Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Change Management**
Number:	**ITP-BW-18**
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”.

Change Management provides a process to apply changes, upgrades, or modifications to the IT environment. This covers all changes to BW hardware or software. It also includes modifications, additions, or changes to any other environmental components such as electrical or cooling systems. The goal of the change management process is to ensure that any change that affects one or all of the environments that BW IT Operations relies on to conduct normal business operations is protected.

2.0 Purpose

The purpose of this policy is to describe the controls to be followed when any changes to BW IT resources are to be made. The Change Management policy is designed to provide a managed and orderly method in which changes to the information technology environment are requested, adequately tested, and approved before installation or implementation. The purpose is to ensure that all controls are in place, there is no negative impact on the infrastructure, all the necessary parties are notified in advance, and the schedule for implementation is coordinated with all other activities.

Changes to the environment arise from many circumstances, such as, but not limited to:

- User requests
- Hardware and/or software upgrades
- Acquisition of new hardware and/or software
- Environmental changes
- Business Operational schedule changes
- Unforeseen events
- Scheduled Periodic Maintenance

The end goal of any Change Management policy is to increase the percentage of uptime and reliability of BW IT systems and network services for students, faculty, and staff and minimize the number and impact of any related incidents.

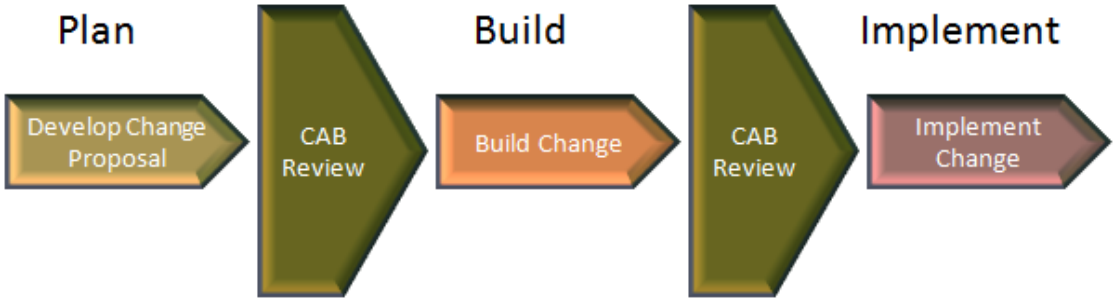
3.0 Scope

This policy applies to all IT resources and applications owned and managed by BW. For non-BW managed IT resources and applications, the requirements in this document must be addressed with Third Parties in the contract agreement per ITP-BW-16 Outsourcing Policy. Student devices are out of scope.

4.0 Policy

4.1 Change Control Process

BW will adhere to a simplified version of the ITIL Change Control process:



4.2 Types of Changes

Major:

Changes that could potentially have a high-impact and/or high-risk items that may alter production systems. These require CAB approval, per section 4.4, along with business approval. These types of changes have the potential to create a significant impact on ongoing business operations and also may have financial implications. Therefore, the Request for Change (RFC) contains a detailed proposal on cost-benefit and risk-impact analysis.

Examples – Restructuring an accounts receivable database; replacing an existing HR application with a new one.

Standard:

Standard changes are generally pre-approved changes that have low impact and low risk. These changes occur periodically and follow a standard procedure. They do not follow the conventional process flow and can be saved as a standard change template for reuse. CAB approval every time is not required as these changes are evaluated and approved once initially.

Examples - Deploying monthly Windows patches, setting up a user account, etc.

Minor:

Minor changes are generally normal changes that do not have a significant impact and are less risky to execute. These are non-trivial changes that do not happen frequently but are required to undergo every stage of the change management lifecycle, including CAB approval. It is important to document related information so that these can be converted to a standard change in the future if needed.

Examples: Application performance improvement, and website redesign.

Emergency:

Emergency changes are unexpected interruptions that need to be fixed as quickly as possible, and time does not permit following the normal RFC (Request for Change)

process. After the work is completed, an RFC (Request for Change) must be submitted for approval via the CAB. These changes must be reviewed to avoid potential infrastructure risks in the future, and detailed documentation is done post-change execution.

Examples - Fix for a security breach, server outage restoration.

4.3 Request for Scheduled or Planned Maintenance

Before the commencement of any planned or scheduled maintenance, a Request for Change (RFC) must be completed and signed off by a supervising member of the IT Department, and if it is a Standard or Major impact, the Change Advisory Board. The only exception to this approval process is if an emergency is declared.

4.4 Change Advisory Board (CAB)

CAB meetings will be held routinely and will discuss the following items:

- Approve or Deny new proposed RFCs.
- Review all completed RFCs and Emergency changes in the past two weeks.
- In the event of a failed change or one that caused unexpected issues, the CAB will review and approve the post-mortem report on the change to prevent future similar events.

4.5 Documentation of Changes

A ChangeLog shall be kept in an accessible location for the entire IT department to view. Every member of the IT Department, who is in a position to make changes to a system or network resource, will be required to place an RFC into this process to document any changes being made without exception. Other members of the IT department are encouraged to review the log from time to time to keep abreast of the changes going on in the computer network.

4.6 Maintenance Windows and Scheduled Downtime

Certain tasks require systems or application services to be taken offline, either for a simple reboot, an upgrade, or other maintenance. When this occurs, the IT Staff must perform the tasks during a scheduled weekly or monthly maintenance window.

4.7 Emergencies

Emergencies exist only as a result of:

- There is a degradation of service needing immediate action,
- A system/application/component is inoperable, and the failure causes a negative impact
- A response to an emergency business needs.

In the event of an emergency, the work may be completed without approved change control. However, after the emergency is over and the work completed, an RFC must be completed and approved by the CAB.

4.8 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 will 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.