Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Configuration Management**
Number:	**ITP-BW-25**
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”.

Configuration Management (CM) is a discipline to ensure that the configuration of an item (and its components) is known and documented and that all subsequent changes to it are controlled and tracked. The goals of using CM are to ensure the integrity of a product and to make its evolution more manageable. Effective CM imposes controls over the activities that require updating and using multiple versions of project artifacts.

The Information Technology Infrastructure Library (ITIL) Framework highlights four classic operational aspects of CM:

- Identification:

  An identification scheme is needed to reflect the structure of the product. This involves identifying the structure and kinds of components, making them unique and accessible in some form by giving each component a name, version identification, and configuration identification.

- Control:

  Control the release of a product and changes to it throughout the life cycle by having controls in place that ensure consistent software via the creation of a baseline product, an approval mechanism for changing baselines, and access control mechanisms that ensure changes are only made by authorized personnel/processes. This often involves implementing policies and processes to manage change both internally within the performing organization as well as change requests coming from external sources such as client requests and regulatory changes.

- Status:

  Record and report the status of components and change requests and gather vital statistics about the product.

- Audit/Review:

  Validate the completeness of a product and maintain consistency throughout the entire project life cycle to ensure that the product is maintained as a well-defined collection of components.

2.0 Purpose

The purpose of this policy is to establish controls related to Configuration Management. It provides management’s directives in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

3.0 Scope

All IT assets managed by BW IT include software applications and products, supporting hardware and software infrastructure (e.g., equipment, networks, and operating systems), and associated documentation, whether located at the BW campus or a site housing those assets on behalf of BW.

Non-BW IT managed software/hardware is required to adhere to these same standards and practices as outlined in this policy.

4.0 Policies

The Configuration Management System (CMS) consists of a multi-layered structure comprised of policy, processes, procedures, and standards, with each layer providing an increased level of detail. The CM policy, processes, procedures, and standards shall be followed unless specifically designated as optional or discretionary. BW's CMS is intended to align as applicable with ITIL Configuration Management (CM) to the extent it meets BW business requirements. This will assist in the protection and support of IT assets and confidential information.

4.1 Baseline Configurations

BW IT shall develop, document, and maintain baseline configurations for servers, endpoints, and network switches/routers. Each type of asset has different requirements and relevant configuration data that should be maintained in their respective management applications to ensure that as new devices are installed, they start with a uniform set of security settings, patches, and configuration options wherever possible. It is the responsibility of the BW Administrators of those systems to maintain this data in a format for each type of system that is reproducible for consistent deployments.

All vendor-supplied default passwords must always be changed before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) community strings, etc.)."

All unnecessary default accounts must be removed or disabled before installing a system on the network.

4.2 Configuration Management Process

BW IT is responsible for coordinating and approving changes to BW IT managed systems. Each managed system change is approved by the respective BW IT Director responsible for the system that the change will primarily be affecting. If there will be a significant campus impact, the CIO may also be required to approve the change, and the impact is communicated to the campus via email whenever possible at least one day before the change when part of scheduled downtime.

Individual systems may define more detailed processes for change approval as necessary for the upkeep and maintenance of that particular system or where approvals outside of IT are required to authorize changes.

4.3 Analyze Security Impact of Configuration Changes

BW, where possible, will evaluate the security impact of significant planned or needed configuration changes. This should consider the impact of the change as well as the associated system risk of the affected system to maintain the existing security posture to protect confidential data. BW Directors can accept the associated risk of changes after considering this impact.

4.4 Utilization of Change Management

Utilization of a Configuration (or Change) Advisory Board (CAB) is the CM required change control forum for establishing CM baselines and approving/disapproving subsequent changes to those baselines. See ITP-BW-18 Change Management Policy for more details on the process.

4.5 Restrict Access for Implementing Changes

The relevant system administrator or owner of each system should limit the ability to affect configuration changes to only those personnel who require it for their job duties. This helps ensure that only qualified individuals who are responsible for managing a system will be able to initiate significant changes within the system that would either impact the availability or the security of that system.

4.6 Standardize Security-Related Configuration Settings

Security-related settings include but are not limited to rulesets, settings for ports and protocols, directory settings, and access controls including group and role-based policy objects. Where possible, BW IT will standardize the processes and procedures around the configuration of security-related settings to establish best practices and baseline configurations. These baselines should be stored in any applicable management tool used to administer the corresponding systems if available or documented as a process.

4.7 Manage Hardware and Software Lifecycles

Another aspect of configuration management is coordinating and establishing an asset lifecycle process. Lifecycle management addresses the issues of maintaining an asset over its estimated “shelf life” in the organization. In alignment with the mission of BW, these refresh cycles allow for long-term planning and budgeting to ensure that the needs of faculty, students, and staff are met.

Lifecycle management is important beyond ensuring the availability and efficiency of a system. To protect the data assets from degradation, data loss, failing hardware, and evolving security threats, systems must be refreshed at regular intervals. The rate of change for modern threats evolves at such a pace that the security landscape can be drastically altered over a relatively short period of years. Lifecycle management helps ensure that IT systems are replaced and maintained with updated security features to meet new and evolving security standards to protect BW assets and stakeholders. Each IT system, wherever possible, should have a defined refresh lifecycle to determine the budget year for replacement or retirement. BW IT is responsible for developing and maintaining the lifecycle plans for each category of system or individual system.

4.8 Exceptions

If an exception from this policy is required, a BW Policy Exemption Form needs to be submitted to the CIO, and it must clearly articulate the reason for the exemption. An operational risk assessment by the IT Security Governance Committee will be conducted to identify the risks associated with this exemption. The recommendation is then submitted to the Vice President of Finance and Administration if the University can accept the risk, an exemption to this policy may be granted.

4.9 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.