# Table of Contents

## Overview 3

## Scope of Program 3

## Program Officer 3

## Elements of the Program 4

## Applicability 5

## Responsibility 5

### Information Security
- Data Classification 6
- Password 7
- Access Authorization 7
- Security Monitoring 8
- Security Awareness Training 8
- Email Security 8
- Security Incident Response 9
- Use of Computing and Networking Resources 10

### Safe Computing
- Remote Access 10
- Workstation Security 11
- Server Authorization 11
- Use of Unlicensed Software 12
- Compliance with Copyright Laws for Text, Audio and Video 12
- Compliance with Copyright Laws for Software 12

## Adjustments to Program 13

## Annual Reporting 13
Overview

This document summarizes Widener University’s comprehensive written information security and compliance program (the “Program” or “Policy”) mandated by legislation, including but not limited to the Federal Trade Commission’s Safeguards Rule, the Gramm-Leach-Bliley Act (“GLBA”) and Payment Card Industry (PCI) compliance. In particular, this document describes the Program elements pursuant to which the University intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to employees, students, and prospective students. The Program is in addition to any university policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA. All prior electronic use, security and/or compliance policies, to the extent inconsistent with this Policy or Program, are hereby revoked and rescinded, effective immediately.

Scope of Program

The Program applies to any record containing nonpublic personally identifiable information about a student or other third party who has a relationship with the university, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the University or its affiliates. For these purposes, the term personally identifiable information shall mean any information (i) a student or other third party provides in order to obtain a service from the University, (ii) about a student or other third party resulting from any transaction with the University involving a service, or (iii) otherwise obtained about a student or other third party in connection with providing a service to that person.

Program Officer

The University’s Chief Information Officer is designated as the Program Officer who shall be responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the University to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer.
Elements of the Program

1. **Risk Identification and Assessment.** The University intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the University’s operations, including:

   - **Employee training and management.** The Program Officer will coordinate with the applicable representatives of the University to evaluate the effectiveness of the University’s procedures and practices relating to access and to use of student records. This evaluation will include assessing the effectiveness of the University’s current policies and procedures in this area.

   - **Information Systems and Information Processing and Disposal.** The Program Officer will coordinate the risks to nonpublic financial information associated with the University’s information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic personally identifiable information. The Program Officer will also coordinate the assessment of procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

   - **Detecting, Preventing and Responding to Attacks.** The Program Officer will coordinate the evaluation of procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies.

2. **Designing and Implementing Safeguards.** The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic personally identifiable information, whether in electronic, paper or other form. The Program Officer will, on a regular
basis, recommend to the Senior Vice President-Administration & Finance safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures. All Senior Leadership Team members, Deans, Assistant Deans, Assistant Vice Presidents, Associate Vice Presidents and Directors of the Widener University network are annually required to complete a risk questionnaire. The purpose of the Risk Questionnaire is to receive information about the current use of confidential data, as defined in this policy.

3. **Overseeing Service Providers.** The Program Officer shall coordinate with those responsible for the third party service procurement activities to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic personally identifiable information of students and other third parties to which they will have access. In addition, the Program Officer will work with the Senior Vice President-Administration & Finance to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate standards. Any deviation from these standard provisions will require the approval of the Senior Vice President- Administration & Finance.

**Applicability**

This policy is applicable to all users of the University network. The University network is defined as, but not limited to, telecommunications infrastructure, connected devices and services, wireless connectivity, computers and services. Each user plays a critical role in information protection. Users are defined as any faculty, support staff, administrative staff, employees, students, contractors, alumni, consultants, fellows and temporary employees.

**Responsibility**

All users are required to maintain compliance with all stated University policies. Any user activities deemed to cause harm, whether intentional or unintentional, to Widener University, the users of Widener University or to others outside of Widener University while using Widener University assets or network will be reported to the Senior Vice President-Administration & Finance, who will confer with the Program Officer and the applicable Vice President. Violations of
these policies can result in Human Resources sanctions for employees and disciplinary sanctions for students.

**Information Security**

The purpose of the information security section of this policy is to (1) ensure the protection of data, (2) ensure access to systems is authorized, (3) notify users of requirements for passwords, and (4) monitor for violations of university policy and/or local/state/federal laws and regulations.

**Data Classification**

All data receives a classification level to ensure logical and physical data protection. Any transmission, printing or extraction of information must adhere to the requirements of this section. The classification levels are as follows:

<table>
<thead>
<tr>
<th>Classification Level</th>
<th>Examples</th>
<th>Electronic Form</th>
<th>Print Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>SSN, Passwords, Credit Card Numbers</td>
<td>Must be encrypted when on the network and in electronic or physical data storage. Data must be protected with strong passwords. Data cannot be copied onto portable media without managerial consent (including laptops). Must not be posted on any website or sent through email.</td>
<td>Trash documents must be shredded. Retained documents must be stored in locked cabinets.</td>
</tr>
<tr>
<td>Restricted</td>
<td>Personally identifiable (combination of name, address, date of birth) student records, student grades, infrastructure design</td>
<td>Data must be protected with strong passwords. Data cannot be copied onto portable media without executive consent (including laptops).</td>
<td>Retained documents must be stored in locked cabinets.</td>
</tr>
<tr>
<td>Public</td>
<td>Not confidential or sensitive. Information on University website.</td>
<td>May be posted externally with appropriate approval (department head). May be sent through email.</td>
<td>Trash documents do not require shredding.</td>
</tr>
</tbody>
</table>
**Passwords**

Passwords must exist for all accounts on the Widener University logical network.

Passwords are not permitted to be shared for unique user accounts including both Widener University accounts and accounts provided to administration for communication with external entities on behalf of Widener University. Generic accounts require the sharing of passwords; however, only authorized personnel are permitted to receive the password to the account. Authorized personnel are determined, documented and communicated as defined in the Access Authorization process defined below.

Passwords are required to be changed in a defined timeline implemented and communicated by Information Technology Services. Upon the change of access or termination of an individual, passwords may be requested to be changed to protect access to information.

Passwords required for the continuity of key business functions of Administration and Finance as determined by the Senior Vice President of Administration and Finance may be shared. The sharing of the passwords will be documented as part of the Access authorization process below. Any password protection provided to users with respect to e-mail or voice mail is only given to prevent unauthorized users from accessing one’s communications.

**Access Authorization**

All user access must be authorized and users will be given access to computing resources through accounts. There are two types of accounts: user accounts and generic accounts. One user account will be defined for each user in the Widener University community. Shared access accounts will also be established for administration access, vendor access, and other external parties requiring access to the Widener University network and its resources. The use of shared accounts is authorized for only the users specifically defined and approved. The Information Security Office in Information Technology Services will monitor the access rights of each user.

Access to non-Widener University websites or forums as a requirement for authorized business purposes for Widener University, which includes the exchange of restricted or confidential data as defined in the Data Classification section of this policy will also be explicitly authorized as part of this process.
Security Monitoring

Information Technology Services will continually monitor all users of the Widener University network, including but not limited to users, students, faculty, staff, alumni and visitors. All communication in email, voicemail and other means will be subject to monitoring at all times for violations of university policy and/or local, state or federal laws and regulations.

Any devices determined to be involved in incidents will be inspected with the authorization of the Program Officer and the Senior Vice President-Administration & Finance. Any information on those assets is subject to removal.

Security Awareness Training

All staff and faculty of the Widener University network will receive formal training annually for security awareness. Formal training and annual assessment provides a knowledge level of awareness for the user community. The training will increase the awareness of threats and impacts to the University.

All staff and faculty of the university with access to the network are required to sign an annual agreement (Security Awareness Acknowledgement). The Acknowledgement demonstrates that the user is aware of and will adhere to the university policies and procedures.

Email Security

University email systems shall not be used for the creation or distribution of any non-academic related disruptive or offensive messages, including disparaging comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, or national origin or ancestry, gender identity, marital status, status as a veteran of the Vietnam era or other covered veteran, or any other protected class under federal, state or local law or the University’s Discrimination and Harassment Codes. Individuals who receive any emails with this content from any Widener University account should report the matter to their manager immediately. The manager should then notify the Program Officer. This requirement applies to faculty, support staff, administrative staff, employees, students, contractors, alumni, consultants, visitors and temporary employees who are provided email accounts at Widener University.

Mass electronic mailings from Widener University shall be approved by the Information Technology Services (ITS) Director of Customer Support and the
appropriate Vice President and only authorized accounts and individuals will be permitted to send mass electronic mailings.

Confidential and restricted information as defined in the Data Classification section of this policy is not permitted to be sent in an unencrypted email. Encryption of this information is required for any transmission of these data types, and the ITS Director of Customer Support can assist any user in the encryption of data.

**Security Incident Response**

The investigation of any network-related incidents must be approved by the Program Officer.

A network-related incident is including but not limited to

- any issue identified in security monitoring (as defined in the Security Monitoring section above),
- any issue identified in troubleshooting that impacted system or network performance,
- any issue identified in troubleshooting a user issue or reviewing a user’s machine,
- any issue reported to ITS by members of the user community,
- any issue reported to ITS by external parties including, but not limited to, local, state and federal law enforcement.

Individuals working on any security incident will be determined by the Program Officer and the details of security incidents are confidential until the investigation is completed. ITS can seize any logical and physical assets for inspection if determined to be a cause of a security incident. Based on the incident severity, law enforcement at local, state and/or federal levels may be contacted. The University shall provide notice of any breach or unauthorized access for any individual whose information was accessed or acquired as required by the Pennsylvania’s Breach of Personal Information Notification Act.

Security incidents will be investigated to determine root cause and a report will be made by the Program Officer to the Senior Vice President-Administration and Finance, who will then share it with the appropriate University personnel. All security incidents will be investigated using appropriate seizure rules and forensic measures as defined in the security incident response procedure.
Use of Widener University’s communications systems (including, without limitation, computing facilities, data contained on the University systems, servers, storage devices, or transmitted over the University’s networks, voice mail and all Widener.edu accounts), and access thereto by the University, outside enforcement authorities or other third parties, are subject to applicable federal and state laws. Use of the University’s computing and networking resources is limited to authorized University-related persons and University-related business only. While the University does not seek to monitor all traffic across its networks and through its equipment, it is possible that, while performing routine monitoring, the University may identify conduct that is inconsistent with or in violation of University policies. As a result, information on Widener computing equipment and accounts (even if deleted) can be subject to interception or retrieval by authorized University personnel, if necessary, as well as by outside enforcement authorities or other third parties, subject to proper legal process. The installation and/or use of software not expressly owned by the individual or granted for use to the University is strictly prohibited.

Safe Computing

Widener University has defined this section to ensure the safety and security of the information and the technology devices that support the University network.

Remote Access

Logical connections to the University for the use of internal non-email systems require the use of ITS approved configuration devices. Authorized users connecting remotely to Widener University are bound by the requirements defined in the Information Security section of this policy. The configuration and applications provided to users for access to Widener University remotely may only be installed on a Widener University issued laptop and may not be copied to any other device.

Authorization for remote access is part of the Access Authorization process as defined in this Policy.

Workstation Security

Any workstation computer or laptop used by administrative staff, support staff or faculty must be approved and configured by ITS.
All Widener University workstations and laptop computers will require anti-
virus software provided and monitored by ITS, power user account setup to limit
the impact of malware to the machines, and workstation security enhancements
including password protected screen savers, and user authentication to the asset
when not connected to the network.

Workstations required to continuously house confidential or restricted data will
be defined as critical hosts. Critical hosts must be administered by ITS or by
ITS approved vendors and any exceptions must be approved by the Senior Vice
President-Administration & Finance.

Server Authorization

ITS at Widener University will work with the University administration, faculty
and staff to identify and assess the security of servers on the University network.
Administration, faculty and staff with a need to add a server to the network will
apprise ITS of the content, function and users of the server. A server is defined
as any computer providing content to users.

A request for server access to the network will require the completion of the
Server Authorization Form and this request will be reviewed by ITS. Approved
servers will be assigned static ip addresses and network access to the server will
be restricted based on the business requirements. Security precautions are
necessary for the addition of all servers to the network to ensure the security of
the server content. Servers connected to the network will be evaluated on a
continuous basis as defined in the Security Monitoring section of this policy.

Servers housing confidential or restricted data as defined in the Data
Classification section of this policy will be defined as critical hosts. Critical
hosts must be administered by ITS or by ITS approved vendors.

Use of Unlicensed Software

All software installed on the University’s computer systems must be properly
licensed, either by the University or by the individual user. The University will
monitor its computer systems to ensure that unlicensed software is not installed
on its computers. Individuals who install software on their office computers
must keep records to show that this software is properly licensed, and they must
inform ITS in writing that the software has been installed.
Compliance with Copyright Laws for Text, Audio and Video

Nearly all written, audio and video material is protected by copyright laws, regardless of whether it is in a hard copy, in an electronic copy, or on the Internet. The exceptions to this rule are so few that users of the University’s technology should assume that all written audio and video materials in hard copy or available through the Internet are protected by copyright laws, including The Digital Millennium Copyright Act of 1998, unless there is clear information to the contrary. Simply stated, the copyright laws allow a user to read the copyrighted material. The copyright laws do not allow a user to modify a copyrighted work, make copies of it (beyond those allowed by fair use), distribute copies of a work through the Internet, or broadcast a copy of work (such as in the case of video) on any channel or network. As with materials from a library or other sources, the user is responsible for using materials obtained off the Internet in compliance with the copyright laws.

Compliance with Copyright Laws for Software

Nearly all computer software is protected by the copyright laws. The exceptions to this rule are so few that users of the University’s technology should assume that all software on the Widener computer system, on third party systems, or available through the Internet is protected by copyright, unless there is clear information to the contrary. Simply stated, the copyright laws allow a user of software to use the software, load it onto the hard drive of a computer, and retain the original disk as an archive copy. The copyright laws do not allow a user to modify the software, make more copies of it, store copies on both a home and a campus computer, or distribute the software through the Internet, unless the license agreement permits those activities. Unless a user of the Widener computer systems knows that any of those activities is permitted by the applicable license agreement, users of the University’s computer systems shall not copy any software, modify any software, load copies of it onto a network or on multiple hard drives, or distribute the software in any way, including through the Internet.

Adjustments to Program

The Program Officer is responsible for evaluating and recommending changes to the Program to the Senior Vice President-Administration & Finance, based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the University’s operations or other circumstances that may have a material impact on the Program. The Program may be amended at any time in the sole discretion of the University.
Annual Compliance Reporting

The Program Officer will annually report the status of the overall policy compliance of the University to the Senior Vice President-Administration & Finance, who will share the report with the President and the appropriate committees of the Board of Trustees.