Baldwin Wallace University Information Technology Standard

Issued by:	**Information Technology**
Title:	**Data Classification**
Number:	**ITS-BW-04-01**
Publish date:	**June 1, 2022**

Baldwin Wallace University is hereinafter referred to as "BW".

The BW Data Classification Standard is a framework for assessing data sensitivity, measured by the adverse business impact a breach of the data would have upon the campus. This standard provides the foundation for establishing protection profile requirements for each class of data.

The BW Data Classification Standard covers BW campus data. BW campus data is information prepared, managed, used, or retained by an operating unit or employee of BW relating to the activities or operations of the University. BW campus data does not include individually-owned data, which is defined as an individual's personal information that is not related to University business. Data classification does not alter public information access requirements. Ohio Public Records Laws or federal Freedom of Information Act requests and other legal obligations may require disclosure or release of information from any category.

A. Business Considerations and Impact

Evaluating potential business considerations and impact on the campus due to loss of data confidentiality or integrity include but is not limited to:

- Loss of critical campus operations
- Negative financial impact (money lost, lost opportunities, the value of the data)
- Damage to the reputation of the campus
- Potential for regulatory or legal action
- The requirement for corrective actions or repairs
- Violation of University or campus mission, policy, or principles
- Loss of availability of critical campus systems
- Establishing and maintaining the confidentiality and integrity of student records

Additionally, BW is subject to many regulatory requirements that must also be considered when classifying data. These regulations include:

- HIPAA (Med Center and Athletic Medicine)
- PCI-DSS (Point of sale, bursars office)
- FERPA (Colleague, Enrollment, online directories, trusted partners)
- FTC's Red Flag Rules
- SOC 2, GLBA (Giving programs, Financial Aid)
- State of Ohio Laws: Title XXXIII ORC 3319.321(B)

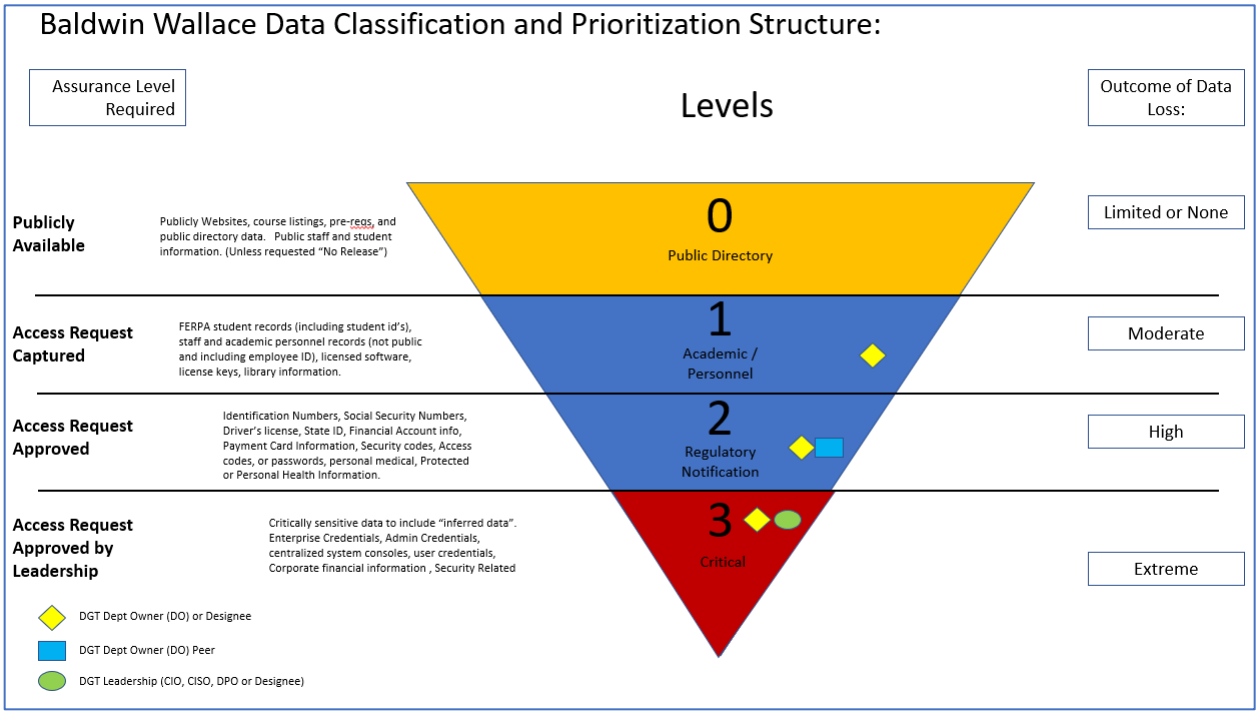
B. Data Classification Table

The following table classifies data at BW according to importance and impact:

Class	Business Impact:	Examples of Data to include but are not limited to:
Protection Level 0 Public Directory Information	Limited or none	Information intended for public access, e.g.: • Public directory information • Public websites • Course listings and pre-requisites
Protection Level 1 Academic Related Personnel and Student Records	Moderate	Information intended for release only on a need-to-know basis, including personal information not otherwise classified as Level 0, 2, or 3, and data protected or restricted by contract, grant, or other agreement terms and conditions, e.g.: • **FERPA** student records (including Student ID) • Staff and academic personnel records (including Employee ID) • Licensed software/software license keys • Library paid electronic subscription resources
Protection Level 2 Regulatory Requirement for Notification	High	Data or information with a legal requirement for notification to affected parties in case of a confidentiality breach:(See Appendix A.II Legal Requirements for Notification for more information) • Full name (if not common) • Home address • Email address (if private from an association/club membership, etc.) • National identification number • Passport number • An IP address (when linked, but not PII by itself in the US) • Vehicle registration plate number • Driver's license number • Face, fingerprints, or handwriting • Credit card numbers • Digital identity • Date of birth • Birthplace • Genetic information • Telephone number • Login name, screen name, nickname, or handle • Social security number • Driver's license number, California identification number • Financial account numbers, credit or debit card numbers and financial account security codes, access codes, or passwords • Personal medical information • Personal health insurance information For International students applicability to General Data Protection Standards apply to any information collected by the various departments at BW: • Basic identity information such as name, address, and ID numbers (Passport ID/copy, Citizenship documents)

		• Web data such as location, IP address, cookie data, and RFID tags • Health and genetic data • Biometric data • Racial or ethnic data • Political opinions • Sexual orientation • Grades and related scores (TOEFL Score) • Financial related information (list of these required such as International financial statement)
Protection Level 3 Critical Data or "Inferred Data"	Extreme	Data or information that creates "Inferred Data" (See Appendix A) risk between multiple sensitive systems, e.g., enterprise credential stores, backup data systems, and central system management consoles.

C. Data Classification Requirements



Level 0: Public Directory Information

1) "**Non-Personal" Academic Personnel** Information:
   - Name
   - Date of hire or separation
   - Current position title
   - Organizational unit assignment including office address and telephone number
   - Full-time, part-time, or other employment status
2) **Staff personnel records are** designated as "public information".

- Name
- Date of hire
- Current position title
- Organizational unit assignment
- Date of separation
- Office address and office telephone number
- Current job description
- Full-time or part-time, and appointment type

3) **Student Directory Information, <u>unless the student has requested that information about them not be released as public information</u>:**
   - Name of student
   - Telephone, e-mail
   - Dates of attendance
   - Number of course units in which enrolled
   - Class level
   - Major field of study
   - The last school attended
   - Degrees and honors received
   - Participation in official student activities
   - Name/weight/height (intercollegiate athletic team members only)

   Access Control(s): to this data requires
   a) **A documented request via Data Governance Request Form (if needed)**
   b) **Review by the assigned Data Governance Team Departmental Owner**

Level 1: Academic Related Personnel and Student Records

1) **Student records** include, but are not limited to:
   a) FERPA student records (including Student ID)
   b) Staff and academic personnel records (including Employee ID)
   c) Licensed software/software license keys
      - Library paid electronic subscription resources
      - Transcripts (grades)
      - Exam papers
      - Test scores
      - Evaluations
      - Financial aid records
      - Loan collection records
      - Directory information for students who have requested that information about them not be released as public information

   d) See Appendix A.II Legal Requirements for Notification section above for the list of protection level 2 data, which also applies to student data. See the Student Directory Data section under Public Directory Information below for the list of protection level 0 student data.
   e) **Access Control(s):** Access to this data requires:
      i) **Completed Data Governance Request Form**
      ii) **Submitted to, and reviewed/approved by the appropriate Department DGT Owner**
      iii) **With an additional DGT Peer Check by one or more of the DGT members.**
      iv) **Completed Level 1 DGT Requests shall be archived and audited periodically by the DGT.**

2) Level 1: Personnel Records
   c) **Academic Personnel Records** include, but are not limited to:
      - Confidential academic review records
      - Non-confidential academic review records
      - "Personal" information.

   d) Staff Personnel Records include, but are not limited to:

- Home telephone number and home address
- Spouse's or other relatives names
- Birthdate
- Citizenship
- Income tax withholdings
- Information relating to the evaluation of performance
- Any information relative to pay and/or compensation

e) See Appendix A.II Legal Requirements for Notifications section above for the list of protection level 2 data, which also applies to student data. See the Student Directory Data section under Public Directory Information below for the list of protection level 0 student data.

f) **Access Control(s):** Access to this data requires:
   i) **Completed Data Governance Request Form**
   ii) **Submitted to, and reviewed/approved by the appropriate Department DGT Owner**
   iii) **Completed Level 1 DGT Requests shall be archived and audited periodically by the DGT.**
   iv) **(See DGT Approval and Authorization Process)**

Level 2: Regulatory Requirement for Notification

1) Ohio State Law and other legal statutes, such as the Health Information Portability and Accountability Act (HIPAA), require notification to individuals in the event of a security breach of certain personal information. (Note: FERPA does not require notification of a breach, only "recordation" of the incident)
2) The BW campus refers to this data as "Notice Triggering" information:
   - Social security number
   - Driver's license number, Ohio identification number
   - Financial account numbers, credit or debit card numbers, and financial account security codes, access codes, or passwords
   - Personal medical information
   - Personal health insurance information
3) Note the following registration and approval requirements applicable to notice-triggering information:
   - Campus Credit Card transactions are handled differently based on the method of payment. Specialized training and Data Governance approval are required for BW staff, faculty, and/or students to handle credit card transactions on behalf of Baldwin Wallace.
   - Storage, transmission, or use of notice-triggering data requires that the requestor fill out a Data Governance Request Form.
4) For International students, applicability to General Data Protection Standards applies to any information collected by the various departments at BW:
   - Basic identity information such as name, address, and ID numbers (for example **Passport ID/copy, Citizenship documents**)
   - Web data such as location, IP address, cookie data, and RFID tags
   - Health and genetic data (for example **BW Health Center Med Center information)**
   - Biometric data
   - Racial or ethnic data
   - Political opinions
   - Sexual orientation
   - Grades and related scores (for example, **TOEFL Score**)
   - Financial related information (list of these required such as **International financial statement**)
5) **Access Control(s):** Access to this data requires:
   - **Completed Data Governance Request Form**
   - **Submitted to, and reviewed/approved by the appropriate Department DGT Owner**
   - **With an additional DGT Peer Check by one or more of the DGT members.**

- **Completed Level 1 DGT Requests shall be archived and audited weekly by the DGT.**
- **(See Appendix C: DGT Approval and Authorization Process)**

Level 3: Critical or Inferred Data

1) This data includes but is not limited to enterprise credentials, leadership credentials, financial information, backups, access to data resident on centralized system consoles, monitoring data, and security-related data.
2) If a data compromise would cause further and extensive data compromise from multiple (even unrelated) sensitive systems, the data creating this "Inferred-Data" warrants an elevated data protection level.
3) **Access Control(s):** Access to this data requires:
   - **Completed Data Governance Request Form**
   - **Submitted to, and reviewed/approved by the appropriate Department DGT Owner**
   - **This data shall only be released after the approval by either the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Data Protection Officer (DPO), or designee.**
   - **Completed Level 3 DGT Requests shall be archived and audited weekly by the DGT.**
   - **(See Appendix C: DGT Approval and Authorization Process)**

D. DGT Approval and Authorizations