

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student All people with UC email accounts</p>	<p>Policy Title: Email Retention on Central Servers</p> <p>Effective Date: 9/18/2009</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 27001/17799, COBIT 4.0, GLB, UC Policy, HIPAA, FERPA, PCI, FIA</p>	<p>Policy Number: 9.1.37</p> <p>Policy Owner: AVP, Information Security Chief Information Officer</p> <p>Responsible Office(s): UCit E-Mail Services Information Security</p>
---	---	---

Background

Certain federal regulations and international standards require organizations to (1) establish policy establishing the retention of the contents of email accounts provided by that organization and (2) to abide by that policy.

This policy provides the retention schedule for email on UCit central servers.

Policy

Exchange Email

MS Exchange is currently used to host employee email. For disaster recovery purposes, a full backup of the entire MS Exchange database is made each day and retained for a period of thirty (30) days.

Employee email is, by this mechanism, retained by UCit on central systems for a period of 30 days. The backups are deleted from those central systems after 30 days.

Email accounts of employees who separate from the University are retained for 6 months from the day their status changes in the HR system or the day that the Email team processes a manual account removal request.

UConnect Email

UConnect is currently used to host student email. It is running on Microsoft's Live@edu service. Per the user agreement with Microsoft, deleted emails can be recovered for a period of fourteen (14) days. This system does not support single mailbox recovery.

Email retention based on content

Depending on the content of any given email, other retention requirements may apply. It is the responsibility of the user to understand and comply with these requirements. Details may be found in policy 9.1.8

Audience

This policy applies to all organizations and individuals associated with the University of Cincinnati.

Procedure

ISO 27001/17799	International Standards Organization for Information Security
COBIT 4.0	ISACA Audit Controls Objective for IT
GLB	Gramm-Leach-Bliley Act
UC Policy	General Policy on the Use of Information Technology
UC Policy	Information Technology Management Policy
UC Policy	Information Security Policies
UC Policy	General UC Archive Policies
HIPAA	Health Insurance Portability and Accountability Act
FERPA	Family Educational Rights and Privacy Act
PCI	Payment Card Industry
FIA	Freedom of Information Act

Related links

- [International Standards Organization 17799:2005](#)
- [Control Objectives for IT](#)
- [Gramm-Leach-Bliley Act](#)
- [UC Policy - General Policy on the Use of Information Technology](#)
- [UC Policy - Information Technology Management Policy](#)
- [UC Policy - Information Security Policies](#)
- [Health Insurance Portability and Accountability Act](#)
- [The Family Educational Rights and Privacy Act](#)

Phone Contacts:

UC Information Security	558-ISEC
AVP, Information Security	556-9177
UC Office of the CIO	556-2228

Disciplinary Actions:

Violation of this policy may result in revocation of network access for the effected system(s).

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants and dismissal for interns and volunteers. Additionally, individuals

are subject to loss of University of Cincinnati Information Resources, access privileges, civil, and in some cases criminal prosecution.

DRAFT