

 <p><b>Category:</b> Information Technology</p> <p><b>Policy applicable for:</b> Faculty/Staff/Student</p>	<p><i>Policy Title:</i> <b>UC InfoSec Trusted Entity Policy</b></p> <p><b>Effective Date:</b> 01/04/2008</p> <p><b>Prior Effective Date:</b> N/A</p> <p><b>Enabling Acts:</b> ISO 27001/17799, COBIT, GLB, HIPAA, FERPA, PCI</p>	<p><i>Policy Number:</i> <b>9.1.20</b></p> <p><b>Policy Owner:</b> Director, Information Security</p> <p><b>Responsible Office(s):</b> Information Security</p>
---	--	---

## Background

Operation of various departments and processes at the University of Cincinnati require that trust be granted to certain individuals. For example, the UC computer network requires people with a high level of knowledge and highly privileged access in order to setup and maintain the system. It is important that the University do its due diligence when providing physical and logical access to UC sensitive data.

## Policy

Positions with Privileged Access to information or systems at the University of Cincinnati or positions that come in contact with sensitive information will be staffed by Trusted Entities.

To establish a person as a Trusted Entity, the following must be completed:

- A Background Check is to be completed by the subject.
  - This will require that the person present themselves UC Public Safety with two forms of picture ID to provide their fingerprints.
- The completed forms are to be submitted to the local HR representative for review and processing.
- To be designated a Trusted Entity the background check must come back clear of any felony convictions.
- All certifications and degrees provided in the subject's application or resume must be confirmed. This step is completed by the subject's local HR representative and recorded in the Trusted Entity package.
- Employers for the past 7 years must be contacted and employment confirmed. This is done by the subject's local UC HR representative and results are recorded in the Trusted Entity package.
- The person must be a UC employee or work for a 3rd party provider who provides all the data checks required for a person to obtain the Trusted Entity label. (Background checks that show no Felony Convictions, degree and employment verification)
- The completed package is presented to the department's Dean or VP for review and approval.
- The completed Trusted Entity package is retained by the employee's or contractor's local UC HR representative.

## Audience:

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

## Definitions:

**Privileged Access:** enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network.

**Highly Restricted Information:** See Appendix A

**Procedure:**

<b>ISO 27001/17799</b>	International Standards Organization for Information Security
<b>COBIT 4.0</b>	ISACA Audit Controls Objective for IT
<b>GLB</b>	Gramm-Leach-Bliley Act
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>FERPA</b>	Family Educational Rights and Privacy Act
<b>PCI</b>	Payment Card Industry

**Related links:**

- [International Standards Organization 17799:2005](#)
- [Control Objectives for IT](#)
- [Gramm-Leach-Bliley Act](#)
- [Health Insurance Portability and Accountability Act](#)
- [The Family Educational Rights and Privacy Act](#)
- [Payment Card Industry](#)

**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.

**Appendix A:**



InfoSec Data  
Classification Guid