

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> System Level Account Policy</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, Federal Corrupt Practices Act of 1977, Federal Computer Security Act of 1987</p>	<p><i>Policy Number:</i> 9.1.19</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	--	---

Background

This policy applies to system-level accounts which are delivered with a system (default accounts), such as root, super user, or administrator and to system-level accounts that are created by UC system administrators. These types of accounts typically have full access to a system or a group of systems and the data that resides on those systems.

Policy

- The delivered system-level account name must be changed prior to putting a system into production. This means the name of the account must be changed to something not recognized as a default system level account.
- The description of the system-level account must be changed or removed to make it undetectable as the default system-level account.
- A false system-level account should be created, such as a false “administrator” account. This account must have no privileges and may even be disabled.
- The system-level account must be password protected with a strong password.
- The password for a system-level account must be changed every 60 days at a minimum.
- The system-level account and corresponding password may not be known by more than one system administrator and one backup.
- No user may access a system-level account unless authorized to do so.
- Access to system-level accounts may not be used to damage a system, obtain extra resources, take resources from another user or to gain access to systems or use other systems for which proper authorization has not been given.

Audience:

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

Definitions:

System-Level Account: Accounts including, but not limited to, root and administrator, which allow full system access with no tracking.

Root User: The UNIX superuser account that overrides file permissions. By extension, the privileged system-maintenance login on any operating system. This account ignores permission bits. This is an account with unlimited access privileges that can perform any and all operations on the computer.

Superuser: A special UNIX privilege level, with unlimited access to all files, directories, and commands. The superuser’s login name is usually root.

Administrator: All Microsoft Windows systems have a local Administrator account, usually called “Administrator”. This account has elevated privileges (super user) access. This account allows the

user to make system wide changes to the computer, install programs, and access all files on the computer. This account has full access to other user accounts on the computer. This user:

- Can create and delete user accounts on the computer
- Can create account passwords for other user accounts on the computer
- Can change other people's account names, pictures, passwords, and account types

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
HIPAA	Health Insurance Portability and Accountability Act
FERPA	Family Educational Rights and Privacy Act
PCI	Payment Card Industry
Federal Computer Security Act of 1987	Security and Privacy of Sensitive Information
Federal Corrupt Practices Act of 1977	Accounting Transparency Requirement under the Securities Exchange Act of 1934

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](#)
- [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.

DRAFT