INFORMATION SECURITY PRIVACY STATEMENT

Overview

The Winthrop University Information Security Office works to ensure the confidentiality, integrity and availability of University data and resources as well as to protect it from unauthorized disclosure, alternation and/or destruction.

The Information Security (InfoSec) Office duties include but are not limited to:

- Conducting investigations into information security and data privacy incidents
- Auditing processes and procedures to ensure information security policies and best practices are being followed
- Evaluating potential purchases that have an information security component
- Managing information security training

The InfoSec office also serves as the liaison between the campus and various state agencies in reference to information security and privacy matters.

What information do we collect?

In the process of executing InfoSec duties, this office may collect data including, but not limited to: Full name, University affiliation (student, faculty, staff, vendor, visitor, etc), home/local address, phone number(s), email address, supervisor name and contact information, computer and/or phone information (model, operating system, software, etc), specific details on a given incident, how is data stored, how is data transmitted, who has access and what level of access, potential software purchases and uses, who has physical access/keys to an area.

Only the information needed for a given task is gathered.

This information can be collected via paper forms, emails, phone and/or face-to-face communications.

How do we use your information?

The information gather by this office is used in various ways. Some, but not all, of the possible uses are:

- Incident response – How to stop unauthorized disclosure, alternation and/or destruction of information and prevent further incidents
- Procedure changes – Determining if there is a better, more secure method to handle data
- Software evaluation – Looking at potential software purchase to ensure data is handled securely and meets information security standards

How do we protect your information?

Student data is protected by the Family Educational Rights and Privacy Act of 1974 (FERPA). With few exceptions, the University cannot disclose any non-directory student information to anyone other than the student unless the student has given specific written consent.

Documents and information collected are stored in locked offices in the case of paper files and on secure storage systems in the case of digital files.

Any data that needs to be transferred to other parties is done so using secure methods such as encrypted emails, secure file transfers, encrypted USB drives, etc.

Can information be corrected?

Our Office works closely with all parties regarding appropriate data entries. If you have any questions, or objections regarding the validity of your data, please contact our office as soon as possible if you believe there is an issue.

Information shared with outside parties

Information obtained in the InfoSec office may be shared with specific areas depending on the nature of the information. Information Security and Privacy Incidents are shared with the department management in which the incident occurred, the Risk Management office and also, depending on the nature of the incident, with the South Caroline State Department of Information Security or other appropriate entities. If there is a technology solution to help mitigate the incident, then anonymized incident information may be shared with the Information Technology department. In the event that an incident is deemed to be a criminal act, appropriate law enforcement agencies will be contacted.

Third party links

Occasionally, at our discretion, we may include links to third party sites on our website. Please be aware that we have no control, responsibility, or liability for the content and activities of these linked sites. These third party sites have separate and independent privacy statements and we encourage our users to be informed and aware and to read the privacy statements of any other site that collects your personal information. However, we continually seek to protect the integrity of our site and welcome any comments for improvements, including any links to third party sites.

Compliance with the other jurisdictional privacy regulations

Other states or countries may have privacy regulations which serve to protect their citizens. For example, the European Union General Data Protection Regulation (GDPR) is a European Union (EU) legal framework for data privacy and security of personal data for individuals within the EU. The GDPR sets forth obligations for organizations that collect, use, share, and store personal data of constituents who reside in the European Union.

Students, or potential students have created a contractual need with Winthrop University to collect and retain certain data at the time of submitting an application for enrollment. Personal information is be required by the University as an essential part of the academic process and must be retained per legal requirements.

For non-students, Winthrop University is committed to securing the appropriate consent (opt-in) in the collection and processing of personal data. If you have any questions, or objections to the collection, use and retention of your personal data, on legitimate grounds, Winthrop University shall consider all requirements of notice, choice, transfer, security, data integrity, and access. Please direct any questions you may have concerning Winthrop University's obligations and compliance with GDPR to privacy@winthrop.edu.

How long do we keep your information?

Personal data will be retained in this office in accordance with applicable federal and state laws, regulations, and accreditation guidelines, as well as University policies. Personal data will be destroyed when no longer required for University services and programs, upon request or after the expiration of any applicable retention period, whichever is later. GDPR, or other jurisdiction privacy regulations, do not supersede legal requirements that Student Financial Services maintain certain data.

Your Consent

By utilizing Winthrop University-owned resources, you have created a contractual need that requires the sharing of required personal information. Your consent was established at the time of usage.

Changes to this Privacy Statement and University Policy.

Any changes to this policy will be posted to this website and the date noted at the bottom. Winthrop University policies, including our University Privacy Policy, may be found in the Winthrop University Policy Repository.

Last updated: January 21, 2020

Contact Information:

If you have any questions regarding this statement please contact:

Information Security Office
infosec@winthrop.edu