the Office of the VP of IT) provides a one-stop, interactive view of key metrics across the institution.This Power BI dashboard is designed to be a centralized source of institutional information for end users, breaking down historical silos of data and making information accessible in one place. Initially, such dashboards have been rolled out to administrators for planning purposes, but they are being expanded for use by faculty and staff as needed, aligning with Pierpont's goal of broadening data-informed decision making across the campus.

Reporting Tools and Processes: The IT and Institutional Effectiveness teams collaborate to maintain the data dashboard and reporting system. Data from core systems is refreshed on a regular schedule into Power BI – some data updates are near real-time (for instance, new admissions or enrollment numbers might update daily during peak periods), while other metrics update each term or year as appropriate. Power BI allows the creation of interactive reports and visualizations that users can drill down into (e.g. an administrator could filter retention rates by year or by student demographics). In addition to live dashboards, static reports are generated on a schedule for official needs. For example, an Enrollment Report might be produced after each semester's census date, summarizing total enrollment, new student counts, and credit hours, which is then shared with the President and Board of Governors. Likewise, Retention and Graduation Reports could be prepared annually to review how many students persisted or completed, often aligning with the academic year cycle or reporting deadlines of external agencies like IPEDS. The college uses Power BI to automate much of this reporting; once data models are in place, updated data automatically flows into charts and tables for each reporting period, reducing manual work and error.

Key Performance Indicators (KPIs): Pierpont's data analytics efforts focus on a set of institutional KPIs that align with strategic priorities. These KPIs are the metrics deemed most crucial for monitoring institutional health and progress. While specific targets for these KPIs may be set by the President’s Executive Cabinet and leadership (following a philosophy of continuous improvement), the Data Management Plan ensures these indicators are measured and reported consistently. Common KPIs at Pierpont include:

- Enrollment Metrics: such as the number of applications, admit rates, yield (conversion of admitted to enrolled students), and total student headcount by semester. These metrics help gauge recruiting effectiveness and are often reported each term. For instance, Power BI dashboards track the admissions funnel – inquiries, applicants, admits, and enrollments – with comparisons to past years and targets.

- Student Retention Rates: including fall-to-spring retention and fall-to-fall retention for first-year students and other cohorts. Retention is a key student success metric; Pierpont monitors it closely, reporting outcomes annually and by term. The college looks at overall retention as well as breakdowns (full-time vs part-time, program-wise retention, etc.), using tools like the dashboard and IPEDS data for benchmarking.

- Graduation and Completion Rates: for degree and certificate programs, typically measured at 150% of program length (e.g., 3-year graduation rate for 2-year programs). These are reported annually and used in strategic planning to improve completion. Pierpont tracks graduation rates for various student groups (such as first-time full-time students, Pell grant recipients, etc.) to identify gaps and improvements.

- Academic Achievement Indicators: such as course completion rates (percentage of students passing courses), average GPA by term, and progress metrics like credit accumulation. Additionally, data from academic assessments (e.g. general education competency results, licensure exam pass rates for certain programs) are reported to gauge learning outcomes. For example, the college compiles data on general education assessment results each year to inform curriculum improvements (as noted in assessment reports appended to strategic plans).

- Student Engagement & Success Measures: including utilization of support services (advising contacts, tutoring sessions), early-alert referrals, and other engagement metrics that can predict student success. These may be tracked via both CRM (Salesforce) data and LMS data. The data management plan includes these as KPIs to ensure student services initiatives are data-informed (e.g., seeing if an increase in tutoring usage correlates with higher course pass rates).

- Operational and Financial Metrics: Pierpont also monitors data such as budget performance, revenue and expenditure trends, and efficiency metrics (like student-to-faculty ratio, class fill rates). While academic and student data are the primary focus, financial and operational data are included in analytics for a comprehensive view of institutional effectiveness. Dashboards might show budget vs. actual spending by quarter, or key ratios that are reported to the Board. HR metrics like employee turnover or faculty workload could also be considered if they align with strategic goals.

Each KPI has an associated reporting schedule. For example, enrollment funnel metrics might be reviewed weekly during recruitment season and in a formal report each semester; retention and graduation rates are reviewed after each academic year (and mid-year for internal progress checks); academic performance indicators are analyzed at the end of each term; and financial metrics are monitored monthly and compiled in quarterly reports. The Institutional Effectiveness office ensures that for each KPI, there is a designated data source and method of calculation documented, so reports are consistent over time. They also coordinate the creation of an annual institutional effectiveness dashboard/report that combines these KPIs to provide an overall performance snapshot to leadership and stakeholders.

The use of Power BI and a centralized database greatly streamlines Pierpont's reporting capabilities. Instead of hunting for data across different offices, stakeholders can rely on the official dashboards where "all information is available" in one place. This not only improves efficiency but also data transparency; trends and outcomes are visible to those who need them. Moreover, by analyzing these KPIs, the college can identify areas of success or concern. For instance, if retention rates dip, the data will highlight that quickly, prompting an investigation and response. In summary, data reporting and analytics at Pierpont turn raw data into meaningful insights via dashboards, regular reports, and KPI tracking – all to support informed decision-making at every level of the institution.

5. COMPLIANCE & BEST PRACTICES

Pierpont's data management practices adhere to high standards of data privacy, security, and ethical use, ensuring that all institutional data is handled in compliance with applicable guidelines and with respect for individual confidentiality. While specific laws (such as student privacy regulations or data protection laws) are not enumerated here, the college is committed to following all relevant legal requirements and prevailing best practices in higher education data management. Key principles and best practices include:

- Data Privacy & Confidentiality: The privacy of student, faculty, and staff information is paramount. All institutional data – especially personally identifiable information (PII) like social security numbers, grades, health or financial details – is treated as confidential. Access to such data is limited and governed by the policies outlined above. Staff and faculty are trained to not disclose sensitive information to unauthorized parties and to report any suspected privacy breaches immediately. When data is used for analysis or reporting, only the required information is extracted, and wherever possible, data is aggregated or anonymized to protect individual identities. These practices align with the idea that colleges must protect sensitive data (student records, financial info, etc.) from unauthorized access or use. By maintaining confidentiality, Pierpont also builds trust with students and employees that their personal information is safe.
- Accuracy & Integrity of Data: The value of data for decision-making depends on its accuracy. Pierpont follows best practices to maintain data integrity at all stages. This includes validation rules at data entry (to reduce errors), regular data cleaning routines, and reconciliation processes (for example, ensuring that enrollment numbers in Banner match those reported in summary dashboards). If discrepancies or errors are found, they are documented and corrected promptly. Data owners (stewards) in each area are responsible for the accuracy of the data in their purview – e.g. the Registrar for student academic records, HR director for employee data. The Data Governance Committee supports a culture of data quality by establishing standards and auditing critical datasets periodically. By ensuring data is "accurate, consistent, and reliable," the college can trust the information used in planning.

- Data Security: Strong security measures (as detailed in Section 3) are a fundamental best practice to prevent data breaches or loss. Pierpont continuously updates its security protocols in line with emerging threats and technology standards. This includes keeping systems patched and up-to-date, enforcing complex passwords and multi-factor authentication, and monitoring network activity for any signs of intrusion. Access logs are maintained so that any inappropriate access or unusual data download can be detected and investigated. The college also has an incident response plan: if a data breach or suspected breach occurs, there are clear steps to contain the issue, notify affected parties and authorities as needed, and remediate the vulnerability. Regular security awareness training is mandatory for employees, covering topics like phishing scams, proper handling of sensitive data, and device security. These efforts reflect industry best practices and ensure compliance with general data protection obligations to secure data assets.
- Ethical Data Usage: Pierpont encourages the use of data to drive decisions, but it must be done ethically. This means data should be used in ways that are fair, transparent, and in service of the college's mission to educate and support students. Examples of ethical considerations include: avoiding bias in data analysis (e.g., not using data to unjustly profile or discriminate against any group), ensuring that data analysis is presented honestly (with no manipulation to mislead), and respecting student autonomy and consent when appropriate (for instance, if survey data is collected from students, being clear about how it will be used). The Data Governance Committee may develop guidelines or case studies to help employees navigate ethical dilemmas, reinforcing an institutional norm that data is a tool for improvement, not surveillance or punishment. By establishing clear ethical guidelines, Pierpont ensures that all stakeholders understand how data should and should not be used.
- Compliance with Regulations and Policies: Although this plan doesn't list specific regulations, the college complies with all applicable federal, state, and accreditation requirements regarding data. For example, student educational records are handled in accordance with privacy principles common to laws like FERPA (which restrict disclosure without consent), even if not named here. Financial data handling follows standards akin to those required by auditors and financial regulations, ensuring

accuracy and security. Any research involving personal data would go through an Institutional Review Board (IRB) process if applicable, to uphold ethical standards. Additionally, Pierpont aligns its data practices with guidance from bodies like EDUCAUSE or state higher education authorities on managing and protecting data. Internal policies (such as an Acceptable Use Policy for IT systems, data retention policy, etc.) complement this plan and are regularly reviewed to stay current. The Data Governance Committee conducts periodic reviews to verify that data management practices remain in compliance with any new laws or institutional policies, and recommends updates as needed.

In essence, the college is proactive about safeguarding data and using it responsibly. This commitment to privacy, accuracy, security, and ethics in data management not only avoids compliance pitfalls but also supports an environment of trust and accountability. Stakeholders can be confident that data-driven initiatives at Pierpont are carried out with respect for individuals' rights and the integrity of information. Such a foundation is crucial because it enables the institution to leverage data effectively for student success and institutional improvement without compromising ethical standards.

6. REVIEW & CONTINUOUS IMPROVEMENT

This Data Management Plan is not a static document – it is intended to evolve as the college's needs, technologies, and external conditions change. Pierpont commits to an annual review process for the Data Management Plan to ensure it remains effective and up-to-date. The Data Governance Committee (or a designated data management task force) will lead this yearly review, typically at the end of each academic or fiscal year. During the review, the committee will:

- Evaluate Effectiveness: Assess how well current data practices are working. This involves gathering feedback from data users (faculty, staff, analysts) on any challenges they faced in data access or quality, and reviewing any incidents (such as security breaches or significant errors) that occurred in the past year. If, for example, users report difficulty in retrieving certain reports or if inconsistent data definitions caused confusion, those issues will be noted for improvement.
- Incorporate New Needs and Technologies: Update the plan based on any new institutional needs, systems, or tools. If Pierpont adopts a new technology (for instance, a new Learning Management System replacing Blackboard, or an upgraded Banner version, or a new data analytics platform), the plan's sections on data collection, access, and security will be revised accordingly. Similarly, if the college embarks on new strategic initiatives (say, a push for online programs that requires tracking additional data, or a new research partnership), the scope and protocols will be adjusted. The annual review will include checking for any emerging best practices in the field that Pierpont should adopt.
- Ensure Ongoing Compliance: As part of the review, the committee will verify that the Data Management Plan and all related procedures are in line with current laws, regulations, and policies. If new data protection regulations have come into effect or if accrediting bodies have updated their data requirements, those will be integrated into the plan. The committee references any audits or compliance reports (for example, results from a security audit or a data privacy assessment) to identify required changes.

This practice mirrors what other institutions do – for instance, conducting annual compliance checks against new laws– to make sure the college is never out of step with legal obligations.

- Update Policies and Documentation: Based on the findings, the Data Governance Committee will draft revisions to policies or procedures. Changes could range from minor (clarifying a definition or adding a new data element to the scope) to major (introducing a new data access protocol or security measure). The revised Data Management Plan will be reviewed and approved by senior leadership (ensuring alignment with institutional strategy). After approval, the updates are communicated campus-wide. Documentation, such as user guides for the data dashboard or the data request process, will also be updated to reflect any changes. Training sessions may be held if there are significant updates that faculty/staff need to be aware of.

Pierpont embraces a philosophy of continuous improvement in its planning and assessment processes, and data management is no exception. The annual review cycle allows the college to continually refine how data is governed and used, rather than letting policies become obsolete. Moreover, the Data Governance Committee remains active throughout the year – not just during the annual review – by meeting regularly to discuss ongoing issues or proposals. If an urgent need for a policy change arises (for example, addressing a data security vulnerability or an urgent report requirement), the committee can convene and adjust the plan on an interim basis, with proper approvals, rather than waiting for the year-end review.

Continuous Improvement Example: If the college notices that a certain KPI target is consistently not being met because the underlying data was not being captured accurately, the committee might decide mid-year to implement a new data collection procedure for that metric. This would then be formally written into the plan during the annual update. Another example is user feedback: suppose department heads find the current access request process too slow, the committee might streamline it (perhaps by introducing a new online request form or delegating certain approvals) and update the plan accordingly. By responding to feedback and outcomes, Pierpont ensures the Data Management Plan remains a living document that truly supports its institutional effectiveness goals.

Communication and Accountability: After each review cycle and update, the revised Data Management Plan is redistributed to all relevant stakeholders (published on an internal site and highlighted in meetings or training). Everyone who interacts with institutional data is reminded of their responsibilities under the updated plan. The college might also include a summary of data management improvements in its annual institutional effectiveness report or strategic plan progress report, thereby maintaining transparency about how data governance is adapting to support the college's mission.

In summary, Pierpont's Data Management Plan is subject to regular assessment and enhancement. By instituting an annual review and embracing continuous improvement, the college ensures that its data practices remain current, secure, and aligned with both best practices and the evolving needs of the institution. This iterative approach enables Pierpont to better leverage data for decision-making and student success year over year, making data management a dynamic asset rather than a static policy document.

REFERENCES

1. Allegheny College. (n.d.). Data governance and institutional effectiveness framework. Retrieved from https://sites.allegheny.edu/ir/institutional-effectiveness/

2. Atlan. (2023). Data governance best practices: A guide for higher education institutions. Retrieved from https://atlan.com/data-governance-best-practices/

3. Blackboard. (2023). Learning analytics and student performance tracking in Blackboard LMS. Retrieved from https://www.blackboard.com

4. Columbia Advisory Group. (2023). Higher education data governance and IT security best practices. Retrieved from https://www.columbiaadvisory.com

5. EDUCAUSE. (2021). Higher education data governance: Best practices and implementation strategies. EDUCAUSE.

6. Ellucian. (2023). Banner student information system: Data governance and integration best practices. Retrieved from https://www.ellucian.com

7. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99 (1974).

8. Higher Learning Commission (HLC). (2022). Criteria for accreditation and institutional effectiveness guidelines. Retrieved from https://www.hlcommission.org

9. Integrated Postsecondary Education Data System (IPEDS). (2023). IPEDS data reporting guidelines for postsecondary institutions. U.S. Department of Education.

10. Microsoft. (2023). Power BI best practices for higher education institutions. Retrieved from https://www.microsoft.com/en-us/power-platform

11. National Center for Education Statistics (NCES). (2023). Best practices for institutional data reporting and analytics. U.S. Department of Education.

12. Pierpont Community & Technical College. (2024). Strategic alignment plan 2024-2026. Retrieved from https://www.pierpont.edu

13. Privacy Technical Assistance Center (PTAC). (2020). Data security and student privacy in higher education. U.S. Department of Education.

14. Salesforce. (2023). Education cloud for higher education: CRM data management and student engagement tracking. Retrieved from https://www.salesforce.org/highered

15. West Virginia Community & Technical College System (WVCTCS). (2022). Data collection, reporting, and institutional effectiveness guidelines. Retrieved from https://www.wvctcs.org

Tab

4

PIERPONT
COMMUNITY & TECHNICAL COLLEGE

Data Access Policy

Effective: June 2025

PURPOSE

The Data Access Policy establishes the rules and procedures by which authorized individuals obtain and use access to Pierpont C&TC's institutional data. The purpose of this policy is to ensure that employees, faculty, and other users have appropriate access to the data they need to perform their duties, while protecting sensitive information from unauthorized access or misuse. This policy balances the College's responsibility to safeguard data with its commitment to operational efficiency – data security measures should not unduly interfere with the College's business or academic processes. By defining access levels, data sharing methods, and user responsibilities, the policy aims to facilitate secure and ethical data sharing in compliance with applicable laws such as FERPA, the West Virginia Student DATA Act, and other privacy regulations.

SCOPE

This policy applies to all requests for and uses of institutional data at Pierpont C&TC, regardless of the data's format (electronic databases, cloud systems, paper records, etc.) or location. It covers all College employees, contractors, consultants, vendors, volunteers, and any other affiliates who are granted access to College data. The scope includes student educational records, employee records, financial data, research data, and any other institutional data used in official College operations. It encompasses both internal access (within the College) and external data sharing parties. All systems, applications, and computing devices that store or transmit College data are subject to this policy. Notably, this policy covers data sharing mechanisms (e.g. network file shares, email, reporting tools) and outlines secure methods for handling Personally Identifiable Information (PII) and other confidential information. It works in conjunction with the College's information security policies and any data-sharing agreements or contracts. Where stricter requirements are imposed by law or specific agreements (such as grant data use agreements or HIPAA for certain health-related data), those requirements will also apply within the framework of this policy.

POLICY

Policy Statement:
Pierpont C&TC will manage access to institutional data based on the principles of least privilege (users receive the minimum access necessary for their job) and need-to-know. The value of data as a College resource is maximized by its appropriate and widespread use, and conversely diminished by misuse, misinterpretation, or unnecessary restriction. Therefore, the College's policy is to allow broad access to data for legitimate institutional purposes, while implementing strong safeguards against unauthorized access. All institutional data must be classified by a Data

Steward to determine its appropriate access level, as defined in the data classification scheme below. Data designated as public may be freely accessed or released, whereas confidential and restricted data require stringent access controls. Data access decisions will comply with FERPA (for student records confidentiality) and other applicable laws, ensuring that personally identifiable information is disclosed only to authorized parties or with consent, except as permitted by law. The College will protect its data assets through technical, physical, and administrative security measures and will continuously monitor access for proper use. Any individual denied access to data that they believe is needed for their role may appeal the decision to the appropriate Data Steward, Data Trustee, or Data Governance Committee for reconsideration. Ultimately, data access is a privilege and carries with it the responsibility to use data ethically, securely, and in compliance with all College policies.

Roles and Responsibilities:

Proper data access management relies on coordinated Data Governance Policy. The key roles and their specific responsibilities for data access are:

- **Data Trustee**: Data Trustees have overall accountability for who may access data in their functional area. They set high-level access policies and ensure that Data Stewards in their area are reviewing and approving access appropriately. Data Trustees resolve conflicts or gray areas regarding access (for example, if data spans multiple departments). They also ensure that institutional data access practices comply with external regulations, such as reviewing that FERPA rules are upheld in granting access to student records. Data Trustees may periodically audit or require reports on data access provisioning to verify compliance with this policy.
- **Data Steward**: Data Stewards are the primary decision-makers for access to data under their oversight. They must classify each data element or dataset (see Data Classifications below) and assign an access level. Data Stewards review requests for access: they will grant access to institutional data only to individuals with a legitimate educational or business need as defined by their job duties. That access granted is appropriate (e.g., read-only versus edit rights) and corresponds to the user's role. Data Stewards maintain records of what access has been approved and periodically re-evaluate those permissions. In addition, Data Stewards work with Data Custodians to implement any special security requirements (such as two-factor authentication for highly sensitive data) and with Data Trustees to handle any appeals of denied requests. They also enforce the Data Usage rules outlined in this policy, ensuring that data under their care is used only for approved purposes and in compliance with FERPA and other laws.
- **Data Custodian**: Data Custodians (IT administrators, database managers, etc.) implement the technical side of data access control. Upon receiving authorization from a Data Steward, Data Custodians create user accounts, set permissions, and configure system settings to grant the approved level of access. They are responsible for maintaining secure systems, including regularly updating access controls, removing access that is no longer authorized (e.g., when a user's role changes or they leave the College), and monitoring for any unusual access patterns. Data Custodians should ensure that shared data storage solutions (like network folders or collaboration tools) have proper access restrictions and encryption as needed. They also educate Data Users on

secure data transfer methods (such as using encrypted email or approved file-sharing platforms) and enforce password policies and other safeguards for protecting login credentials. If a Data Custodian discovers any unauthorized access or security breach, they must immediately report it as outlined in the incident response procedures.

- **Data User**: Data Users are individuals who have been granted access to certain institutional data to fulfill their job or academic responsibilities. Each Data User must use data only for the purpose for which access was granted and must not share their access (e.g., passwords or accounts) with others. They are expected to understand and follow all guidelines for proper data handling – for instance, not downloading sensitive data to unencrypted personal devices, not emailing unencrypted PII, and respecting any data use agreements. If a Data User is unsure whether they are authorized to use a particular data set for a new purpose, it is their responsibility to seek clarification from the relevant Data Steward. Data Users must also promptly report any data they believe to be mis-classified (too open or too restricted) or any unauthorized data access they become aware of. By accepting access, Data Users acknowledge the obligation to protect the confidentiality, integrity, and privacy of the data.

Additionally, Information Technology (IT) Department staff play a support role in data access by maintaining identity management systems (such as single sign-on and directory services), auditing systems for access control effectiveness, and assisting in implementing technology for secure data sharing (e.g., secure file transfer services). The Office of Institutional Effectiveness/Research or similar units may be involved in brokering data access for reporting and analytics, ensuring such access complies with privacy rules and this policy.

Procedures or Requirements:

1. **Access Authorization Process**: Departments must follow a defined process to request access to institutional data or systems. Typically, a supervisor or department head will submit a request on behalf of a Data User, specifying the data or system and level of access needed. The request is routed to the appropriate Data Steward for approval. The Data Steward verifies the need-to-know and checks the data's classification to determine if additional approvals are required (for example, accessing confidential student data might also require FERPA training certification). Once approved, the Data Custodian (IT) provisions the access and confirms back to the requesting party. All approvals should be documented, and the principle of least privilege must be applied – e.g., granting read-only access if edit rights are not required. If a request is denied, the Data Steward will provide a reason. The requester may appeal a denial to the Data Trustee of that area, who will consult relevant policies and possibly the Data Governance Committee for a final decision.

2. **Secure Data Sharing Methods**: Whenever institutional data, especially sensitive or PII, needs to be shared between authorized users or transmitted outside the College, only approved secure methods should be used. The College provides certain tools for secure data sharing:

- *Shared Network Folders:* The IT Department can set up restricted-access network drives or SharePoint sites for departments or project teams. These shared folders are appropriate for collaborating on internal documents and can only be accessed by designated users with login authentication. Data Custodians ensure permissions on these folders are kept up to date.

- *Encrypted Email:* The College supports email encryption (e.g., using S/MIME or an email encryption gateway) for sending sensitive information. If a Data User must send PII or confidential data via email, they are required to use the College's encryption solution and follow guidelines (such as not putting PII in the subject line or body, but rather in password-protected attachments). The sender may need to coordinate with the recipient to exchange decryption information (such as a one-time passcode sent via text message).
- *Secure File Transfer and Document Management:* The College may utilize a secure document management system (such as Etrieve/SoftDocs or similar) to route and store documents containing sensitive data. These systems typically require user authentication and have audit trails for access. When sending large data files or reports, Data Users should use the College's approved secure file transfer service rather than email or personal cloud services.

All members of the College must refrain from using unapproved platforms (e.g., personal cloud storage, personal email) to share institutional data, especially if it is confidential or restricted. If there is a need for a new method of data sharing, it should be vetted and approved by the IT Department and Data Governance Committee.

3. **Data Usage Rules**: Access to data is granted for specific legitimate purposes, and any other use is prohibited. College personnel must access and use data only as required for the performance of their job functions, not for personal curiosity or gain. Data Users are categorized by their usage rights:

- *Update (Write) Access:* Only granted to users whose job duties require entering or modifying data (e.g., Registrar staff updating student records). This is tightly controlled and limited to avoid unauthorized data changes. Data Stewards grant update access based on roles, not individual preference, and ensure that users are properly trained.
- *Read-Only Access:* Most employees who need data for reference or decision-making will have view access. The College strives to grant read-only access widely when appropriate to empower employees, if such access does not risk privacy or security. Read-only access means the user cannot alter the data, only view, or download it.
- *External Data Dissemination:* Sharing institutional data with external parties—whether for regulatory reporting, research, accreditation, public relations, or any other purpose—must adhere to institutional, state, and federal guidelines, including FERPA and the College's External Data Reporting and Approval Policy.

    - Pre-Approval Requirement: All external dissemination of data must be reviewed and approved by the Office of Institutional Effectiveness (OIE) prior to release, regardless of format or audience. This includes reporting to agencies, external researchers, publishers, or the general public. No individual employee or department may release institutional data externally without OIE review, unless an explicit exemption has been granted.

- Data Classification and FERPA Compliance:
  Only data classified as Public or defined as Directory Information under the Family Educational Rights and Privacy Act (FERPA) may be released without individual consent. Even in these cases, the College reserves the right to restrict disclosure in alignment with individual privacy requests. Students may opt out of directory information sharing; such requests must be honored by all employees.

  Any data containing personally identifiable information (PII)—including academic records, financial details, or protected demographic information—must not be released externally unless:

  - Individual, informed consent has been obtained; or
  - A clear legal exception under FERPA permits disclosure (e.g., to authorized government officials, financial aid providers, or for health and safety emergencies).

  Any student-level data shared externally must be aggregated or de-identified, unless a valid FERPA exception applies, and OIE approval has been secured. The Data Steward(s) responsible for the data in question must also approve any such sharing when it involves non-public elements.

- Security and Access Protocols:
  As a matter of institutional and state best practices (e.g., modeled in part on WVBE Policy 4350), any external transfer of sensitive student data must follow secure data transfer protocols. Only authorized individuals should receive such data, and methods such as encryption must be used during transmission. Access to individual student records by parents or students is governed under FERPA and is managed solely through the Office of the Registrar—not through individual staff or faculty members.

4. **Data Classification Levels**: Pierpont C&TC utilizes a data classification scheme to categorize institutional data by sensitivity and to determine access control requirements. The classification levels, aligned with industry best practice definitions, are:

- *Public:* Data that may be freely disclosed to the public without risk. This includes information intended for public disclosure such as press releases, campus maps, directory information (as defined by FERPA, unless a student has opted out), and other public-facing information. Public data requires no special authorization to access, though the integrity of public data must still be protected (e.g., official published statistics should be accurate and released by authorized offices).
- *Internal*: Data meant for use within the College community that is not public but also not highly sensitive. Examples include internal memos, policies in draft, routine business records, or other information that the College prefers to keep within employees and students. Internal data should not be disclosed outside the College without permission, but access is generally open to members of the College who have a need.

- *Confidential*: Data that is sensitive and access is limited to specific groups or roles. This typically includes most FERPA-protected student education records, employee personnel records, non-public financial information, research data under confidentiality, and similar information. Confidential data should only be accessible to those in designated roles (e.g., an academic advisor can view their students' records, HR staff can view employee files). Unauthorized disclosure of confidential data could violate privacy laws, harm individuals, or the institution. Thus, it requires a higher level of security controls (login authentication, perhaps role-based security, etc.).
- *Restricted*: Data that is extremely sensitive, with very limited access on a strict need-to-know basis. This may include Social Security Numbers, health records covered by HIPAA, passwords or encryption keys, certain strategic plans or legal documents, and other information that, if breached, could lead to identity theft, legal liability, or significant harm. Restricted data often has additional safeguards such as encryption at rest, multi-factor authentication for access, and possibly dedicated secure environments. Only a few individuals (Data Trustees or specific designees) may have access to Restricted data, and any access or action on this data may be logged and reviewed.

Each Data Steward is responsible for classifying the data in their area into these categories. The classification must be documented (e.g., in the data inventory or next to each data element in the data dictionary). The classification then dictates handling requirements: for example, public data might be hosted on a public web server; Confidential data must be stored on secure servers and never in public repositories; Restricted data might be kept only in encrypted databases with very limited permissions. If there is uncertainty about classification, the Data Governance Committee can advise or modify definitions. Data classification will also inform how we respond to FOIA requests (Public data generally must be released if requested; Confidential/Restricted data likely falls under exemptions, such as FERPA or personal privacy exemptions in WV Code).

5. **Monitoring and Review**: Access logs and data usage may be monitored by IT and Data Stewards to ensure compliance. Systems that contain Confidential or Restricted data may have audit logging enabled to track who accessed what data and when. Periodically (at least annually), Data Stewards and Custodians should review user access lists for their systems (user accounts, group membership, report distribution lists) and remove or adjust access that is no longer needed. The College's Internal Audit or compliance office may conduct reviews of data access as part of broader audits. Findings from such reviews might include over-privileged accounts, unused accounts, or potential segregation of duties issues (e.g., someone who can both enter and approve a transaction) – these should be corrected under the guidance of Data Trustees.

6. **Consequences for Unauthorized Access or Misuse**: Any person who accesses data without proper authorization, or misuses data (for example, by exceeding their authorized access, sharing confidential data with unauthorized parties, or using data for personal gain or malice) is in violation of this policy. As soon as such an incident is identified, it should be reported as a security incident. The College will follow its incident response procedures, which may involve the IT security team and possibly law enforcement if laws are broken. Consequences may include immediate termination of access pending investigation, and, if confirmed, could lead to disciplinary action up to termination and legal action. The Consequence of Noncompliance with data usage rules is serious: violators may be subject to College conduct code penalties and even

civil or criminal penalties under laws like FERPA (which can lead to federal action). In less severe cases (e.g., accidental minor breaches), the College may require re-training and a reaffirmation of the individual's understanding of data policies, or temporarily suspend access.

Compliance and Enforcement:

Compliance with the Data Access Policy is mandatory for all individuals covered under the Scope. Pierpont C&TC will enforce this policy through oversight and technical controls. Data Custodians will implement system-enforced access controls that align with the policy, and any attempt to circumvent such controls (hacking, using another's credentials, etc.) is prohibited and subject to discipline. Data Stewards and supervisors are responsible for ensuring that their staff complete required training and follow procedures when requesting or using data access.

The College will utilize compliance checks, such as quarterly reviews of high-risk data access or reports from security tools that highlight policy violations (for instance, alerts if someone emails a file with Social Security numbers in plain text). Unannounced audits may be conducted on user activity for systems containing sensitive data to verify that usage aligns with job functions.

Enforcement actions for non-compliance with this policy can include:

- Revocation of access rights, either temporary or permanent, to prevent further unauthorized activity.
- Mandatory security or privacy training for those who violate guidelines unintentionally or due to lack of understanding.
- Disciplinary measures in accordance with College HR policies or student conduct codes. This might range from a written warning up to termination of employment or student expulsion, depending on severity and whether it is a repeat offense.
- Legal action or reporting to law enforcement in cases of unlawful data breaches. For example, willful disclosure of confidential student information without authorization could violate FERPA; the College would report such incidents to the U.S. Department of Education and could face sanctions, and the individual could face legal consequences. Similarly, computer misuse might violate state or federal computer crime laws.

Pierpont C&TC also acknowledges external compliance requirements. Under WV Code §18-2-5h, although targeting K-12, the spirit is that we must have transparency about data collected and robust security measures. We will therefore make available information on what types of student data we collect and why, ensuring our data practices can withstand public scrutiny. At the same time, the West Virginia Freedom of Information Act will be complied with by the College: any public records request for College data will be forwarded to the College's Office of Communications or Legal Counsel. They will work with Data Trustees to determine what can be released. Education records and confidential information will be withheld or redacted per FOIA exemptions (e.g., personal privacy exemption, FERPA-protected records). The College maintains a FOIA response registry as required by law (logging FOIA requests and responses).

If a data breach or incident occurs related to unauthorized access, enforcement will also mean executing the incident response plan – containing the incident, notifying affected individuals (for example, if a breach exposes student PII, we would notify those students in line with state policy which expects prompt notification to parents or students after a breach, and possibly notifying state authorities (the WV Attorney General or Governor's office, as applicable, for significant breaches as suggested in WV Code §18-2-5h for WVDE-level incidents). The College will take corrective actions post-incident, which are part of enforcement to prevent future violations.

Ultimately, every user's adherence to this policy is critical. By signing College employment or access agreements, users acknowledge their responsibility to follow this Data Access Policy. Willful or negligent non-compliance will be addressed firmly to protect the College's data assets and maintain trust with our students, employees, and other stakeholders.

Related Documents and References:

- Pierpont C&TC Data Governance Policy
- Pierpont C&TC Data Integrity Policy
- Family Educational Rights and Privacy Act (FERPA)
- WV Code §18-2-5h: Student Data Accessibility, Transparency and Accountability Act
- West Virginia Freedom of Information Act (WV FOIA), W. Va. Code 29B-1-1 et seq.
- WVDE Data Access and Management Guidance
- Pierpont C&TC Information Security Policy
- Pierpont C&TC Incident Response Plan
- WVBE Policy 4350

Tab

5

PIERPONT
COMMUNITY & TECHNICAL COLLEGE

Data Integrity Policy

Effective: June 2025

PURPOSE

The Data Integrity Policy is intended to ensure that Pierpont Community & Technical College's data is valid, reliable, consistent, and accurate across all systems and uses. The purpose of this policy is to uphold a high degree of integrity for the College's sensitive data so that faculty, staff, administrators, and decision-makers can trust the information for operational needs and strategic planning. By establishing standards for data definition, documentation, and quality control, and by clarifying responsibilities for maintaining data integrity, the College seeks to enable effective data integration across functional units and information systems. This policy also supports compliance with internal and external reporting requirements, ensuring that reports to state and federal agencies (and to the public) are based on consistent and correct data. Ultimately, the Data Integrity Policy helps protect the College's credibility and decision-making by preventing data errors and inconsistencies.

SCOPE

This policy applies to all institutional data defined in the Data Governance Policy and used by Pierpont C&TC. It covers all systems that store College data (student information systems, finance systems, learning management systems, etc.) and all personnel who enter, manage, or utilize data. The scope includes:

- **Data Entry and Capture:** How data is initially collected or input into College systems (e.g., admission forms, employee onboarding data, grade entry).
- **Data Maintenance:** Ongoing processes that update or modify data (e.g., changes to addresses, program curriculum updates, financial transaction entries).
- **Data Integration:** Transfer or synchronization of data between systems (e.g., syncing of student IDs between registration system and library system) and aggregation of data for reporting.
- **Data Reporting and Use:** Generation of reports, analytics, and decision-support information that rely on underlying data being consistent and well-defined.

All departments and units of the College are within scope, including any third parties or contractors who manage College data (such as a vendor managing a cloud-based system containing College records). If any data is shared with or reported to external entities (like the WV Community and Technical College System office, federal IPEDS reports, accreditation bodies), this policy ensures that such data has integrity from the point of origin. The policy particularly addresses "core data elements" that are used widely, such as student IDs, course codes, financial account codes, etc., because these must be consistent across all platforms. Note that while this policy focuses on accuracy and consistency (quality of data), issues of data confidentiality or access are covered in the Data Access Policy. However, some overlap exists (e.g., correcting a data error might involve access to correct it). In case of any conflict, data integrity should be maintained without violating access rules (meaning corrections should be done by authorized persons). This policy is aligned with **WVBE Policy 4350** and other guidelines to ensure that when we collect and maintain student data, we follow standardized definitions and procedures to keep that data accurate and meaningful.

POLICY

Policy Statement:

Pierpont C&TC asserts that institutional data must be consistently defined and understood, and that data values are to be correct and trustworthy. Data integrity refers to the accuracy, completeness, and reliability of data over its lifecycle. The College will establish and enforce standards such that key data elements have the same meaning across different departments and systems. For example, terms like “full-time student,” “faculty FTE,” or “operating expenditure” will have one official definition used College-wide for all reporting purposes. All College data systems should be designed and maintained to incorporate these standard definitions and acceptable value ranges. Each Data Steward is responsible for the correctness of data values within their area of responsibility, which means they must put in place processes to prevent and detect errors. The Information Technology department will support the integrity of data by ensuring technical consistency (such as referential integrity constraints in databases, removal of duplicate records, and accurate synchronization between systems). The IT Department will ensure that the needs of data users are considered when designing or modifying data structures, so that systems support correct and meaningful data capture. When institutional data is used for official reporting or decision-making, it must come from the authoritative sources defined by the College’s data governance framework (for example, official enrollment numbers should come from the student information system after census date to guarantee consistency). Any transformation or aggregation of data for reporting must preserve accuracy and be documented. In summary, College data will be consistently interpreted across all College systems according to best practices agreed upon by Data Stewards, with documented definitions and values. Where discrepancies or errors are discovered, the College is committed to correcting them at the source and communicating the corrections to all stakeholders who use that data.

Policies and Responsibilities:

Maintaining data integrity is a shared responsibility, but specific roles have the following duties:

- Data Trustee: Data Trustees have leadership responsibility for data integrity in their respective areas. They ensure that adequate resources and attention are given to data quality. This can include sponsoring data cleanup projects, approving data quality tools or software, and ensuring cross-department cooperation. Data Trustees work with Data Stewards to set priorities for improving data (for instance, deciding to standardize a particular data element College-wide). They also arbitrate any conflicts in data definitions or usage between departments. If external reporting issues arise (e.g., a state report uncovered inconsistent numbers), Data Trustees coordinate the response and remediation plan. They promote a culture that values accuracy over convenience – for example, encouraging staff to take the time to enter data correctly and to verify information. Data

Trustees may also be involved in approving any exceptions to data standards when a unique situation occurs.

- Data Steward: Data Stewards are the front-line managers of data integrity. For each key data element in their domain, they must ensure a clear definition exists and that it is used uniformly. They document these definitions and business rules in the College's data dictionary or metadata repository. Data Stewards establish procedures for data entry and maintenance that uphold integrity (for example, requiring dual review of critical data entries, or setting validation rules such as allowable value ranges for certain fields). They are responsible for conducting periodic data quality audits within their area – this might include running reports to find missing or anomalous values (like students without a birthdate on file, or courses with zero credits) and correcting them. Data Stewards also collaborate with one another for data that crosses functional areas; for instance, the Registrar (student data steward) and the Financial Aid Director (financial aid data steward) might coordinate to ensure that a student's enrollment status is consistently recorded for both academic and aid purposes. If Data Stewards identify systemic issues (e.g., a form is collecting data incorrectly, or users are misunderstanding a definition), they can recommend changes to processes or systems. It is ultimately the responsibility of each Data Steward to ensure the correctness of the data values for the elements within their charge, meaning they take ownership of data quality in their domain.

- Data Custodian: Data Custodians have technical responsibilities that significantly impact data integrity. They implement and maintain technical controls such as data validation rules in software, database constraints (like primary/foreign keys to enforce referential integrity between related records), and automated checks that prevent obviously bad data (for example, preventing an invalid date or an out-of-range value from being entered). Data Custodians performing data integrations between systems (such as importing data from one system to another) must ensure that mappings are correct and that no data is lost or mis-translated in the process. They should create or utilize scripts to identify duplicate records or inconsistencies (for example, two IDs for the same person) and work with Data Stewards to resolve them. Backups and disaster recovery plans are also within the purview of Data Custodians – while these are often seen as security measures, they are crucial for integrity, as they allow restoration of correct data in the event of data loss or corruption. Data Custodians must make sure that when systems are upgraded or patched, data integrity is preserved (e.g., by testing that reports still produce the same results after a system change). If a Data Custodian notices unusual data issues (like a sudden surge in errors or missing data fields), they should alert the Data Steward and investigate the root cause (which could be a technical glitch or a user process issue).

- Data User: All Data Users, especially those who enter or update data, play a vital role in maintaining integrity. They must follow the procedures and data standards provided to them – for example, using the proper format for names, entering data in the correct fields, and not bypassing required fields. Data Users should double-check their work when inputting critical data and are encouraged to ask for clarification if they encounter ambiguous cases. Just as important, Data Users are expected to be vigilant for potential errors or inconsistencies. If a Data User discovers what they believe to be incorrect data (such as a report that shows implausible numbers, or a student record that seems wrong), they should report it to the appropriate Data Steward or their supervisor. All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate Data Steward or the Data Trustee. This means Data Users have a responsibility not to ignore data issues; reporting and fixing small errors can prevent larger issues down the line. In addition, some Data Users (like analysts or report writers) may be tasked with combining data from multiple sources – they must do so using the official definitions and ensure they aren't inadvertently creating inconsistencies (for instance, by using unofficial data from a spreadsheet that conflicts with official system data).

Everyone in the College community must understand that data integrity is foundational – without accurate data, the analyses or decisions based on that data will be flawed. Therefore, each role from Trustees to end-users must perform their duties with care for data quality.

Procedures or Requirements:

To enforce data integrity, the College sets forth the following procedures and requirements:

1. Data Definition and Documentation (Metadata): The College will maintain a data dictionary or metadata repository for key institutional data elements. The Data Trustee (or a designated Data Steward) will oversee this repository. Each entry in the data dictionary will include: the data element name, a clear definition, the owner (Data Steward) responsible, the system of record (where it primarily resides), acceptable values or format, and any business rules (e.g., how it's derived, update frequency, and applicable date ranges). For example, an entry might define "Student Credit Hours" and specify how it's calculated and in what context (term, session) it's valid. This documentation should be available to all Data Users (at least those with relevant access) so they can consistently interpret the data. When new data elements are introduced (such as a new field in a system or a new report metric), they must be defined and added to the dictionary. Likewise, if any data element's definition is changed, the change must be approved by the Data Governance Committee and updated in the documentation. This practice aligns with the Student Data Accessibility and Transparency Act requirements for having a data inventory and definitions for elements, promoting transparency and clarity.

2. Data Input Controls: Departments must follow standardized procedures for entering and updating data. These procedures can include using official forms (physical or electronic) that have built-in validations, following an approval workflow for certain changes (e.g., grade changes might require approval, budget transfers might require dual authorization), and adhering to timelines (for instance, ensuring that all data for a semester is entered by a certain cutoff date for reporting). The IT systems will enforce many low-level validations (like not allowing letters in a numeric field, or requiring mandatory fields). Beyond that, Data Stewards should identify critical data fields that require extra verification. For example, when entering a new student record, an admissions officer might be required to verify the Social Security Number against existing records to avoid duplicates. Training will be provided to data entry personnel on common errors to avoid

and the importance of accuracy. In cases where data originates from an external source (like standardized test scores from a testing agency), procedures should ensure that the data is imported accurately and that any conversion or matching to internal records is done correctly (for instance, matching test scores to the right student).

3. Data Quality Monitoring: The College will implement routine data quality checks. These checks can be automated or manual. Examples include:
    - Data Audit Reports: Scheduled reports that look for anomalies, such as duplicate IDs, null values in fields that should always be populated, out-of-range values, or inconsistent data between systems (e.g., a student marked “graduated” in one system but still “active” in another).
    - Reconciliation Processes: Regular reconciliation between related systems. For instance, the Business Office and Financial Aid Office might reconcile financial records to ensure that student charges in the billing system match the records in the student information system. Similarly, HR data in the payroll system might be reconciled with data in a personnel system.
    - Key Performance Indicators (KPIs) for Data Quality: The Data Governance Committee may define metrics like “error rate in data entry” or “percentage of records with complete information” and monitor these over time. If a department has a high error rate, additional training or process changes can be implemented.

Data Stewards will review quality reports and coordinate data cleansing efforts when needed. Data cleansing might involve correcting data in bulk (with careful oversight) or one-by-one fixes for unique cases. Any systematic issues discovered (like a certain field frequently being left blank due to a form design problem) should be addressed by changing the process or system.

4. Change Management for Data Structures: When changes to data structures are proposed (such as adding a new field, changing a code value set, or redesigning a database), a change management process must be followed to ensure data integrity is maintained. This involves:
    - Impact Analysis: Assessing how the change will affect existing data and reports. For example, if a new student type code is introduced, how will it impact enrollment reports or downstream systems that consume that code?
    - Data Conversion or Migration: If data needs to be converted (e.g., splitting one field into two, or merging codes), a plan must be developed to transform the old data to the new structure without loss of meaning. Data Custodians would run conversion scripts or manual updates, and Data Stewards would verify a sample of records for correctness post-conversion.
    - Testing: Before changes go live, they should be tested in a non-production environment with real or realistic data to catch any issues. Key reports should be run to ensure they still work and produce expected results with the new changes.
    - Approval: Significant changes should be reviewed by the Data Governance Committee or at least the relevant Data Trustee and Steward to ensure the changes align with data standards. They must update the data dictionary if definitions or acceptable values change.

By managing changes carefully, the College prevents unintended data corruption or inconsistency that can occur when systems or business processes change.

5. Data Integration and System Alignment: The College will maintain a single logical data model or an enterprise architecture plan that maps how data in one system relates to data in another. Practically, this means identifying systems of record for each data domain (for instance, the HR system is the system of record for employee data, the Student Information System for student enrollment, etc.) and ensuring other systems either pull from those sources or update back to them. Interfaces and data feeds between systems should be timely and reliable. If multiple systems hold the same data element, one is designated authoritative and updates flow from it to the others. Data Custodians and Stewards should meet to discuss any discrepancies that arise between systems and correct them. The goal is that a data point (say a student's status or a faculty member's title) is the same in every system that uses it. This reduces confusion and errors when reports combine data. In support of the WV State data integration goals, our policy ensures that any data reported to the state or federal level is drawn from integrated, consistent sources so that, for example, enrollment numbers reported to the WV Higher Education Policy Commission match those in our internal reports and IPEDS submissions.

6. Issue Resolution and Continuous Improvement: When data issues are reported by Data Users or identified through audits, the College will address them systematically. Minor, isolated errors will be corrected by the responsible Data Steward or Data Custodian. For more widespread issues, a data integrity task force or the Data Governance Committee may form a project to clean and correct the data. The steps typically include identifying all affected records, determining the correct values (which may involve research and cross-checking sources), updating the data (preferably through controlled scripts or tools to avoid manual error), and confirming the fix. After resolution, the team should analyze why the issue occurred and implement safeguards to prevent it from recurring. For example, if a batch of student records had incorrect program codes due to a manual entry mistake, the solution might include adding a dropdown menu for that field to avoid typos. All employees are encouraged to provide suggestions to improve data processes, and these suggestions will be reviewed.

Additionally, incident response for data integrity overlaps with security incident response when data integrity is compromised maliciously (e.g., unauthorized alteration of records). In such cases, incident response procedures (like those in the Privacy Incident Response Plan) will be invoked to investigate and recover the correct data state, including restoring from backups if necessary. The College will ensure that breach planning and mitigation not only considers confidentiality but also the integrity and availability of data. If any data integrity issue rises to the level of impacting report accuracy externally (such as a published report with errors), the College will issue corrections and notify stakeholders as appropriate.

Compliance and Enforcements:

All College personnel and units must comply with the Data Integrity Policy. Given that data integrity lapses can be unintentional, the College's approach to enforcement emphasizes prevention and correction over punishment. However, willful neglect or manipulation of data will face strict consequences. For instance, knowingly falsifying data in a College record (such as altering a student's grade or misreporting financial figures) is a serious offense that could lead to disciplinary action including termination and referrals for academic or legal consequences as applicable.

Accountability: Data Stewards are accountable for monitoring compliance within their domains. If a department or user is repeatedly responsible for data errors, the Data Steward (with support from the Data Trustee) may require additional training or process changes in that department. Supervisors should treat data accuracy as part of job performance for employees who handle data extensively. The Office of Institutional Research or a similar body may periodically review data submissions for accuracy and report any concerns to Data Stewards and Trustees.

Auditing and Review: The College may conduct audits of data integrity, possibly in conjunction with internal audit or external auditors (for example, auditing the accuracy of data submitted in accreditation reports or financial statements). Any audit findings related to data inconsistencies must be addressed with a formal action plan. Data Trustees will ensure that these plans are executed, which might include data cleanup or improved controls.

Enforcement Actions: In the event of non-compliance that jeopardizes data integrity, several actions can be taken:

- If an individual is found to be careless or not following procedures (e.g., bypassing validations or ignoring the required process), their data access may be suspended until they are retrained. Persistent failure to follow data integrity procedures can lead to HR disciplinary processes.
- If a particular system or process is identified as a weak link (for example, a legacy system that cannot enforce needed rules), the College will prioritize it for upgrade or replacement. Interim measures (like extra manual checks) will be enforced.
- In cases of academic or research data, if integrity is compromised (for instance, a research dataset is mishandled), the incident might be referred to academic integrity or research compliance offices for additional review, given that it could overlap with research misconduct policies.

The College also aligns this policy with state and federal compliance requirements. For instance, the WV Student DATA Act implies routine compliance audits for privacy and security which can encompass data integrity checks as well. The College will include data integrity verification as part of ensuring FERPA compliance – e.g., verifying that data reported out under FERPA exceptions (like health/safety emergencies or studies) is accurate and goes to the right recipients. Under WVBE Policy 4350, educational institutions must maintain procedures for data quality when collecting and reporting student data; while Pierpont C&TC is a higher ed institution, we strive to meet similar standards by documenting how data is collected and ensuring it remains accurate through its use.

Incident Consequences: If poor data integrity leads to a significant incident (like incorrect data sent in an official report or a breach of data accuracy due to a security incident), the College will analyze the root cause and enforce any needed accountability. This might mean revising this policy, updating training, or in severe negligence cases, holding responsible parties accountable. A data breach that corrupts data (as opposed to exposing it) is still a breach; the College would follow the incident response plan to restore correct data and possibly involve law enforcement if malicious tampering occurred.

All employees and students are reminded that maintaining data integrity is part of our ethical responsibility. The College's Code of Conduct (or equivalent) covers honesty and accuracy in record-keeping. Therefore, compliance with this Data Integrity Policy is not just an IT or administrative requirement, but a fundamental part of each community member's duty. The College will enforce this through both technical means and community standards, ensuring that our institutional data can be relied upon with confidence.

Related Documents and References:

- Pierpont C&TC Data Governance Policy
- Pierpont C&TC Data Access Policy
- WV Code §18-2-5h (Student DATA Act)
- WV Board of Education Policy 4350
- Family Educational Rights and Privacy Act (FERPA)
- Institutional Data Dictionary/Metadata Repository
- WV Higher Education Privacy and Incident Response Plan

Tab

6

PIERPONT
COMMUNITY & TECHNICAL COLLEGE

Data Governance Policy

Effective: June 2025

PURPOSE

The Data Governance Policy establishes a framework for managing Pierpont Community & Technical College's institutional data as a strategic asset. Its purpose is to ensure that data is handled in a consistent, secure, and responsible manner. This policy promotes freedom of access to data by all members of the community while enforcing compliance with all applicable laws and regulations. By defining roles, responsibilities, and procedures for data governance, the College aims to enhance data quality, integrity, and availability for decision-making and operational efficiency.

SCOPE

This policy applies to all institutional data maintained by Pierpont C&TC, whether stored electronically or in paper format. It covers all College departments and units, and all employees, contractors, vendors, or agents, managing or using College data. Institutional data includes any information related to College operations (e.g., student records, employee data, financial and administrative data) that meets one or more of the following criteria: (1) data required for integration across systems or key to institutional processes; (2) data needed to meet internal or external reporting requirements; (3) data used in official College reports; or (4) data required by a broad cross-section of users. This policy is aligned with federal and state requirements, including the Family Educational Rights and Privacy Act (FERPA) and relevant West Virginia laws. In cases where other policies (e.g., IT security policies) overlap with data governance, all applicable policies shall be followed.

POLICY

Policy Statement:

Pierpont C&TC is committed to strategic and effective decision-making regarding its information assets through formal data governance. All institutional data will be managed according to defined standards of security, privacy, quality, and accessibility. The College adopts a philosophy that institutional data should be accessible to authorized individuals for legitimate educational and business purposes, coupled with a duty to protect sensitive information in compliance with FERPA and other privacy laws. Data governance decisions will be made transparently and documented appropriately. Every data element will be classified (e.g., Public, Internal, Confidential, Restricted) and given an appropriate security level by the responsible Data Steward. Data policies and procedures will be coordinated College-wide, ensuring consistent interpretation across systems and proper safeguards for data throughout its lifecycle. Any new systems or processes involving institutional data must adhere to this policy and receive approval through the data governance framework.

Roles and Responsibilities:

Effective data governance requires clearly defined roles. The following roles are responsible for implementing and enforcing this policy:

- **Data Trustee**: A senior College official accountable for oversight of data governance in their functional area. Data Trustees are responsible for the security, privacy, and quality of institutional data, and for ensuring compliance with data management policies and standards. They work with Information Technology, Institutional Effectiveness, and other stakeholders to allocate resources (staff, technology) to support data needs across the College. Data Trustees coordinate campus-wide data governance efforts, define the overall structure of data stewardship, and chair the Data Governance Committee or equivalent. They also promote data-informed decision making and ensure that critical data assets (student, financial, human resources data, etc.) have defined stewardship. Data Trustees make or approve strategic decisions about data policies and resolve conflicts or issues escalated by Data Stewards.
- **Data Steward**: A functional area manager or subject-matter expert assigned by a Data Trustee to oversee specific data sets or domains (e.g., student records, HR, finance, academic affairs). Data Stewards implement and enforce data policies and procedures within their area. They are responsible for classifying data elements under their care, defining data definitions, and ensuring data accuracy and consistency. Data Stewards approve or deny requests for access to data within their domain in accordance with this policy and FERPA guidelines. Their responsibilities include completing data governance and classification training, identifying all major data systems and repositories for their domain, and appointing Data Custodians for technical management. They must safeguard data from unauthorized access or alteration and authorize data use only for legitimate purposes. Data Stewards also meet regularly (for example, as a Data Governance Committee) to review data issues, coordinate data definitions, and plan for data needs across the College.
- **Data Custodian**: An IT or operations staff member (such as a database administrator, system administrator, or security officer) responsible for the technical environment and day-to-day management of institutional data systems. Data Custodians maintain systems housing institutional data and enforce access controls as specified by Data Stewards. Their duties include implementing backup and recovery procedures, monitoring system security, and applying data protection measures (encryption, user authentication, etc.). Data Custodians process authorized requests for adding, modifying, or removing user access, ensuring that access permissions align with the Data Steward's approvals. They document and uphold operational standards and procedures for data handling, and work with Data Stewards to update procedures as needed. In addition, Data Custodians are involved in technical aspects of data integrity, such as maintaining data integration between systems and preventing data loss or corruption.
- **Data User**: Any individual (faculty, staff, contractor, or other authorized agent) who accesses or uses institutional data to perform their job functions or academic responsibilities. Data Users are only granted access to the data necessary for their role ("need-to-know" basis) and must use data solely for official College business purposes. They are expected to understand and adhere to all relevant data policies, including privacy and security requirements. Data Users must protect any confidential information

they access and report any suspected data issues or incidents to the appropriate Data Custodian or Steward. They do not own the data they use; rather, they act as custodians of the information on behalf of the College and are accountable for using it ethically and legally.

All members of the College community have a shared responsibility to ensure data is handled properly. Information Technology (IT) personnel support the data governance process by providing the infrastructure and tools for secure data storage, sharing, and backup, and by assisting Data Trustees and Stewards in technical implementation of data standards. The Office of Institutional Effectiveness also plays a key role by facilitating data-informed decision-making, promoting data quality, and supporting institutional research efforts aligned with governance standards. If any questions arise regarding roles, the Data Trustee for the area or the College's executive leadership will clarify responsibilities.

Procedures or Requirements:

Data Governance Structure: Pierpont C&TC will maintain a Data Governance Committee or similar committee comprised of Data Trustees and Data Stewards from key functional areas (e.g., academics, student services, finance, IT, human resources). This committee will meet regularly (e.g., monthly) to discuss data-related issues, approve data standards, and review compliance with data policies. Meeting agendas and decisions will be documented. The committee is responsible for reviewing any new institutional data collections or proposed changes to data systems to ensure alignment with governance standards.

Data Classification: As part of governance procedures, every institutional data element must be assigned a classification level by the relevant Data Steward, in line with the College's Data Access Policy. The categories generally include Public, Internal, Confidential, and Restricted, as defined in the Data Access Policy (see Related Documents). Classification determines the security controls and access permissions required for that data. Data Stewards should maintain an inventory or data dictionary of the data elements under their purview, including definitions and classification of each element. In accordance with West Virginia's Student DATA Act principles, the College will document data elements and their purposes, and make publicly available a high-level inventory of the types of student and institutional data collected, where appropriate. This inventory will not include any sensitive personally identifiable information but will improve transparency of our data practices.

Data Standards and Quality: Data Stewards, in consultation with Data Trustees, will define standards for data entry, naming conventions, and metadata for their areas to ensure consistency across systems. Key data elements that are shared across multiple systems (for example, student ID numbers, course codes, employee IDs) must be consistent and synchronized. The College will maintain a central repository of metadata (data about data) for core institutional data. This metadata will include technical definitions, valid values, and business rules for each data element. For example, if "full-time enrollment" is a data element, the repository would describe how it's calculated, the term definitions, and any timing considerations (such as census dates). Adhering to these standards is mandatory; any changes to core data definitions must be reviewed by the Data Governance Committee.

Access and Authorization Procedures: All requests for access to institutional data (beyond what a user is automatically granted by virtue of their role) must follow formal procedures. Typically, a Data User's supervisor or department head will request access for the user to specific systems or reports. The appropriate Data Steward will review the request to ensure it aligns with the user's job responsibilities and the data's classification. Approved requests are then implemented by Data Custodians, who will grant the minimum necessary access privileges. Data Trustees and Stewards will periodically review user access lists to verify that access remains appropriate and revoke any access that is no longer needed (for example, when an employee changes roles or leaves the College). If a Data Steward denies a request for access, that decision can be appealed to the Data Trustee or the Data Governance Committee for further review.

Training and Awareness: All individuals with roles in data governance (Trustees, Stewards, Custodians, and Users) must undergo training relevant to their responsibilities. Data Trustees and Stewards should receive training in data stewardship, classification, FERPA compliance, and relevant privacy/security laws. Data Users must receive basic training on data security, privacy, and proper data usage. The College will also provide periodic awareness programs about data governance policies, updates on any changes in laws (such as FERPA regulations or state privacy laws), and guidance on ethical data practices. Compliance with training requirements is considered part of each role's duties.

Incident Reporting and Response: In the event of any suspected or actual data breach, unauthorized disclosure, or significant data error, it must be reported immediately to the appropriate authority (e.g., the IT security office, Data Custodian, or Data Trustee). The College will follow the West Virginia Higher Education Policy Commission's Privacy Management and Incident Response Plan, which provides procedures for containing and managing data breaches. This includes classifying the incident, notifying affected parties in accordance with state law, and mitigating any damage. Under West Virginia's Student Data Act, the College is mindful of the expectation to notify authorities and individuals of breaches involving personally identifiable information. Pierpont C&TC will ensure timely notification to affected students or employees if their confidential data is compromised, consistent with state and federal guidelines. After an incident, the Data Governance Committee will review the incident to identify lessons learned and recommend improvements to policies or practices to prevent future occurrences.

Compliance and Enforcement:

All College community members must comply with the Data Governance Policy. Failure to adhere to this policy may result in disciplinary action as per College procedures or employment agreements. Specifically, employees or students who violate data governance standards – for example, by accessing data without authorization, mishandling sensitive information, or failing to follow required procedures – will be subject to investigation. Minor or inadvertent violations may be addressed through remedial training and temporary suspension of access; serious or willful non-compliance can result in formal discipline up to termination of employment or dismissal from the College and may carry legal consequences if laws (such as FERPA or data protection laws) are violated. Data Trustees are responsible for overseeing compliance in their areas and ensuring that any compliance issues are corrected. The College's executive leadership (or a designated compliance officer) may conduct periodic audits or reviews of data handling practices to ensure this policy is followed.

The College also recognizes the West Virginia Freedom of Information Act (WV FOIA) as a legal framework governing public access to records. While many educational records are protected by privacy laws and thus exempt from disclosure, the College will respond to FOIA requests in compliance with W. Va. Code §29B-1-1 et seq., ensuring that any release of records is reviewed by the appropriate Data Trustee and the College's legal counsel. Public records (as defined by law) will be provided upon valid request, whereas confidential student or personnel data will be withheld or redacted according to legal exemptions (e.g., FERPA-protected information). Any willful violation of FOIA or wrongful withholding of public records can result in penalties, so the College will balance transparency with privacy compliance diligently.

Adherence to this policy will be enforced by the Data Governance Committee and the College administration. Enforcement mechanisms include requiring remediation plans for units found non-compliant, removing, or limiting access for individuals until compliance is assured, and reporting serious breaches to senior administration or regulators as required. All College personnel are expected to report any suspected violations of this policy to their supervisor, a Data Steward, or anonymously through any established ethics or compliance reporting structure. Reports of non-compliance will be reviewed confidentially and without retaliation.

Related Documents and References:

- Pierpont C&TC Data Access Policy
- Pierpont C&TC Data Integrity Policy
- Family Educational Rights and Privacy Act (FERPA)
- West Virginia Freedom of Information Act, W. Va. Code §29B-1-1 et seq.
- WV Code §18-2-5h: Student Data Accessibility, Transparency and Accountability Act
- WV Board of Education Policy 4350
- WV Higher Education Policy Commission – Privacy Management and Incident Response Plan
- WVDE Data Access and Management Guidance

Tab

7

PIERPONT
COMMUNITY & TECHNICAL COLLEGE

External Data Reporting and Approval Policy

Effective: June 2025

PURPOSE

The purpose of this policy is to ensure the accuracy, consistency, and integrity of all data reported to external parties by the College. By requiring review and approval of data by the Office of Institutional Effectiveness (OIE) prior to release, the College can maintain a single source of truth for institutional data. This policy supports compliance with accreditation standards and government regulations and protects the College's reputation by preventing the dissemination of incorrect or conflicting information.

SCOPE

This policy applies to all departments, faculty, staff, and units of the College, without exception unless a specific exemption is granted as described below. It covers any data values or statistical information prepared for audiences outside the College, regardless of the medium of communication. This includes, but is not limited to:

- Official reports to government agencies (federal or state reports, regulatory submissions, IPEDS data, etc.).
- Accreditation materials and reports to accrediting bodies or professional licensing organizations.
- Public relations and marketing content (press releases, brochures, website content, social media posts, presentations) that contain numerical data or institutional statistics.
- Surveys and questionnaires from external organizations (ranking surveys, research studies, media inquiries) where institutional data is provided.

For the purposes of this policy, "external reporting" means any information sharing where the intended audience includes individuals or organizations outside of the College. If there is any uncertainty about whether data will be considered external, employees should err on the side of caution and seek OIE review.

Exemptions: In rare cases, a specific department and the OIE may jointly grant a written exemption for certain data or reports. Such an exemption must be agreed upon by both the Office of Institutional Effectiveness and the relevant department head and must clearly outline the scope of data covered. Exemptions are expected to be minimal and are typically granted only when alternative review processes are in place that satisfy the intent of this policy. Unless an explicit exemption has been approved in writing by both parties, this policy remains applicable.

POLICY

Policy Statement:

All data values intended for external reporting must be reviewed and approved by the Office of Institutional Effectiveness (OIE) prior to release. No faculty member, staff member, or department shall disseminate institutional data externally without obtaining approval from OIE. This requirement covers every instance of sharing quantitative information such as enrollment figures, graduation rates, performance metrics, survey results, or any other statistical data about the College.

Under this policy, the OIE serves as the authoritative source for official institutional data. The OIE is responsible for verifying that data are accurate, up-to-date, and consistent with official records and definitions. Only data that has been vetted and approved by OIE may be considered official and ready for external use. This ensures that the College "speaks with one voice" regarding institutional data, thereby avoiding confusion or misrepresentation that could arise from multiple sources reporting similar information. Any discrepancies identified by OIE during the review process must be resolved before the data can be released outside the College.

Non-numerical information (qualitative descriptions, general statements) typically does not fall under this policy unless it includes or is based on specific data values. However, all members of the College community are encouraged to consult OIE when in doubt about any information planned for external distribution. Adhering to this policy is mandatory and is a condition of employment and departmental operation within the College.

Roles and Responsibilities:

Office of Institutional Effectiveness (OIE): The OIE is charged with overseeing the implementation of this policy. Key responsibilities of OIE include:

- **Data Verification and Approval:** Review all proposed external data submissions for accuracy and consistency with official college records. Approve data for release or provide corrected figures if necessary.
- **Official Data Source Maintenance:** Maintain the official institutional databases and reference documents (e.g., enrollment statistics, retention and graduation rates, faculty/staff data, program outcomes) that serve as the source for external reports.
- **Guidance and Training:** Offer guidance to departments and individuals on data definitions, reporting standards, and proper procedures for requesting data. Provide training or resources as needed to ensure compliance (for example, training on how to request data or common data definitions used in reports).
- **Record-Keeping:** Keep a record of data requests and approvals. Document what data was reviewed and the date of approval. Retain copies of approved datasets or reports for accountability and future reference.
- **Periodic Review:** Periodically review the policy's effectiveness and update procedures in collaboration with college leadership. OIE may also perform audits or spot-checks of externally released information to ensure ongoing compliance.

Department Heads and Supervisors: Leaders of each department or unit are responsible for enforcing this policy within their areas. Their responsibilities include:

- **Communication:** Ensuring that all employees (faculty and staff) in their department are aware of and understand this policy. New employees should be informed of this requirement during onboarding.
- **Internal Oversight:** Establishing internal processes so that any data prepared for external use by members of the department is routed to OIE for review. This may involve creating an internal checkpoint or requiring departmental approval before OIE submission.
- **Coordination with OIE:** Acting as a liaison between their department and OIE when needed. For complex data requests or large reports, department heads should coordinate early with OIE to schedule sufficient review time.
- **Enforcing Compliance:** Addressing any instances of non-compliance within the department. If a staff or faculty member in the department releases data without approval, the department head should take corrective action in line with this policy and in consultation with OIE and Human Resources if necessary.

Faculty and Staff (All Employees): Every employee of the College has a responsibility to uphold this policy. Specific duties for individuals include:

- **Prior Approval:** Before sharing any institutional data externally (even informally, such as in response to an email inquiry from outside, or a presentation at a conference that will be publicly available), employees must ensure the data has been approved by OIE. If the data or report is new, it is the employee's responsibility to submit it to OIE for review **well in advance** of the intended release date.
- **Use of Official Data:** Wherever possible, use data provided directly by OIE or data from official publications released by OIE (such as an annual fact book or official statistics on the College website) for external reporting. Do not rely on personal compilations or unofficial sources for official reporting.
- **Complete and Accurate Submission:** When requesting OIE review, provide all relevant information about the data, including context, definitions, and sources used. For example, clarify the time period covered, population definitions (e.g., "first-time full-time students entering Fall 2024"), and any calculations or methodology. This helps OIE verify the data correctly.
- **External Requests Handling:** If an employee is directly approached by an external entity (e.g. a survey firm, news reporter, or government agency) requesting data, the employee should **not** provide the data immediately. Instead, they should either redirect the inquiry to OIE or gather the requested information and submit it to OIE for approval before responding. It is acceptable to tell the requester that "I will confirm these figures with our Office of Institutional Effectiveness and get back to you."
- **Confidentiality and Data Security:** While this policy is about accuracy in external reporting, employees must also maintain confidentiality and data privacy as required by other policies (e.g., FERPA for student data). Only non-confidential aggregate data should ever be considered for external release, and OIE will also ensure that no sensitive personal data is being inappropriately disclosed.

Executive Leadership: The college's executive leaders (President, Vice Presidents) support this policy by reinforcing its importance and ensuring adequate resources for OIE to fulfill its role. They are also involved in enforcement actions if policy violations need escalation. For instance, a Vice President or the President may issue formal communications or directives in cases of serious non-compliance to underline the institutional commitment to data integrity.

Procedures:

All College personnel must follow these procedures when preparing data for external release:

1. **Identify Need for External Data:** When a department or individual determines that data needs to be shared outside the College (for example, completing an external survey, drafting a grant proposal with institutional data, or creating a marketing brochure with statistics), they should plan for OIE review as early as possible. Ideally, notify OIE of the need as soon as it is identified, especially if there are deadlines imposed by the external party.
2. **Submit Data or Request to OIE:** The responsible employee (or department) compiles the data intended for external use and submits it to OIE for review. If the data is not already compiled, the employee should submit a **data request** to OIE outlining what information is needed. Submissions to OIE should include:
   - A clear description of each data element (e.g., "total fall 2025 enrollment, including full-time and part-time students").
   - The source of any preliminary data the department has (e.g., internal database, survey results).
   - The context or purpose of the data use (who will receive it and how it will be used externally).
   - The deadline by which the approved data is needed to meet external requirements.
3. **OIE Review Process:** Upon receiving the data or request, OIE will verify the accuracy and consistency of the information:
   - OIE will cross-check figures against official records (student information systems, HR records, finance systems, or other authoritative data sources as appropriate).
   - If data definitions or calculations are involved, OIE will ensure they align with standard institutional definitions or, if it's for a specific survey, align with the definitions provided by that survey.
   - OIE may contact the requester for clarification or additional information during this review to resolve any discrepancies or questions.
4. **Revision and Clarification (if needed):** If OIE finds that the submitted data contains errors, is outdated, or uses non-standard definitions, OIE will correct the data or advise on necessary revisions. OIE will communicate any changes to the requester and explain the reasons (for instance, "updated graduation rate to 55% to include the latest fall cohort, which differs from the 50% initially provided").
5. **Approval:** Once OIE is satisfied that the data is accurate and compliant with official definitions, OIE will formally approve the data for external release. Approval may be communicated via an official email, a signed form, or a documented note on the request. The approval will explicitly list the data values that are approved, and if appropriate,

attach the finalized dataset or report. **Only after receiving this approval may the data be released externally.**

6. **Release of Data to External Party:** The department or individual may then proceed to transmit or publish the data to the external party or platform, using the OIE-approved figures exactly as provided. No substitutions or modifications should be made to the data post-approval without further consultation with OIE. If the external party has follow-up questions or requests for additional data not covered in the original approval, those additional data points must also undergo review (return to step 2 for new data).
7. **Documentation and Archiving:** The OIE will record that the data was reviewed and approved, including what was approved and when. The requesting department is encouraged to keep a copy of the OIE approval (such as saving the approval email or form) and the final data submitted externally. This documentation can be important for future reference, especially if questions arise later about what was reported.
8. **Timeline Considerations:** Employees should allow sufficient time for the OIE review process. Typically, a minimum of **5–7 business days** advance notice is recommended for standard data requests. Larger or more complex data reports (such as major accreditation self-study data or comprehensive surveys) may require more lead time (several weeks). OIE will make efforts to accommodate urgent requests, but last-minute submissions risk being delayed or not approved in time, which could jeopardize the external reporting deadline. It is the responsibility of the requester to plan accordingly and engage OIE early in the process.
9. **Emergency or Expedited Cases:** In exceptional situations where data must be released immediately (e.g., an urgent request from a government agency with a 24-hour turnaround), the requester must still notify OIE. OIE will attempt to expedite the review. If OIE is unable to formally approve due to time constraints, at minimum an **verbal or email clearance** should be obtained from the Director of OIE or a designated representative before releasing the data. Such cases should be followed up with a full review after the fact to ensure the data released was indeed accurate.
10. **Exemption Procedure:** For any instance in which a department believes an exemption to this policy is justified (for example, a specialized research unit that regularly reports data to a federal research body under its own quality controls), the department head should submit a written request to the OIE outlining the rationale for exemption. The OIE will evaluate the request and, if it agrees, will document the terms of the exemption jointly with the department. Even with an exemption, the department might still be required to provide periodic reports to OIE to ensure consistency. All exemptions must be reviewed at least annually to determine if they remain warranted.
11. **External Data Requests Routing:** The College may establish a standard point-of-contact for external data requests (for example, instructing external parties on the College website to direct data inquiries to the OIE's email). Employees who often receive external questions can refer requesters to that contact. This helps streamline the process and ensures OIE is aware of all outgoing data. OIE will coordinate with relevant departments to fulfill such requests.

By following these procedures, the College ensures that data released to external audiences is accurate, consistent, and approved, thereby upholding the integrity and credibility of the institution's communications.

Enforcement:

Ensuring compliance with this policy is critical. All employees and units are expected to adhere to the requirements outlined above. **Non-compliance** with the External Data Reporting and Approval Policy will be taken seriously and may result in corrective actions or disciplinary measures. Enforcement of this policy will be carried out as follows:

- **Monitoring and Audit:** The OIE, in collaboration with College leadership, may monitor external communications and reports for compliance. This can include reviewing copies of reports submitted to external agencies or scanning public releases for data that should have been approved. If unapproved data releases are discovered, the responsible department or individual will be contacted for an explanation.
- **Correction and Retraction:** If data is released externally without OIE approval or if incorrect data is released, the first priority is to correct the information. The responsible individual or department, in coordination with OIE, must **immediately notify the external entity** that received the data and issue a correction or retraction. For example, if an incorrect statistic was published in a press release or report, a corrected version must be sent out as soon as possible. The College may also post corrections on its own platforms if needed (such as issuing an updated press release or footnote on the website).
- **Formal Warning:** The employee(s) and their supervisor may receive a **formal written warning** for failing to follow this policy. This warning will be documented in the individual's personnel file. The warning will outline the nature of the violation (e.g., "Released enrollment figures to media without OIE approval on [date]") and reiterate the expectations moving forward. In the case of faculty, such warnings may also be copied to the academic dean or relevant vice president.
- **Mandatory Training:** In some cases, the College may require the person or department in violation to undergo additional training. This might involve a refresher session with OIE on data reporting procedures or an online training module on data governance. The goal is to prevent future incidents by ensuring a full understanding of the policy.
- **Restrictions on Future Communication:** An individual or department that violates the policy may be subject to **heightened oversight** for future external communications. For instance, a department could be required to route *all* external communications (even those without data) through a supervisor or the Public Relations office for a certain period. An individual might lose the privilege of responding to external data requests directly; instead, any inquiry they receive must be forwarded to OIE or their supervisor. These restrictions would typically be temporary and reviewed after a period (e.g., after one year of compliance, the restrictions might be lifted).
- **Repeated or Egregious Violations:** If a person or department repeatedly fails to comply with this policy, or if a single violation is deemed especially serious (for example, willfully providing false data externally, or causing significant reputational or legal harm to the College), the matter will be escalated. Consequences can include:
    - Reporting the issue to the appropriate Vice President or the President's Office.
    - Disciplinary action in accordance with the College's human resources policies, which could range from additional reprimands up to and including termination of employment in severe cases.

  - Removal of certain responsibilities from a staff member (e.g., they may be barred from handling data or participating in external reporting projects).
  - If the violation involves academic departments, it may affect considerations in performance evaluations or leadership appointments.
- **Accountability and Review:** All enforcement actions taken will be documented by OIE and, where applicable, by Human Resources. The College's Policy Committee or similar governing body may review cases of non-compliance to determine if further changes to procedures or additional safeguards are needed. On an annual or biennial basis, OIE will report summary information (without personal identifiers) to senior leadership on the number of approvals processed and any compliance issues encountered, to ensure transparency and improvement of the process.

The College is committed to a culture of data integrity and accountability. Enforcement of this policy is not intended to be punitive, but rather to underscore the importance of accurate data reporting and to remedy issues before they can compromise the College's obligations or reputation. By following this policy and cooperating with OIE for all external data reporting, employees help protect both themselves and the College from the consequences of misinformation. All members of the College community share in the responsibility to uphold these standards and will be held accountable for their role in maintaining the integrity of external data communications.