Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Incident Response**
Number:	**ITP-BW-10**
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”.

A security incident can come in many forms as it affects the Confidentiality, Integrity, and/or availability of information or information systems. Examples may include a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident.

2.0 Purpose

This policy is intended to ensure that BW is prepared if a security incident were to occur. It requires what must occur if an incident is suspected, covering both electronic and physical security incidents as it relates to IT or data.

3.0 Scope

The scope of this policy covers all IT-related physical and information assets owned or provided by BW, whether they reside on the BW network or elsewhere. Out of scope are physical security incidents typically not involving IT such as fire, severe weather, breaking and entering, active shooter, assault, and other non-IT-related incidents.

4.0 Policies

An information security incident is defined as any incident that potentially exposes BW data to anyone who has not been authorized to see the data or anyone who abuses an IT resource. E.g. it affects the Confidentiality, Integrity, and/or availability of information or information systems. An incident may occur from an external or internal source. The following are examples of security incidents and are not a complete list:

- A system is breached by an external hacker
- A denial of service attack
- A virus, worm, rootkit, keylogger, etc. compromises a system
- A laptop is lost or stolen
- A user shares their password or a restricted resource with another person
- A user gains access to unauthorized data through technical or social engineering
- A backup tape has been lost or stolen
- A thumb drive, CD, etc. is lost or stolen
- A user uses his/her access in a non-authorized manner
- Data is sent by e-mail to non-authorized users
- A hard copy report is lost or stolen that contains PCI data

As the examples illustrated above, a security incident may occur from an accidental occurrence or a malicious activity.

4.1 Confidentiality

All information related to a security incident must be treated as confidential information until the incident is fully contained and investigated. This will serve both to protect people’s reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers via approved BW methods.

4.2 The Incident Management Process

BW will adhere to the SANS Institute incident management model known as PICERL which stands for Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

4.3 Incident Response Team

The Computer Security Incident Response Team (CSIRT) responds to and investigates security events to determine whether an incident has occurred, and the extent, cause, and damage of incidents. If an incident is declared, the CSIRT will work the incident per the PICERL process. The membership of the CSIRT team will vary depending on the type and severity of the incident as detailed in the ITS-BW-10-01 Incident Response Standard.

4.3 Authority and Responsibility of the CSIRT

The CSIRT directs the Identification, Containment, Eradication, Recovery, and Lessons Learned phases of all IT security incidents and may authorize and expedite changes to information systems necessary to do so. The CSIRT also coordinates responses with external parties when existing service agreements place responsibility for incident investigations on the external party.

During the conduct of security incident investigations, the CSIRT is authorized to monitor relevant IT resources within the scope of the incident and retrieve communications and other relevant records of specific users of BW IT resources, including login session data and the content of individual communications without notice or further approval. However, all such access performed during an incident must be logged by the CSIRT Team Leader.

Any external disclosure of information regarding information security incidents must be reviewed and approved by the Office of General Counsel and University Relations.

The CSIRT Team Leader coordinates with law enforcement, government agencies, the Security Operation Center, peer CSIRTs, and relevant Information Sharing and Analysis Centers (ISACs) in the identification and investigation of security incidents. The CSIRT is preauthorized to share anonymized threat and incident information with ISACs.

4.4 Preparedness

The Chief Information Officer shall have in place the appropriate contacts, contracts, and plans to leverage additional resources as needed such as, but not limited to, Legal Counsel, Crisis Communications, external incident response team, and both Local and Federal law enforcement.

4.5 Review, Testing, and Maintenance

The Chief Information Security Officer shall conduct a tabletop exercise annually to test all the plans and processes required by this policy. A full report of the tabletop results must be documented, along with improvement recommendations, to the Chief Information Officer.

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.