Data Governance Charter

December 8, 2021

Baldwin Wallace University

Table of Contents

1 History of Data Governance 3
2 Current Status 3
3 Scope 5
4 Vision 5
5 Our Purpose is to… 5
6 Responsibilities 6

1 History of Data Governance

Historically, a culture of evidence was lacking due to mistrust in data reporting. Data was heavily siloed in various departments with no common definition and no consensus on how data was derived or reported. Communication between departments was sparse. It was not uncommon to have reports claiming to be data-driven but offering very different conclusions.

On November 19 – 21, 2013 a three-day workshop was conducted with our outside consultant, Michael Kurtz from the Center for Institutional Excellence at Ellucian, to establish a Data Governance team, a charter, and establish the processes and technologies to remedy this problem.

> **Executive Summary: (Quoted from the report)**
>
> Baldwin Wallace University contracted with Ellucian and the Center for Institutional Excellence to provide a three day seminar to jump start the focus on data and data governance at the university. The three day seminar was conducted on November 19, 20, & 21 2013.
>
> The objectives for the three days were to:
>
> - Enlighten participants with an institutional view of the current data issues at Baldwin Wallace.
> - Provide Baldwin Wallace with a framework for developing a sustainable, quality data management system to improve data reporting and informed decision making.
> - Begin to populate the framework with institutional specific actions.
>
> The seminar included a combination of learning, brainstorming, understanding the current situation at BW and beginning the process of visioning for the future.
>
> The group identified key problems with the current situation at BW including (but are not limited to): a lack of understanding who updates specific data, not knowing who fixes data problems, fractured processes and no communication between departments. All of these problems as well as many of the other problems that were identified can be solved with a good Data Governance Strategy.
>
> NOTE: A full copy of the final report can be found in the Data Governance team sharepoint site at: https://sp.bw.edu/sites/datagov/default.aspx

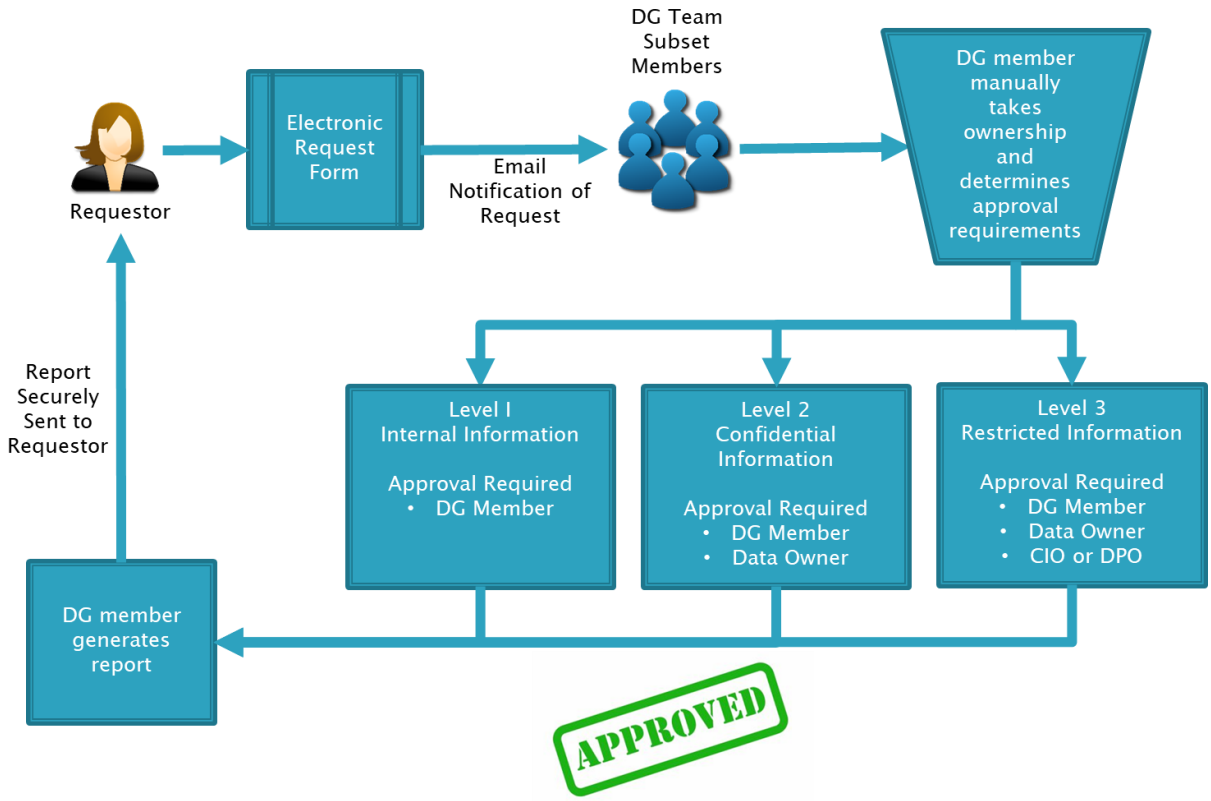
Membership on the team represented most of the University: Admissions, Athletics, Financial Aid, IT, Residence Life/Commuter Services, Philanthropy, and Alumni Engagement, University Relations, Registrar, Academic Affairs, Institutional Planning

Weekly team meetings were established to work on data governance issues.

2 Current Status

Many high-level reports have been created in BW's Business Objects web intelligence (WEBI) reporting tool in an attempt to have one version of the truth, instead of multiple conflicting reports. Internal KPIs have been defined and data owners have been identified. While not all reports have been consolidated, a significant portion has.

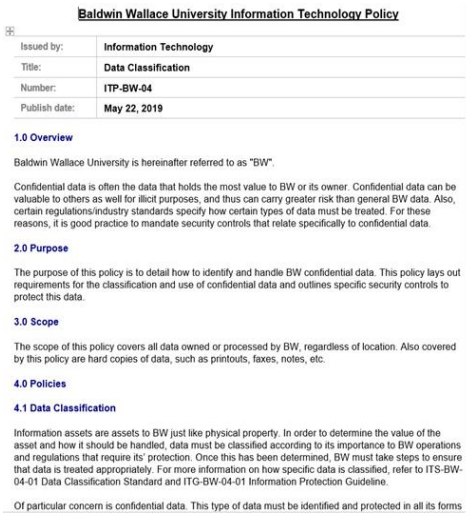
Requests for data have been formalized into an auditable workflow that requires the Data Owner, or their designate, approval and some definitions of report data have been standardized. See the following link to access it: www.bw.edu/datarequest



Policy status:

The Data Governance team issued and maintains a data governance policy. Additionally, IT via the IT Security Governance Committee has published the following policies on their website at https://help.bw.edu/policy.html in support of the Data Governance policy.

- ITP-BW-04 Data Classification Policy
- ITS-BW-04-01 Data Classification Standard
- ITS-BW-04-02 Data Dissemination Standard
- ITG-BW-04-01 Information Protection Guideline



Baldwin Wallace University Information Technology Policy

Issued by:	Information Technology
Title:	Data Classification
Number:	ITP-BW-04
Publish date:	May 22, 2019

1.0 Overview

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

Confidential data is often the data that holds the most value to BW or its owner. Confidential data can be valuable to others as well for illicit purposes, and thus can carry greater risk than general BW data. Also, certain regulations/industry standards specify how certain types of data must be treated. For these reasons, it is good practice to mandate security controls that relate specifically to confidential data.

2.0 Purpose

The purpose of this policy is to detail how to identify and handle BW confidential data. This policy lays out requirements for the classification and use of confidential data and outlines specific security controls to protect this data.

3.0 Scope

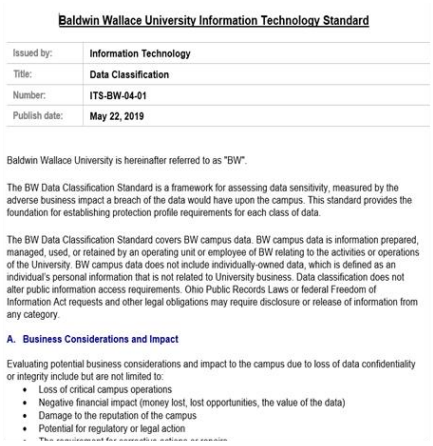
The scope of this policy covers all data owned or processed by BW, regardless of location. Also covered by this policy are hard copies of data, such as printouts, faxes, notes, etc.

4.0 Policies

4.1 Data Classification

Information assets are assets to BW just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to BW operations and regulations that require its' protection. Once this has been determined, BW must take steps to ensure that data is treated appropriately. For more information on how specific data is classified, refer to ITS-BW-04-01 Data Classification Standard and ITG-BW-04-01 Information Protection Guideline.

Of particular concern is confidential data. This type of data must be identified and protected in all its forms



Baldwin Wallace University Information Technology Standard

Issued by:	Information Technology
Title:	Data Classification
Number:	ITS-BW-04-01
Publish date:	May 22, 2019

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

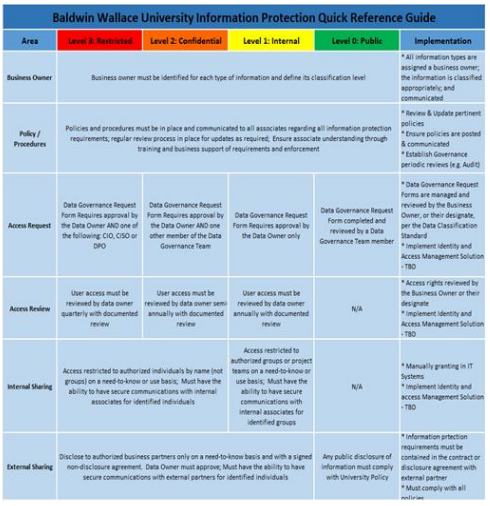
The BW Data Classification Standard is a framework for assessing data sensitivity, measured by the adverse business impact a breach of the data would have upon the campus. This standard provides the foundation for establishing protection profile requirements for each class of data.

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 to the campus due to loss of data confidentiality or integrity include but are 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



Baldwin Wallace University Information Protection Quick Reference Guide

Area	Level 3: Restricted	Level 2: Confidential	Level 1: Internal	Level 0: Public	Implementation
Business Owner	Business owner must be identified for each type of information and define its classification level				* All information types are assigned a business owner; the information is classified appropriately; and communicated
Policy / Procedures	Policies and procedures must be in place and communicated to all associates regarding all information protection requirements; regular review process in place for updates as required; Ensure associate understanding through training and business support of requirements and enforcement				* Review & Update pertinent policies * Ensure policies are posted & communicated * Establish Governance periodic reviews (e.g. Audit)
Access Request	Data Governance Request Form Requires approval by the Data Owner AND one of the following: CIO, CISO or DPO	Data Governance Request Form Requires approval by the Data Owner AND one other member of the Data Governance Team	Data Governance Request Form Requires approval by the Data Owner only	Data Governance Request Form completed and reviewed by a Data Governance Team member	* Data Governance Request Forms are managed and reviewed by the Business Owner, or their designate, per the Data Classification Standard * Implement Identity and Access Management Solution - TBD
Access Review	User access must be reviewed by data owner quarterly with documented review	User access must be reviewed by data owner semi annually with documented review	User access must be reviewed by data owner annually with documented review	N/A	* Access rights reviewed by the Business Owner or their designate * Implement Identity and Access Management Solution - TBD
Internal Sharing	Access restricted to authorized individuals by name (not groups) on a need-to-know or use basis; Must have the ability to have secure communications with internal associates for identified individuals		Access restricted to authorized groups or project teams on a need-to-know or use basis; Must have the ability to have secure communications with internal associates for identified groups	N/A	* Manually granting in IT Systems * Implement Identity and access Management Solution - TBD
External Sharing	Disclose to authorized business partners only on a need-to-know basis and with a signed non-disclosure agreement. Data Owner must approve; Must have the ability to have secure communications with external partners for identified individuals			Any public disclosure of information must comply with University Policy	* Information protection requirements must be contained in the contract or disclosure agreement with external partner * Must comply with all

The Data Governance team, with representatives from across the university, continues to meet weekly and meeting minutes are issued. A website at https://my.bw.edu/Employees/DGT/Pages/default.aspx contains additional information on the team's current membership and efforts.

3 Scope

The Data Governance team charter applies to data in the entire Baldwin Wallace community that is communicated between departments and to the Board of Trustees. This includes all Baldwin Wallace data, information, and assets regardless of their location and whether it resides on a physical medium such as paper or electronically.

Out of scope is data managed and handled only within a single department.

4 Vision

Establish and maintain sustainable processes, job responsibilities, and technologies to deliver information that is secure, consistent, accurate, verifiable, and trusted to improve business decision-making for the university.

5 Our Purpose is to…

5.1 Ensure responsibility, accountability, and sustainability of data policies and procedures centered around people, processes, and technology

Goal 1: In partnership with HR, establish common roles and responsibilities that ensure all data governance processes are followed and include them in all data owners, data coordinators, and their respective designates job descriptions. (Ref: Project scoping document)

5.2 Establish appropriate policies, standards, and guidelines that ensure data preservation, availability, security, confidentiality, and usability of data.

Goal 2: In partnership with the IT Security Governance Committee, establish all appropriate policies, standards, and guidelines to ensure data preservation, availability, security, confidentiality, and usability of data along with annual reviews. (Completed. See IT

policy website at: https://help.bw.edu/policy.html NOTE: The current Data Governance policy will be updated and converted to be in a consistent format as IT's policies.)

5.3 Create a common language and terms used for data collection, reporting, and analytics that is adopted and shared by the entire University.

Goal 3: Create a data dictionary to establish a common understanding of data elements in reports. (Ref: Project scoping document)

Goal 4: Create a data map to establish a common understanding of where essential data elements "source of truth" reside. (Ref: Project scoping document)

5.4 Regulate the utilization of a single source of data across the enterprise and eliminate conflicting secondary sources and 'shadow databases', as well as facilitate data reporting and analysis that is actionable and relevant to the University

Goal 5: Migrate all reports to WEBI and establish processes that ensure all new reports are in WEBI. (Ref: Project scoping document)

Goal 6: Create an educational awareness campaign around WEBI use as BW's standard data reporting tool. (Ref: Project scoping document)

Goal 7: Establish a requirement that all presentations of WEBI data contain a reference to the Data Request that generated the data. (Ref: Project scoping document)

Goal 8: Implement Identity Access Management (IAM) workflows, that are auditable, to manage all WEBI security group memberships. (Ref: Project scoping document)

6 Responsibilities

Below is a high-level description of individual responsibilities. For a complete definition, see ITP-BW-26 Data Governance Policy.

Chief Information Officer:

The university's Chief Information Officer (CIO) has overall responsibility for the management and scheduling of the Data Governance Team. The CIO will ensure that weekly meetings occur and both the charter and data governance policy are updated annually.

Chief Information Security Officer:

The Chief Information Security Officer (CISO) reports to the Chief Information Officer (CIO) and serves as a senior advisor on information security vision, strategy, and direction. The CISO works collaboratively with all university divisions and partners to establish information security and IT risk management functions that support the University in fulfilling its strategic goals, business obligations, and compliance requirements.

Data Owners:

Data owners are solely responsible for granting access to the data in their purview and ensuring its security and integrity.

Data Coordinators:

Data coordinators are the representatives of the Data Owners and are responsible for handling many of the day-to-day duties of managing data.

Departments and Other Units:

Departments and other units are responsible for the data integrity and security of any information they create, manage, or store, and for any information, they acquire or access from other university systems.

Users of Data:

Data integrity and security are everyone's responsibility. Each person in their respective role is responsible for the appropriate use and handling of data. Further, each person is required to follow all university policies, standards, and procedures as they perform their job tasks and report in a timely fashion any issues they may see.