Baldwin Wallace University Information Technology Policy

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

1.0 Overview

Baldwin Wallace University is hereinafter referred to as "BW". BW authorized user is hereinafter referred to as “user”.

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. 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 – electronic, printed, or stored on digital media per the directives in this policy and supporting standards.

4.1.1 Definition of Confidential Information

“Confidential Information” is information in Baldwin Wallace University’s possession that is not generally available to the public. For example, Confidential Information could include both Baldwin Wallace University and/or its customer’s information relating to business plans, finances, products, processes, student information, services, research, development, purchasing, data processing, engineering,

computers, software, firmware, marketing, merchandising and selling. Other Confidential Information could include customer lists, alumni lists, techniques used in education, test methods, etc.

4.1.2 Definition of Personally Identifiable Information

"Personally Identifiable Information" is a subset of Confidential Information and shall mean and include any information that alone or in combination with other information relates to a specific, identifiable person. By way of illustration and not limitation, "Personally Identifiable Information" includes individual's names, personal identification numbers such as Social Security or Social Insurance Numbers, credit card numbers, home telephone numbers, home address, driver's license numbers, account numbers, personal email addresses, and vehicle registration numbers. Specific information that can be associated with Personally Identifiable Information, such as a user ID, shall also constitute Personally Identifiable Information. For example, an individual's age alone is not Personally Identifiable Information, but if such age were capable of being associated with one or more specific, identifiable, individuals then such age would be deemed Personally Identifiable Information. Personally Identifiable Information also includes the fact that an individual has a relationship with Baldwin Wallace University. Supplier acknowledges and agrees that, as between it and Baldwin Wallace University, Baldwin Wallace University is the owner of all Personal Information of Individuals and has the right to direct it in connection with the collection, use, disclosure, and retention of such Personal Information.

4.1.3 Definition of Baldwin Wallace University Information

"Baldwin Wallace University Information" means all information and data, including Personally Identifiable Information and Confidential Information, (i) entered, stored, generated, or processed in or through Supplier's systems by or on behalf of Baldwin Wallace University, its affiliates, and subsidiaries, and/or their end-users or customers; (ii) generated or used by Supplier in connection with the Services under the Agreement; and/or (iii) derived from any of the foregoing.

4.2 Treatment of Information

The following sections detail BW requirements for the processing, storage, transmission, and destruction of information:

4.2.1 Processing (i.e. Use of cloud or third party services)

Only services that have completed an IT risk assessment, been approved by the Chief Information Officer and one of the following: Chief Talent Officer, Provost, or President, and have an established contract in place may be used to process Level I, Level II, or Level III data as defined in ITS-BW-04-01 Data Classification Standard.

4.2.2 Storage

Confidential data must be removed from desktops, computer screens, and common areas unless it is currently in use. Confidential information must be stored under lock and key (or keycard/keypad), with the key, keycard or code secured. Confidential electronic data must be stored in encrypted form, when technically possible, using strong encryption. Note that this requirement applies to backups containing confidential data as well. Confidential data must be stored only when absolutely necessary. Confidential data must never be stored on non-BW-provided systems (i.e., home computers, Internet file-sharing services,…) unless a Third Party agreement is in place with the appropriate controls mandated. See section 4.4 of this policy.

4.2.3 Transmission

Strong encryption must be used when transmitting confidential data, such as credit card data, student data, Personally Identifiable Information (PII) when such transmission takes place inside or outside BW's

networks. Confidential data must not be left on voicemail systems, either inside or outside BW's networks, or otherwise recorded.

4.2.4 Destruction

Electronic media containing Baldwin Wallace University Information must be destroyed in a manner that makes the recovery of the information impossible and per the Media Disposal Policy, ITP-BW-19 Media Disposal Policy.

4.3 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to BW's requirements involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must only access confidential data to perform his/her job functions.
- Users must not seek personal benefit or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor or the HelpDesk.

4.4 Sharing Confidential Data with Third Parties

If confidential data, is shared with third parties, such as service providers, a written agreement must govern the provider’s use and care of the confidential information. The agreement must include the following: 1) an acknowledgment that the provider is responsible for the security of the data that it possesses, and that it will appropriately secure any data that it stores or transmits on behalf of BW; and 2) how the data is to be used, transmitted, stored, and destroyed. See ITP-BW-16 Outsourcing Policy and ITS-BW-16-01 Information Security Exhibit for more details.

If physical media containing confidential is sent to/from BW, rigorous security procedures must be developed and maintained, which will include at a minimum, encryption of electronic media, credential verification, and signature of the service courier.

4.5 Receiving Confidential Data from Third Parties

If BW receives or in any way handles confidential data for other entities, such as customers or partners, it must treat this data as if it were its own confidential data. BW must acknowledge this responsibility in writing, through a formal agreement with the other entity. BW must take all necessary steps to secure any data that it possesses, stores, processes, or transmits on behalf of its customers or partners that may affect the security of the entity’s confidential data.

4.6 Emergency Access to Data

If BW’s confidential data has critical business or health implications (i.e., healthcare information), a procedure for accessing this data during an emergency must be developed and documented. The BW department owning the data must establish a procedure for emergency access in case the normal mechanism for access to the data becomes unavailable or disabled due to physical, system, or network problems.

The procedure should answer the following questions:

- What process must be followed to activate the emergency access procedure?
- What systems will it involve?
- In what situations should it be activated?
- Will it be activated automatically if certain conditions are met, or will it require human intervention? If so, who is authorized to decide to implement the procedure?
- Who will be involved in the process and what roles will they perform?

4.7 Applicability of Other Policies

This document is part of BW's cohesive set of policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

5.1 Employee Enforcement

This policy will be enforced by the Chief Information Security Officer, Chief Information Officer, and BW Administration. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.

5.2 Student Enforcement

Suspected misuse of the facilities should be reported to the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO). The CISO and/or CIO, who is authorized to determine if there has been a violation of policy or law and refer student violators to the Office of Student Conduct for resolution. Pending the outcome, access to the shared technology resources may immediately be restricted or suspended. In some cases, limited access will be provided to the facilities needed for University-related activities, such as classes. Violations can result anywhere from Conduct Probation to suspension or expulsion from the University. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.