

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> Employee Verification</p> <p>Effective Date: 01/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 27001/17799, COBIT, GLB, UC Policy, HIPAA, FERPA, PCI</p>	<p><i>Policy Number:</i> 9.1.9</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	--	--

Background

There are a variety of reasons that organizations outside of the University of Cincinnati may need to verify that a particular person either is currently or has in the past been an employee of UC.

Due to legal and regulatory requirements, the release of this information must follow specific guidelines and processes. If person information about employment is released outside of these processes, the University may be held liable.

Policy

- Any and all questions of employment must be forwarded to the Human Resources department.
- No persons outside of Human Resources should share employment information about another person regardless of whether the person is a current or past employee
- Human Resources is responsible for maintaining the process for release of employment information in a manner that the legal requirements surrounding the release of such information are met.
- If the question is about the employment at another company of a co-op student, contractor, or affiliate, the requestor should be asked to send that question to the other company. UC should not support “second hand” verification.

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

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	8-ISEC
Director, Information Security	6-9177
UC Office of the CIO	6-2228

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.