# Baldwin Wallace University Information Technology Policy

| | |
|---|---|
| Issued by: | **Information Technology** |
| Title: | **Network Security Monitoring Policy** |
| Number: | **ITP-BW-14** |
| 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 intends to provide a secure network infrastructure to protect the confidentiality, integrity, and availability of BW data and minimize the risk of a security incident. Even with appropriate preventative controls in place, no environment is perfect. To assure a reasonably secure environment requires the appropriate monitoring and incident detection to be in place.

## 2.0 Purpose

The purpose of this policy is to establish the basic technical controls required to reasonably monitor and detect malicious activity on BW networks and servers.

## 3.0 Scope

This policy covers all IT networks, systems, and devices that comprise the BW computing environment or are attached to it. This includes personal devices owned by students or employees as well as contractors’ devices that attach to a BW-provided network. For non-BW managed IT resources, these controls must be addressed in the Third-Party contract.

## 4.0 Policies

### 4.1 Log Management

The logging of certain events is an important component of good network management practices. Logs contained on application servers, network devices, and critical systems may all contain different data, but all contain valuable information that BW must record. Thus, BW requires that logging on network-level devices must be enabled to the degree it is reasonably required by a Security Operation Center to detect malicious activity and remediate such incidents. In addition:

- No passwords must be contained in logs and every effort taken to minimize the capture of PII or other sensitive data in logs.
- Key logs are to be continuously reviewed for malicious activity by a Security Operations Center. Other logs should be reviewed periodically based on BW’s overall risk management strategy and operational requirements as determined by the annual risk assessment, and at the discretion of the Chief Information Officer. The frequency of these reviews should be based on BW’s perceived level of risk. Any exceptions or anomalies discovered during the review process must be fully investigated, and the results documented.
- Logs must be retained per the ITP-BW-06 Retention Policy. Unless known to only contain non-proprietary and/or public data, BW must classify network device logs as confidential data. See ITP-BW-04 Data Classification Policy for additional clarification on data types.

An attacker will often try to erase records of what he or she changed on a system. For that reason, BW must secure logs such that they cannot be altered. The following requirements apply specifically to the protection of logs:

- Only those with a job-related need may be able to view or access logs.
- Logs must be protected from unauthorized modifications.
- Where technically possible and not cost-prohibited, logs must be sent to a centralized log server.

### 4.2 Intrusion Detection/Intrusion Prevention

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. These tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad since legitimate network traffic can be blocked along with malicious traffic.

BW requires the use of either an IDS or IPS on critical or high-risk or high-security network segments. If an IDS is used, procedures must be implemented to review and act on the alerts expediently. If an IPS is used, procedures must be implemented that provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic.

### 4.3 File Integrity Monitoring

File Integrity Monitoring (FIM) will alert to changes to critical system files. This can be useful in notifying the IT staff of malicious activity or other significant network events that may otherwise go unnoticed. For mission-critical servers, BW requires the use of an effective change detection mechanism, such as FIM technology, that will alert to changes, additions, and deletions to critical system files, configuration files, or content files. The software must be configured to perform critical file comparisons at least weekly. BW must implement a process to respond promptly to any alerts generated by the change-detection software.

### 4.4 Antivirus/Anti-Malware

Computer viruses and malware are pressing concerns in today's threat landscape. If a system or network is not properly protected, a virus outbreak can have devastating effects on the system, the network, and the entire BW. BW provides the following directives on the use of antivirus/anti-malware software:

- All MS Windows and Macintosh user workstations, laptops, and servers must have antivirus/anti-malware software installed, fully functioning, and up-to-date with both software and signatures.
- Antivirus software must automatically run periodic scans with no user intervention required to initiate the scan.
- For BW-provided devices, BW must ensure that antivirus software is running and cannot be disabled or altered by users.
- If there is a legitimate technical need to disable the antivirus software temporarily, this is permitted only with IT approval and for a limited time. BW should consider implementing additional security measures for the time that the antivirus software is disabled.

### 4.5 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.