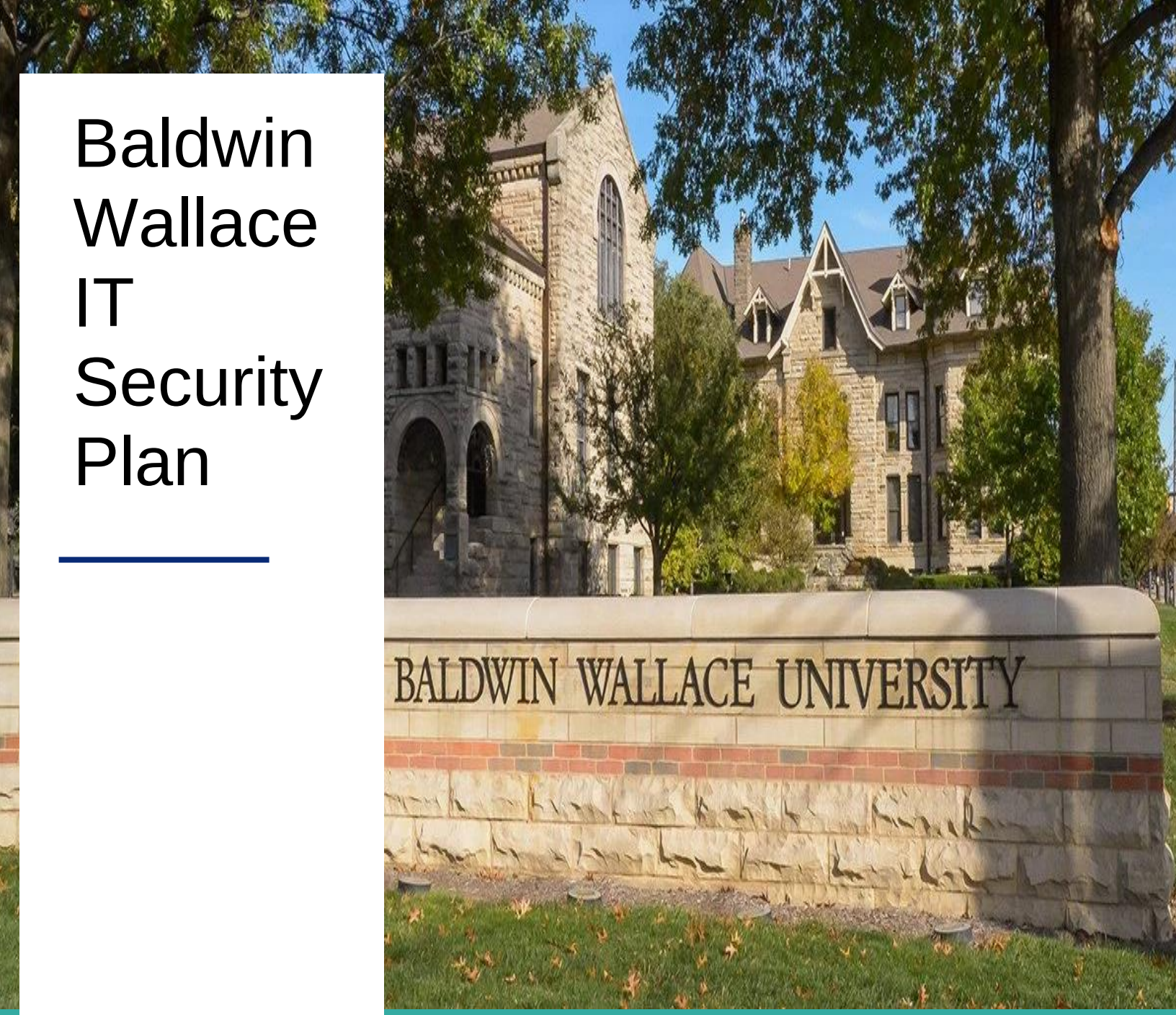
Baldwin Wallace IT Security Plan



JUNE 1, 2022

Baldwin Wallace University

BE ALERT

Table of Contents

1 Baldwin Wallace University Information Security Plan (ISP)

An Information Security Plan (ISP) is designed to protect information and critical resources from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information Technology (IT) security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed, and improved, where necessary, to ensure that the specific security and business objectives of Baldwin Wallace University are met.

This plan governs the privacy, security, and confidentiality of University data, especially highly sensitive data, and the responsibilities of departments and individuals for such data. IT security measures are intended to protect information assets and preserve the privacy of Baldwin Wallace employees, students, sponsors, suppliers, and other associated entities. Inappropriate use exposes Baldwin Wallace to risks including virus attacks, compromise of network systems and services, and legal issues.

All users of Baldwin Wallace's information technology resources are required to follow ***all Information Security Compliance Policies*** and are bound by this plan as well as other University policies and procedures as terms of their employment. All employees share responsibility for the security of the information and resources in their respective departments.

2 Purpose

The purpose of this plan is to ensure the confidentiality, integrity, and availability of data, define, develop, and document the information policies and procedures that support the University's goals and objectives, and allow the University to satisfy its legal and ethical responsibilities concerning its IT resources.

Information security policies and procedures represent the foundation for the University's ISP. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout Baldwin Wallace.

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud, and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business. When consistently applied throughout the University, these policies and procedures assure that information technology resources are protected from a range of threats to ensure business continuity and maximize the return on investments of business interests.

This plan reflects Baldwin Wallace's commitment to stewardship of sensitive personal information and critical business information, in acknowledgment of the many threats to information security and the importance of protecting the privacy of University constituents, safeguarding vital business information, and fulfilling legal obligations. This plan will be reviewed and updated at least once a year or when the environment changes.

3 Scope

This plan applies to the entire Baldwin Wallace community, including the President, Vice Presidents, Deans, Directors, Department Heads, students, faculty, staff, alumni, trustees, temporary employees, contractors, volunteers, and guests who have access to Baldwin Wallace provided information technology resources. In addition, this plan applies to all Baldwin Wallace data, information, and assets owned or procured IT whether it resides on campus or in the cloud.

4 Information Security Objectives

Information security is critical to the interests of the university and the many constituencies it serves. The following list provides some of the objectives of information security at Baldwin Wallace University. This list is representative and is not meant to suggest the full range of objectives of the university's information security policy or program.

- **Support and maintain the ongoing functions of the** university**.** As an increasing percentage of the university's functions are handled electronically, it is critical that information and information systems be protected so the university can operate without interruption.

- **Protect** university **assets.** The university owns many assets including intellectual property, research, and instructional data systems, as well as physical assets. The loss of these assets could have a significant financial impact as well as a major negative impact on critical research and instructional programs.

- **Safeguard the privacy of individuals and information.** With the increasing risk of identity fraud and other potential misuses of personal information, it is paramount that the university safeguards personal information entrusted to its stewardship.

- **Safeguard financial transactions and electronic communications.** The university is the custodian of financial records and transactions; safeguarding these records is critical to maintaining trust relationships essential to our business function.

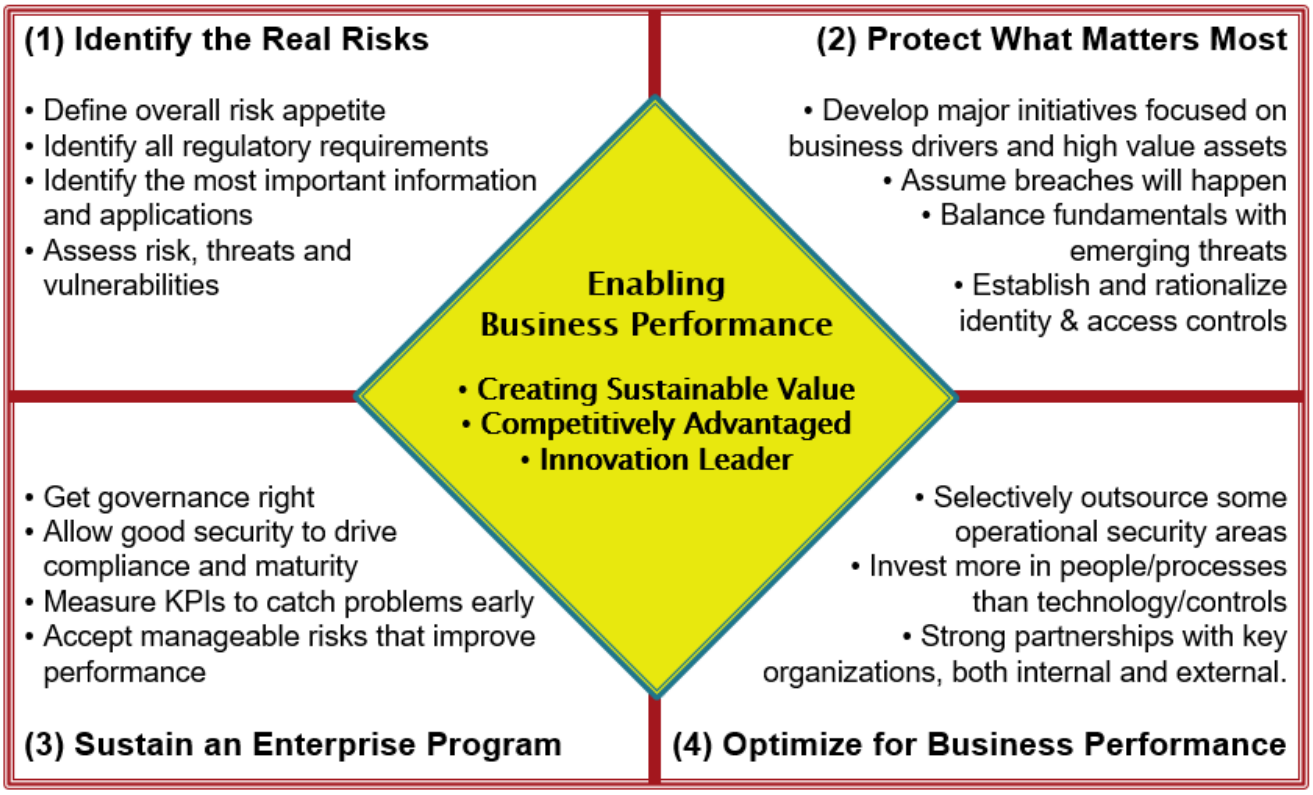
- **Protect the integrity and reputation of the institution.** Security breaches reflect negatively on the capability of the university to manage entrusted resources. In addition, security breaches could result in the potential for criminal or civil action.

- **Prevent the use of** university **systems for malicious acts.** The open nature of the university and the desire to provide ease of access to a large and diverse group of constituents makes us a target for unauthorized users to utilize university resources inappropriately. The university must prevent the use of Baldwin Wallace University systems and infrastructure for malicious acts against its systems as well as attacks against other individuals and organizations.

- **Comply with state and federal laws.** State and federal laws and regulations require the university to take reasonable steps to ensure the security of the data (FERPA, HIPPA, GLBA, GDPR,…).

5 IT Security Strategy

The figure below depicts Baldwin Wallace's risk-based IT Security strategy to adequately protect the university.



6 Responsibilities

Risk Management Sub-Committee:

The Officers of the University and the Board of Trustees Risk Management Sub-Committee is ultimately responsible for managing IT risk, determining which risks to fund for mitigation, and which ones to accept. The CIO, with the support of his staff, is responsible to report on all significant IT risks and their respective mitigation status to the sub-committee a minimum of twice a year.

Chief Information Officer:

The university's Chief Information Officer (CIO) has overall responsibility for the management, operations, and budgeting of the university's information technologies and its security. Implementation of security policies is delegated throughout the university to various university services, departments, and other units; and to individual users of campus information resources.

Chief Information Security Officer:

The Chief Information Security Officer (CISO) reports to the Chief Information Officer (CIO) and serves as a senior advisor on information security vision, strategy, and direction. The CISO works collaboratively with all university divisions and partners to establish information security and IT risk

management functions that support the University in fulfilling its strategic goals, business obligations, and compliance requirements.

University Services:

Various officers within the university have the primary responsibility and authority to ensure Baldwin Wallace University meets external and internal requirements for intellectual property, research, and institutional data, and privacy and security of confidential and business information. Multiple departments are responsible for general security issues (legal issues, security compliance, physical security, communications, and IT infrastructure security). These individuals or departments are responsible for assisting in the development of university information security policies, standards, and best practices in their areas of responsibility. They are also responsible for advising departments and individuals in security practices related to areas they oversee, as follows:

- Personnel information and confidentiality - Human Resources
- Student information and confidentiality - Registrar's Office, Provost
- Financial information and transactions - Finance and Administration
- Student I.D. information- I.D. Office
- Student loan information and student financial records - Financial Aid, Bursar
- Infrastructure, communication, and systems security and audit - ITS
- Legal Issues - Finance and Administration division for engaging legal counsel service
- Health information - Student Life, Health Center
- Alumni, parent, and donor information - Advancement Office
- Other information – Chief Information Officer

Departments and Other Units:

Departments and other units are responsible for the security of any information they create, manage, or store, and for any information, they acquire or access from other university systems (i.e. student records, personnel records, business information).

Users of IT Resources and Data:

Security is everyone's responsibility. Each person in their respective role is responsible for the appropriate use and handling of IT resources and data. Further, each person is required to follow all university policies, standards, and procedures as they perform their job tasks and report in a timely fashion any issues they may see.

7 Enforcement

All individuals accessing University data at Baldwin Wallace University are required to comply with federal and state laws, University policies, and procedures regarding the security of data. Any University employee, student, or non-university individual with access to University data who engage in unauthorized use, disclosure, alteration, or destruction of data violates this plan and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action. Failure to comply with University policies, standards, and procedures may result in loss of computing privileges and/or disciplinary action, up to and including termination

8 Regulatory Compliance Requirements

Baldwin Wallace University, being a higher education facility that is involved in every aspect of student living and education, houses a medical facility, payment centers, financial/loan services, capture of student information, and is involved in all aspects of student living. As such, BW is subject to many cybersecurity standards with the following applicable cybersecurity standards having been identified as a priority:

- HIPAA (Med Center and Athletic Medicine)
- PCI-DSS (Point of sale, bursars office)
- FERPA (Colleague, Enrollment, online directories, trusted partners)
- FTC's Red Flag Rules
- GLBA (Giving programs, Financial Aid)
- State of Ohio Laws: Title XXXIII ORC 3319.321(B)

Further, Baldwin Wallace University has standardized on the NIST Cyber Security Framework (CSF) as its' overarching set of IT Security controls and will assess itself against NIST CSF in addition to the above-mandated control frameworks.

9 IT Security Steering Committee

Baldwin Wallace has implemented an IT Security steering committee that provides direction and guidance to the security program and its strategies. The main benefit of the steering committee is that it solicits feedback from other parties and ensures there is a formalized approval process. A collaborative approach is taken for the committee to ensure it works properly and generates the required outputs. Membership includes:

- Tom Mathis, CISO / CISSP
- Dan Schrag, Assistant Professor Business - Audit
- Edward Napoleon, CISM /BW Board of Trustee
- Frank Braun, CISM / Outside Advisor UA – Little Rock
- Shane Morehouse, Director of Client Services
- Craig Kitko, Director of Digital Infrastructure
- Melissa Bauer, Director of Administrative Systems
- Greg Flanik, CIO

10 Policies

Policies are management directives on how BW IT Resources should use and maintain as well as the data in them. The University's policies are based around the control requirements stated in NIST FIPS PUB 200 as well as those expected in the Center for Internet Security top 20 controls, the NIST Cyber Security Framework, and other applicable regulatory requirements as they would reasonably apply to a higher education institution and match Baldwin Wallace business requirements.

While the above-stated set of control frameworks do not all cleanly map together one to one, BW policies are presented below roughly mapped to the FIPS PUB 200 categories of controls. Note: Some policies may extend into multiple categories but, for the sake of brevity, only be listed once.

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and the types of transactions and functions that authorized users are permitted to exercise.

ITP-BW-03 Remote Access Policy
ITP-BW-09 Network Access and Authentication Policy
    ITS-BW-09-01 User ID Standard
    ITS-BW-09-02 Identity Management
ITP-BW-11 External Connection Policy
ITP-BW-12 Guest Access Policy
    ITS-BW-12-01 Guest Network Terms and Conditions
ITP-BW-13 Wireless Access Policy
ITP-BW-26 Data Governance Policy

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

ITP-BW-21 Security Awareness Policy

Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

ITP-BW-01 Acceptable Use Policy
    ITS-BW-01-01 Log-On Banner Standard
    ITS-BW-01-02 Computer User Agreement Standard

Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

ITP-BW-20 Pen Testing

Configuration Management (CM): Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

ITP-BW-24 Asset Management Policy
ITP-BW-25 Configuration Management Policy

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

ITP-BW-08 Backup Policy

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

ITP-BW-02 Password Policy
ITS-BW-02-01 PassPhrase Standard

Incident Response (IR): Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

ITP-BW-10 Incident Response Policy
ITS-BW-10-01 Incident Response Standard

Maintenance (MA): Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

ITP-BW-18 Change Control Policy

Media Protection (MP): Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

ITP-BW-19 Media Disposal Policy

Physical and Environmental Protection (PE): Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

ITP-BW-17 Physical Security Policy

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

See the contents of this Document

Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and

transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

See HR policies as well as ITP-BW-16 Outsourcing Policy

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

ITP-BW-23 Risk Assessment Policy

System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

ITP-BW-06 Retention Policy
ITP-BW-16 Outsourcing Policy
    ITS-BW-16-01 Information Security Exhibit Standard

System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

ITP-BW-07 Email Policy
ITP-BW-15 Encryption Policy
ITP-BW-04 Data Classification Policy
    ITS-BW-04-01 Data Classification Standard
    ITS-BW-04-02 Data Dissemination Standard
    ITG-BW-04-01 Data Classification Guideline
ITP-BW-14 Network Security Monitoring Policy
ITP-BW-05 Mobile Device Policy

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

ITP-BW-22 Patch and Vulnerability Policy
    ITS-BW-22-01 Patch and Vulnerability Standard

11 Risk Assessment

A risk assessment is a process that determines what information resources exist that require protection and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. Because

economics, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Objectives must be established before administrators can identify and take the necessary steps to manage risks. Operations objectives relate to the effectiveness and efficiency of the operations, including performance and financial goals and safeguarding resources against loss. Financial reporting objectives pertain to the preparation of reliable published financial statements, including the prevention of fraudulent financial reporting. Compliance objectives pertain to laws and regulations which establish minimum standards of behavior.

The CISO, with the aid of other departments, will bi-annually conduct a risk assessment to:

- Understand and document the risks that may cause loss of confidentiality, integrity, or availability of information resources.
- Identify the level of security necessary for the protection of the resources.

The results of the bi-annual assessment will be reported to the IT Steering Committee and University leadership.

12 Definitions

Accountability	The state in which an individual or group is answerable and held accountable for their activities.
Acquisition	In the context of this document, gaining possession, through purchase or lease, of assets and/or services related to information technology, such as computer hardware, software, or services.
Accreditation	In information system security, the formal authorization for system operation and an explicit acceptance of risk given by the accrediting (management) official. It is usually supported by a review of the system, including its management, operational, and technical controls.
Audit	In IT, an independent, unbiased examination of an information system to verify that it is in compliance with its own rules; the process of collecting and evaluating evidence of an organization's security practices and operations in order to ensure that an information system safeguards the organization's assets, maintains data integrity and is operating effectively and efficiently to meet the organization's objectives.
Auditable event	A single-action (either a command or system call) that affects the security of an information system.
Backup	The process of backing up (copying onto electronic storage media) data that may then be used to restore the data to its original form after the occurrence of a data loss event or data file corruption. Two backup types are referenced in this document: • full – a complete backup of all data, whether or not changes have occurred. • incremental – a backup of only those files that have changed or been added since the last full or incremental backup was performed.

Baldwin Wallace University Information	The definitions of "Personally Identifiable Information", "Confidential Information", and "Baldwin Wallace University Information" can be found in Data Classification Policy ITP-BW-04 at http://bw.edu/ITPolicies
Confidential Information	The definitions of "Personally Identifiable Information", "Confidential Information", and "Baldwin Wallace University Information" can be found in Data Classification Policy ITP-BW-04 at http://bw.edu/ITPolicies
Corrective Maintenance	A form of system maintenance performed after a problem or failure is detected in an information system, with the goal of restoring operability or peak performance to the system.
Criticality	Degree of value.
Data Corruption	The result of errors in computer data that occur during electronic writing, reading, storage, transmission, or processing, that introduce unintended changes to the original data. Generally, when data corruption occurs, the file containing the data becomes inaccessible and/or unusable.
Data Integrity	The accuracy, completeness, and consistency of data stored in an information system, free from either accidental or deliberate, but unauthorized insertion, modification or destruction of data in a database.
Disaster	In the context of information systems, 1) an emergency or other event resulting in the destruction, theft, or corruption of data; 2) an inability to access an information system and/or its data for longer than a reasonable period, the duration of which is determined by the criticality of the system resources and data; 3) extensive damage inflicted on an information system, the availability of which is necessary for the maintenance of confidentiality, integrity, and availability of data required for the operation of an organization.
Disaster Recovery	The process, policies, and procedures preparing for recovery or continuation of the technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery includes planning for resumption of operating system and application software, data, hardware, and communications (networking).
Distributed system	An information system composed of multiple autonomous computers that communicate through a computer system.
FISMA	The Federal Information Security Management Act of 2002, which recognizes and addresses the importance of information security to the economic and national security interests of the United States. FISMA sets down information security requirements that must be followed by federal agencies, as well as any other parties, agencies or organizations

	collaborating with such agencies, in an effort to maximize their effectiveness in safeguarding information systems and the data contained within information systems.
Hacking	Detecting weaknesses in a computer or computer network. Hacking tools are programs designed to assist with hacking; these programs are often malicious and may be used to detect and exploit vulnerabilities in operating systems and/or user accounts.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, which sets national privacy standards for the protection of certain types of health information to the extent such information is electronically transmitted by health plans, health care clearinghouses, and health care providers.
Information system	An integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, communications, and digital products, support, and services.
IT	Information Technology
IT resources	All BW system computing facilities, equipment, hardware, software, data, systems, networks, and services that are used for the support of the teaching, research and administrative activities of the BW System
Maintenance window	The period of time designated in advance by a technical staff during which preventive maintenance that may cause disruption of service will be performed on an information system.
National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the U.S. Department of Commerce. The mission of the NIST is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life in the U.S.
Network/system topography	Describes the arrangement of systems on a computer system, defining how the computers, or nodes, within the system are arranged and connected to each other.
Non-technical controls	Management and operational controls such as security policies, operational procedures, and personnel, physical, and environmental security.
Personally Identifiable Information	The definitions of “Personally Identifiable Information”, “Confidential Information”, and “Baldwin Wallace University Information” can be found in Data Classification Policy ITP-BW-04 at http://bw.edu/ITPolicies
Preventive maintenance	A form of system maintenance conducted on a regular basis and intended to maintain and/or improve information system performance,

	avoid unplanned downtime, keep system software programs up-to-date, and prevent problems from occurring on an information system.
Protected data	Any data governed under federal or state regulatory or compliance requirements (such as FERPA or HIPAA), as well as data deemed critical to BW business and academic processes which, if compromised, may cause substantial harm and/or financial loss.
Residual risk	As it pertains to BW IT, any risk (vulnerability or exposure to loss or harm) that remains after mitigation of a risk or risks identified through the security risk assessment process.
Restricted data	Highly sensitive information intended for limited, specific use by individuals, workgroups, departments, or organizations with a legitimate "need to know." On BW System information systems, data stored digitally requires restrictions to its access and dissemination, as defined by federal or state law, or by BW policies and standards.
Risk	The probability that a particular vulnerability or vulnerabilities in the BW information system will be intentionally or unintentionally exploited by a threat which may result in the loss of confidentiality, integrity, or availability, along with the potential impact such a loss of confidentiality, integrity, or availability would have on BW operations, assets, or individuals.
Risk analysis	The process of identifying the most probable threats to BW information systems, revealing how frequently particular undesired events occur, and of determining the criticality, causes, and consequences of these threats and/or events.
Risk assessment	The overall process of risk analysis and risk evaluation and a key component of risk management that involves identifying and evaluating
Risk evaluation	The process used to determine priorities for risk management by comparing the level of risk against predetermined standards, target risk levels, or other criteria.
Risk management	The overall process for identifying, controlling, and mitigating security risks to information systems. BW System IT risk management comprises risk assessment, risk analysis, and treatment of risk, and includes the selection, implementation, testing, and evaluation of security controls.
Risk mitigation	The systematic reduction in the degree of exposure to a risk and/or the probability of its occurrence.
Security	In IT, the preservation of confidentiality, integrity, and availability of an information system and/or the data that resides on it.
Security authorization	The official management decision made by a senior organizational official to authorize the operation of an information system and to

	accept certain risks to organizational operations and assets, individuals, and other organizations based on the implementation of an agreed-upon set of security controls.
Security incident	Any computer or network-based activity that results (or may result) in misuse, damage, or loss of confidentiality, integrity or availability of an information system and/or the data that resides on it.
Sensitive data	Any data which, if compromised with respect to confidentiality, integrity, and/or availability, could have an adverse effect on the organization's interests, the conduct of its programs, or the privacy to which individuals are entitled.
Sensitivity	A measure of how freely data stored on an information system can be handled.
Software patch	An update that fixes bugs (errors, flaws, mistakes, failures, or faults), increases security or adds new features to a software program. A patch typically does not include substantial enough changes to warrant a new version or release of the entire program.
Software update	Modification to an existing version/release of a software program to develop or improve upon its features, function and/or performance without upgrading it to a new major version.
Software version upgrade	Replacement of a software program with a newer version of the same program in order to bring it up to date or to develop or improve upon its features, function and/or performance.
Storage area network	A dedicated system that provides access to consolidated, block-level data storage; a system with the primary purpose of transferring data between computer systems and storage elements.
ST&E	Security Test and Evaluation
System development life cycle (SDLC)	A conceptual model used in project management that describes the phases involved in an information system development project. A typical information system life cycle includes these phases Initiation – the system is described in terms of its purpose, mission, and configuration. Development and Acquisition – the system is constructed according to documented procedures and requirements Implementation and Installation – the system is installed and integrated with other applications, usually on a network. Operational and Maintenance – the system is operating and maintained according to its mission requirements. Disposal – the system's life cycle is complete; it is deactivated and removed from the network and active use.
System integrity	The state or quality of an information system when its intended functions are performed in an unimpaired manner, free from either

	intentional or accidental, but unauthorized manipulation, changes or disruptions.
System maintenance	The adjustment or modification of an information system to correct faults, improve performance, adapt to change in requirements, or changes in the system environment.
System management	The administration/oversight of a distributed computer system, which may include development, configuration, maintenance, and security and contingency planning.
Technical controls	Safeguards that are incorporated into computer hardware, software, or firmware, such as access control mechanisms, identification and authentication mechanisms, encryption methods, and intrusion detection software.
Threat	Any circumstance or event that has the potential to intentionally or unintentionally exploit a particular vulnerability in the BW Health information system, resulting in a loss of confidentiality, integrity, or availability.
BW	Baldwin Wallace
BW IT	BW Information Technology that provides support to BW Berea OH campus
BW Unit	BW campus or Department that provides IT services to its employees and/or students.
Vulnerability	A flaw or weakness in a BW information system security procedures, design, implementation, or internal controls that could be accidentally or intentionally triggered or exploited and result in a security breach or a violation of the system's security policy.