-->

Email and Content Access Standard

Last Modified on 08/11/2025 4:40 pm EDT

Table of Contents

For more details about the Information Security Office, **please visit our website**!

1. Introduction

The Wharton School adopts this E-mail and Content Access Standard (this Standard) to protect the confidentiality, integrity, and availability of e-mail and document content stored in personal environments for systems managed by Wharton (e.g. Active Role Server, Microsoft 0365, Gmail, DropBox, Box, GDrive, etc.). This standard ensures compliance with the University's Policy on Privacy in the Electronic Environment, Acceptable Use Policy, and all applicable University and Wharton policies, standards, and guidelines which serves as the overarching framework.

The standard enables Wharton to support security incidents/investigations, technical support, legal compliance/e-discovery, HR, or policy violations, etc.

This standard is a living document that is reviewed and updated yearly to adapt to the evolving Wharton mission, technology advancements, and cybersecurity requirements.

1.1 E-mail & Content Access Standard Maintenance

The Wharton Information Security Office (ISO) is accountable for the development and maintenance of this standard and ensuring tactical and operational implementations that align to and meet the directives established therein.

1.2 Scope

This Standard applies to all Wharton faculty, staff, departments, centers, and third-party affiliates authorized to access institutional data and IT systems   This standard's scope relates to work e-mails, storage folders, end point devices, and applications. This standard aligns with the Identity Access & Management Standard, Data Management Standard, and other Wharton/Penn policies and standards, which govern wider activities throughout Wharton.

1.3 Compliance

All Wharton employees must follow this standard. ISO responsible will review this standard annually and update based on changes to Wharton’s varied operational IT environments and alignment with Wharton’s mission. ISO will communicate updates to the relevant stakeholders in a timely manner.

⍰Top

2. Audit

Wharton is required to review privileged IT access on a quarterly basis for the aforementioned IT systems.

Information Security Office will audit the process and access logs at least annually, and on a more frequent basis as appropriate, to ensure compliance with the standard and aligning with the process. The Information Security Office itself is also subject to compliance audits, as warranted.

All actions taken by Wharton should be documented/logged with timestamps and detailed descriptions of what was accessed, modified, or investigated.

⍰Top

3. Training and Awareness

All staff authorized with privileged access to the aforementioned e-mail or content systems are required to review and acknowledge this standard, the University's Policy on Privacy in the Electronic Environment, Acceptable Use Policy, and all applicable University and Wharton policies, standards, and guidelines.

⍰Top

4. Violations

Employees who fail to adhere to the guidelines and process set forth in this standard document may be subject to further employment action, up to and including termination. The Wharton School recognizes that deviation from this standard may vary in severity, ranging from minor departures from process to serious breaches that involve gross misuse or abuse of authority or resources. Each case will be reviewed individually, and in light of the specific circumstances, to determine the appropriate response, which may include no formal action, a verbal reminder, or more serious disciplinary consequences, up to and including termination.

⍰Top

5. Process Scope

The E-mail & Content Access Process aligns with Wharton’s E-mail & Content Access Standard. The purpose of the process is to identify responsible and accountable Wharton Computing teams and the specific process steps necessary to fulfill requests to access and conduct actions within e-mail and content storage systems. The process enables Wharton Computing to support security incidents/investigations, technical support, legal compliance/e-discovery, HR, etc.

Click here for details on the **internal Wharton process** (log-in required).