2.2.19 Data Handling Policy

Policy approved by the Board of Trustees – October 28, 2020

Purpose

The purpose of this document is to provide guidance for protecting college information resources from unauthorized access or disclosure. The goal is to assure that every member of the Westmoreland County Community College (Westmoreland) community can identify non-public data and follow appropriate security precautions to protect the data and to avoid compromising the privacy rights of others or Westmoreland's institutional rights or obligations.

Scope

This policy applies to Westmoreland staff, faculty, students, associates, affiliates, contractors, volunteers, or visitors accessing college owned or managed data, in physical or electronic format.

Contacts

Direct questions about this policy to your area's Security Liaison or Data Governance leaders.

Data Classification Levels

Every member of the Westmoreland community should be able to identify the appropriate classification level of any data they are accessing or maintaining in electronic or physical form.

Data classification levels range from Level 0 (public) to Level 3 (highly restricted). **Any data other than Level 0 data is considered to be non-public data unless such data is required to be made available to the public by application of the Pennsylvania Right to Know Act (RTK).**

The four classification levels are:

Level 0—Public

- College data that is purposefully made available to the public.
- Disclosure of Level 0 data requires no authorization and may be freely disseminated without potential harm to the college.

Level 1 - Internal

- College owned or managed data that includes information that is not openly shared with the general public but is not specifically required to be protected by statute or regulation.
- Unauthorized disclosure would not result in direct financial loss or any legal, contractual, or regulatory violations, but might otherwise adversely impact the college, individuals, or affiliates.

- Level 1 data is intended for use by a designated workgroup, department, or group of individuals within the college.

Note: While some forms of internal data can be made available to the public, the data is not freely disseminated without appropriate authorization.

Level 2 - Confidential/Sensitive

- College owned or managed data that is confidential business or personal information for which unauthorized disclosure could have a serious adverse impact on the college, individuals or affiliates.
- Level 2 data is intended for a very specific use and should not be disclosed except to those who have explicit authorization to review such data.
- There are often general statutory, regulatory or contractual requirements that require protection of the data.
- Regulations and laws that affect data in Level 2 include, but are not limited to, RTK the Family Educational Rights & Privacy Act (FERPA) and the Graham-Leach-Bliley Act (GLBA).

Level 3 - Highly Restricted

- College owned or managed data that is highly restricted business or personal information, for which unauthorized disclosure would result in significant financial loss to the college, impair its ability to conduct business, or result in a violation of contractual agreements or federal or state laws or regulations.
- Level 3 data is intended for very limited use and must not be disclosed except to those who have explicit authorization to view or use the data.
- There are often governing statutes, regulations, standards, or agreements with specific provisions that dictate how this type of data must be protected.
- Regulations and laws that affect Level 3 data include, but are not limited to, RTK, FERPA, Pennsylvania Personnel Records Inspection Act, the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Guidelines for Appropriate Data Handling

Whether data is downloaded from a system or application within Westmoreland's protected infrastructure or acquired by some other means, individuals must ensure that the security of the data is protected appropriate to the level of its classification. Data must also be retained in accordance with the Westmoreland College Record Retention Policy.

Level 3 Data

Due to its restricted nature, Level 3 data requires special handling. Some divisions/departments may handle Level 3 data as part of their business processes; however, that data should not be exported or stored outside of its secured location without express permission of the Data Governance Council.

Note: A limited number of enterprise applications such as an ERP (Enterprise Resource Planning) system or CMS (Content Management System) hold highly restricted Level 3 data. Access to this data is tightly controlled via specific permissions and management authorization. If unsure whether your business data may be stored in one of these systems, discuss it with a Security Liaison or Data Governance leaders.

Research Data

Research data is typically highly sensitive in nature or subject to special contractual requirements and its handling should be coordinated through the college's Institutional Review Board (IRB).

Related Resources

- Data Governance Organizational Chart
- Institutional Review Board (IRB) FAQ
- Westmoreland's Directory Information
- Westmoreland's Record Retention Policy