RISK MANAGEMENT
PRIVACY STATEMENT

Overview

The Office of Risk Management is a vital part of the university and functions in accordance with the policies established by the president and the Board of Trustees. The director reports directly to the University President. The office is guided by the Winthrop University Mission Statement in that it supports the function of the University to provide and preserve its financial resources. These resources are necessary for the continued recruitment and education of the best students, and for the continued recruitment and employment of, and support for a nationally recognized faculty and staff. The organizational status and the support accorded to the director by executive management and staff are major determinants of the scope and value of the Risk Management function to the University.

The office provides independent, objective assurance, and consulting services designed to add value and improve Winthrop University's operations. Its purpose is to evaluate and improve the effectiveness of risk management, control, and governance processes as support to the President and his management team to assist them in accomplishing their objectives.
The office is responsible for providing executive management with information about the adequacy and effectiveness of the university's system of internal administrative and accounting controls and the quality of operating performance when compared with established standards.

The Office of Risk Management also houses Information Security, and General Counsel. Each of those areas have separate privacy statements located at: https://www.winthrop.edu/InfoSec and legal (Coming Soon)

What information do we collect?

In performance of our mission, we sometimes review business or academic areas of the university that house sensitive information. All protected information collected is from another business or academic area of the university and not directly from the individual who submitted information to the University.

Sometimes in the performance of audit duties, survey data may be collected. Any survey data is aggregated and no personal identifiers are retained with the data.

How do we use information collected?

We may collect some of that information in order to determine if effective controls are in place, or to provide objective assurance to senior leadership that data or finances are being properly reported.

How do we protect information?

We take precautions to protect any sensitive information both online and offline. Only employees who need the information to perform a specific job (for example, audit of a specific business unit) are granted access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment. We only collect the information needed for our reviews and keep that information for only as long as it is needed and in accordance with state document retention guidelines.

Can information be corrected?

All audits are sent to business unit managers for review in draft (confidential) form. Auditees have a chance to review the audit and make comments or corrections before the final document is published. Audit reports only contain aggregate or redacted information and no personally identifiable information is published in a final report.

Information shared with outside parties

Our office may share audit reports and data, upon request, by state oversight agencies who are granted access by statute to university records.

In the event of an allegation, or the discovery of, potential criminal misconduct, or fraud, our office will contact the appropriate investigative agency to conduct further criminal investigation and coordinate the access to appropriate university records to assure a proper chain of custody and cooperation with law enforcement agencies.

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

All protected information collected is from another business or academic area of the university and not directly from the individual who submitted information to the University. Any consent would have been granted to the data owner where the information was originally submitted.

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:

Please send any questions, comments, or feedback to: overcashc@winthrop.edu