Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Outsourcing**
Number:	**ITP-BW-16**
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”.

Outsourcing IT services is often necessary but should be carefully considered since, by nature, a certain amount of control will be lost by doing so. The following questions should be considered before outsourcing:

- Can the service be performed better or less expensively by a Third-Party provider?
- Would it be cost-prohibitive or otherwise unreasonable to perform this service in-house?
- Will outsourcing the service positively affect the quality of this service?
- Is the cost of this service worth the benefit?
- Are any risks associated with outsourcing the service worth the benefit?

2.0 Purpose

The purpose of this policy is to specify actions to take and controls to implement when selecting a provider of outsourced IT services.

3.0 Scope

This policy covers all Third-Party services that will store or process BW data.

4.0 Policies

4.1 Evaluating a Provider

Once the decision to outsource an Information Technology function or service has been made, selecting the appropriate provider is critical to the success of the endeavor. Due diligence must be performed after the potential providers have been pared to a shortlist of two to three companies. Due diligence must always be performed before a provider is selected. Due diligence must include a thorough evaluation of the provider's ability to perform the requested services, and must specifically cover the following areas:

- Ability to deliver the service.
- Experience of the provider.
- The reputation of the provider.
- The provider’s policies and procedures related to the service.
- The financial strength of the provider.
- Examination of the service level agreements provided by the provider.
- A vendor risk assessment, per ITS-BW-16-02 Vendor Risk Assessment, must be conducted to ensure the prospective candidate meets BW security requirements
- The provider's IT security controls for how confidential/cardholder data will be secured in transmission and while stored.

- If cardholder data is to be shared or processed, the status of the provider's PCI DSS compliance and has the provider’s compliance been validated by an annual external assessment with evidence provided of compliance.

After the provider is selected, BW must conduct the due diligence above on an annual basis.

4.2 Security Controls

The outsourcing contract must provide a mechanism for secure information exchange with the service provider. This will vary with the type of service being outsourced but may include remote access, VPN, or encrypted file exchange.

BW and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain access to BW data.

4.3 Outsourcing Contracts

Trust is necessary for a successful outsourcing relationship; however, BW must be protected by a contract that details and enforces the terms of the outsourcing relationship. All outsourced Information Technology services must be governed by a legal contract, with an original of the executed contract maintained by BW.

All outsourced IT Technology contracts such as new software/hardware, cloud services, or processing of BW data in any way must be reviewed and approved by the Chief Information Officer. Contracts that are not vetted by IT are in noncompliance with this policy and subject to remediation actions.

In addition, all contracts must:

- Cover a specified time period
- Specify exact pricing for the services
- Specify how the provider will treat confidential information
- Include a non-disclosure agreement
- Specify services to be provided, including Service Level Agreements and penalties for non-compliance
- Allow for cancellation if contractual terms are not met
- Specify standards for subcontracting of the services and reassignment of contract
- Cover liability issues
- Include a “hold harmless clause” as applicable
- Describe how and where to handle contractual disputes

To ensure all appropriate IT Security controls are in place, contracts must also include all relevant sections in the ITS-BW-16-01 Information Security Exhibit.

4.4 Third-Party Access to Information

The provider must be given the “least privileged” amount of network, system, and/or data access required to perform the contracted services. This access must follow all applicable BW policies and be periodically audited.

4.5 List of Providers

BW must maintain a list of vendors/service providers with whom confidential data, as defined by the ITP-BW-04 Data Classification Policy, is shared. This list must include the type of data shared, the date of last due diligence, and any other relevant information for appropriate and secure relationship management (such as contract length, internal/external contact person, etc.).

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 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.