# Baldwin Wallace University Information Technology Policy

| | |
|---|---|
| Issued by: | **Information Technology** |
| Title: | **Asset Management** |
| Number: | **ITP-BW-24** |
| 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”.

Asset management is the process of receiving, tagging, documenting, and eventually disposing of IT equipment and software. It is critically important to maintain up-to-date inventory and asset controls to ensure computer equipment and software locations and dispositions are well known. Lost or stolen assets often contain confidential or sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities

## 2.0 Purpose

The purpose of this policy is to establish the directives for IT asset management and to communicate the governance and controls necessary to support effective organizational asset management specifically focused on electronic devices and software.

## 3.0 Scope

This policy covers all IT systems, devices, and software that are purchased, leased, or rented by BW IT.

## 4.0 Policies

### 4.1 Asset Types

The following minimal asset classes are subject to tracking and asset tagging:

- Desktop workstations
- Laptop mobile computers
- Tablet devices
- Printers, copiers, fax machines, and multifunction print devices
- Handheld devices
- Scanners
- Servers
- Network appliances (e.g., firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)
- Private Branch Exchange (PBX) and Voice over Internet Protocol (VOIP) Telephony Systems and Components
- Internet Protocol (IP) Enabled Video and Security Devices
- Memory devices
- Software of any type

### 4.2 Asset Value

Assets that cost less than $200.00 are not required to be tracked, including computer components such as smaller peripheral devices, video cards, keyboards, or mice. However, assets, that store data regardless of cost, shall be tracked either as part of a computing device or as a part of network-attached storage. These assets include:

- Network Attached Storage (NAS), Storage Area Network (SAN), or other computer data storage
- Temporary storage drives
- Tape or optical media with data stored on them including system backup data

### 4.3 Asset Tracking Requirements

The following procedures and protocols apply to asset management activities:

- All assets must have an internal BW asset number assigned and mapped to the device's serial number.
- An asset-tracking database shall be created to track assets. For devices, it shall minimally include purchase and device information including:
  - Date of purchase
  - Make, model, and descriptor
  - Serial Number
  - Location
  - Type of asset
  - Owner
  - Department
  - Purchase Order number
  - Disposition

Before deployment, IT staff shall assign an ID to the asset and enter its information in the asset tracking database. All assets maintained in the asset tracking database inventory shall have a designated owner.

### 4.4 Asset Deposal and Repurposing

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources before assignment, transfer, transport, or surplus.

When disposing of any asset, sensitive data must be removed before disposal per the ITP-BW-19 Media Disposal Policy.

### 4.5 Audit Controls and Management

Documented procedures and evidence of practice shall be in place for this operational policy. Satisfactory examples of evidence and compliance include:

- Current and historical asset management system checks for various classes of asset records.
- Spot checks of record input and accuracy against the tracking database.
- Evidence of internal processes and procedures supporting this policy for compliance with general workstation computing policies.

### 4.6 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.