Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Secure Software Development**
Number:	**ITP-BW-27**
Publish date:	**September 1, 2024**

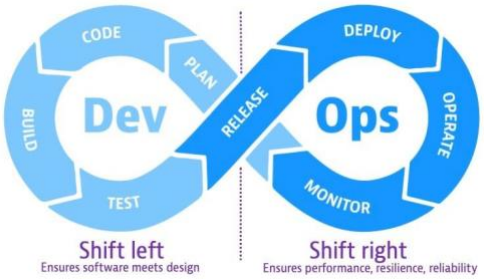
1.0 Overview

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

BW primarily uses off-the-shelf software and does not have an application development staff. However, some of the infrastructures such as Active Directory, and applications such as Colleague have proprietary scripting languages to perform customizations. As such, many of the elements of typical software development lifecycle (SDLC) models are not relevant since BW does not engage in significant application development projects. For the small amount of coding that is conducted, this policy outlines steps that are required to be taken to minimize vulnerabilities and risks to the university and its students.

2.0 Purpose

The purpose of this policy is to ensure that any scripting or software development is managed to an acceptable level of risk in a consistent and systematic process. Relevant elements of the NIST Secure Software Development Framework (SSDF) Version 1.1 and The Open Web Application Security Project® (OWASP) are leveraged for their best practices to “Shift Left” the mitigation of software vulnerabilities. (Shift-left is the practice of moving testing, quality, and performance evaluation early in the development process, often before any code is written.)



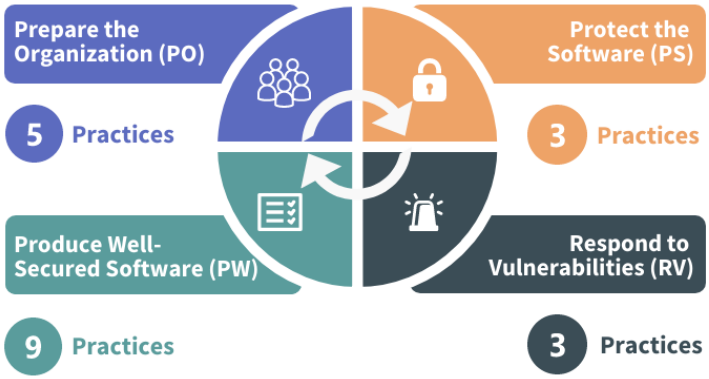
3.0 Scope

This policy applies only to code developed by BW IT that affects sensitive data as defined in the DGP-BW-04 Data Classification Policy in support of the university. For purchased applications or code developed for the university by a third party, BW leverages contractual agreements and the industry-standard “Higher Education Community Vendor Assessment Toolkit” (HECVAT) for vendor risk assessments. The HECVAT is a questionnaire framework specifically designed for higher education to measure vendor risk. See ITP-BW-16 Outsourcing Policy and ITS-BW-16-02 Vendor Risk Assessment for further information.

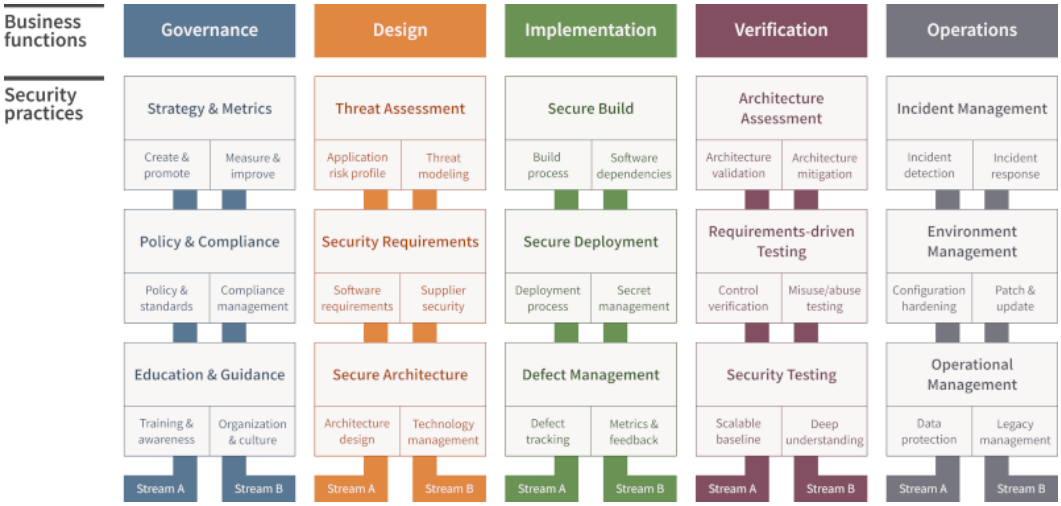
4.0 Policy

4.1 The Process

At a high level, the NIST Secure Software Development Framework (SSDF) Version 1.1 contains 20 best practices to aid in the development of secure code. However, it does not prescribe how to implement each practice. The focus is on the outcomes of the practices rather than on the tools, techniques, and mechanisms to do so.



NIST SSDF then maps practices to several of the industry-recognized Software Develop Lifecycle (SDLC) models such as The Open Web Application Security Project® (OWASP) for the how.



BW has adopted scaled-down versions of these two industry best practice standards, NIST SSDF and OWASP in ITS-BW-27-01 Secure Coding Practices. If the practices in the standard ITS-BW-27-01 Secure Coding Practices do not adequately cover a specific development requirement to meet industry reasonable standards and acceptable levels of risk, the developer should refer to the full NIST SSDF and OWASP standards for additional guidance.

4.2 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.