# Baldwin Wallace University Information Technology Policy

| | |
|---|---|
| **Issued by:** | **Information Technology** |
| **Title:** | **Network Access and Authentication** |
| **Number:** | **ITP-BW-09** |
| **Publish date:** | **September 1, 2024** |

## 1.0 Overview

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

Consistent controls for network access and authentication are critical to BW's information security and are often required by regulations or third-party agreements. Any user accessing BW's computer systems can affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces the risk of a security incident by requiring consistent application of authentication and access controls across the network.

## 2.0 Purpose

The purpose of this policy is to describe what controls must be in place to ensure that users connecting to the BW network are authenticated appropriately, in compliance with BW requirements, and are given the least amount of access required to perform their function or role at BW. This policy specifies what constitutes the appropriate use of network accounts and authentication controls.

## 3.0 Scope

The scope of this policy includes all users who have access to BW-owned or BW-provided computers, systems, and cloud services or require access to the BW networks. This policy applies not only to employees, but also to students, guests, contractors, and anyone requiring access to BW networks or IT resources.

## 4.0 Policies

### 4.1 Account Setup

IT security starts with good user security; thus, BW requires that potential employees or contractors be screened before granting access. The level of screening should be appropriate to the position, with more in-depth background checks required for personnel with greater responsibilities or access to confidential information. Examples of acceptable screening methods include, but are not limited to, checking employment history, criminal records, credit history, and reference checks.

During the initial account setup, certain checks must be performed to ensure the integrity of the process. The following controls apply to account setup:

- Staff accounts will not be available for use until the first day of employment. Faculty, both full-time and adjunct, contractors, and vendors require the completion of a signed contract before accounts can be available for use.
- Computer IDs will only be granted as defined by ITS-BW-09-01 User ID Standard and using the process requirements as defined in that standard.
- Each user must be given a unique user ID before being granted access to network resources.

- Users will be granted access only if they agree to the Computer User Agreement defined in the ITS-BW-01-02 Computer User Agreement.
- Access to the network will only be granted per applicable policies, such as the ITP-BW-01 Acceptable Use Policy.
- The ability to add, delete, and change user IDs, user credentials, user privileges, and other account-related activities, must be limited as much as possible, such as to a small group of administrators with specific authority to make these changes. Any such activities must be documented, including approval from applicable management.
- IT must perform identity verification for any user-requested account changes, such as a passphrase reset, provisioning new tokens, or generating new keys. An example is a secret question or other private information that only the user would know. This helps prevent social engineering attacks, where an attacker will attempt to gain access by masquerading as the user and requesting a password reset.
- During the initial account setup or a passphrase reset, the account must be assigned a unique passphrase, which must be changed immediately after the first use. IT must not use the same passphrase for every new account or password reset.

### 4.2 Account Access Levels

It is BW policy to follow the principle of least privilege, where users will be provided the least amount of access required to perform their role at BW. This is particularly important as it relates to access to confidential student data. Any user account with access to this type of data must be given the minimum amount of access possible to perform their role.

Access levels must be assigned solely based on the user's role. The Business Owner of each system must define the access controls for each role, including systems and data access required to perform the role. Documentation must be kept that details each user's access request as well as approval of the user's access privileges by authorized parties.

An access control process that covers all system components must be utilized that enforces this policy and restricts users' access to data based on defined roles. This system must enforce the principle of least access, and have a default "deny all" setting for new or unrecognized users.

### 4.3 Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following controls apply to account use:

- Account user IDs must be created using a standard format as defined in ITS-BW-09-01 User ID Standard.
- In addition to the user ID, accounts must be protected by using something the user knows (such as a passphrase – refer to ITP-BW-02 Passphrase Policy for more information).
- Sharing of an individual's account is prohibited.
- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the IT or BW Leadership, or as required by applicable regulations or third-party agreements.
- Group accounts may be used for non-confidential or non-business critical functions only. Shared and/or generic user IDs are not used to administer any system components.
- User accounts must not be given administrator or 'root' access unless this is necessary to perform their role. All actions taken by individuals logged in with root or administrative privileges may be logged.
- Occasionally, guests, vendors, contractors, … will have a legitimate business need for access to BW IT resources. When a reasonable need is demonstrated, a Non-Employee account may be requested via the Guest Access process as defined in the ITS-BW-09-01 User ID Standard.

- Guest access to the Internet will not require an account. See ITP-BW-12 Guest Account Policy for additional information.

### 4.4 Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at BW, that employee's account can be disabled as soon as possible. Human Resources must create a process to notify Information Technology in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.) that will result in changes in access levels. The process must include same-day notification for termination or suspension actions. In the event termination is performed under some level of duress or non-mutual agreement, HR must call IT immediately, if not before termination, such that there is no window of opportunity for the person being terminated to maliciously use a BW computer account. Additionally, IT must audit nonstudent user accounts to verify that any inactive accounts over 90 days old are removed or disabled.

Similarly, if a contractor or vendor has been granted access to a BW account, that Third-Party contract must include appropriate notification provisions of their employee terminations as it relates to those who have access to BW accounts. See ITP-BW-16 Outsourcing Policy and ITS-BW-16-01 Information Security Exhibit for more details.

See ITS-BW-09-02 Identity Management for detailed requirements on when accounts are required to be deactivated or deleted.

### 4.5 Database Authentication Requests

Any access to a database containing confidential or cardholder data must require authentication, whether the access is by applications, administrators, or users. BW must restrict direct database access to only database administrators. BW must only allow the user access to, user queries of, and user actions on databases through programmatic methods, such as stored procedures, rather than direct access with a default level of access set to “READ ONLY”. Any application IDs for database applications must only be used by the intended applications, and not individual users or other non-application processes.

### 4.6 Use of Passphrases

When accessing the network locally, a username and passphrase are the minimally acceptable means of authentication. Usernames must be consistent with the requirements outlined in this document, and passphrases must conform to the ITP-BW-02 Passphrase Policy.

### 4.7 Screensaver Passphrases

Screensaver passphrases offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensaver passphrases are required and must be configured to activate after 15 minutes of inactivity.

### 4.8 Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to BW policies concerning antivirus software and patch levels on their systems. Users must not be permitted to access the BW Business network if these standards are not met. This policy may be enforced with a product that provides network admission control, or through other security controls that forbid access unless explicitly provided.

### 4.9 Encryption of Login Credentials

Industry best practices state that username and password combinations must never be sent over the network as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the BW network or across a public network such as the Internet. Username and passwords are considered confidential data, and further guidance regarding the treatment of this type of data can be found in the Data Classification Policy. When stored, all passwords must be stored in an encrypted format using strong cryptography.

### 4.10 Failed Login Attempts

Repeated login failures can indicate an attempt to 'crack' a passphrase and surreptitiously access a network account. To guard against passphrase-guessing and brute-force attempts, BW must lock a user's account after a maximum of 6 unsuccessful logins. This can be implemented as a time-based lockout (for a minimum of 30 minutes) or require a manual reset, at the discretion of IT.

To protect against account guessing, when login failures occur the error message transmitted to the user must not indicate specifically whether the account name or passphrase was incorrect. The error can be as simple as "the login credentials you supplied were incorrect."

### 4.11 Alternate Authentication Mechanisms

All controls about authentication should be viewed as minimum acceptable requirements. Where passphrases are specified, IT has the option to enforce additional controls that are as secure, or more secure, than passphrases, such as tokens or biometrics. When alternate authentication mechanisms are used, IT must ensure that:

- Authentication mechanisms are assigned to an individual account (not shared among multiple users).
- Physical and/or logical controls are in place to ensure that only the intended account can use the mechanism to gain access.

Any security incident involving alternate authentication mechanisms must be immediately reported to the Help Desk.

### 4.12 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.