UNIVERSITY OF CENTRAL FLORIDA
Office of the President

SUBJECT: Enterprise Directory Governance	**Effective Date:** 2/1/2018	**Policy Number:** 4-017
	Supersedes:	**Page** 1 of 5
	Responsible Authority: Vice President for Information Technologies & Resources and Chief Information Officer	

APPLICABILITY/ACCOUNTABILITY

This policy applies to all members of the university community, including all full-time and part-time personnel, student workers, and all persons paid by or through the university such as contractors, consultants, and employees of direct support organizations.

BACKGROUND

Enterprise Directory Governance provides a framework for using directory services, such as authentication, authorization, auditing, and identity lifecycles to securely manage access to resources and university information assets. Inadequate governance of directory services may result in unauthorized collection, modification, deletion, disclosure, or misuse of university information assets, thus potentially compromising the mission of the university, compromising information security, violating individuals' rights to privacy, or non-compliance with state or federal regulations. The intent of this policy is to improve information security, mitigate the risk of unauthorized data access, and optimally govern directory and identity management services.

POLICY STATEMENT

The UCF Enterprise Directory service holds identities and security groups for members of the university community, and provides access by authorized individuals to university

information assets based on job duties and responsibilities. Individuals working for or on behalf of the university who create, view, or manage the directory services are responsible for implementing appropriate managerial, operational, physical, and technical controls. Controls must be implemented in compliance with the standards and procedures set forth by the Enterprise Directory Governance Committee for the access to, use of, transmission of, storage of, and decommissioning of directory information.

Any violation of this policy may result in immediate loss of network and computer access privileges, seizure of equipment, or removal of inappropriate information posted on university-owned computers or university-supported internet sites. In addition to these corrective actions, failure to comply with this policy and procedures may result in disciplinary action up to and including termination.

DEFINITIONS

Credentials. A combination of user name, password, and possibly additional information or key such as a PIN, biometric scan, or app that together are used to authorize access to a computer system or information resource.

Data. Alphanumeric or other information represented either in a physical or digital form suitable for electronic processing or storage.

Directory Service. A distributed repository that provides identification and authentication data as well as an infrastructure for locating, managing, administering, and organizing network resources.

Distributed Directory. Any university directory service other than the Enterprise Directory.

Enterprise Directory. A centrally-administered database containing data used to control identity and access management.

Family Educational Rights and Privacy Act of 1974 (FERPA) also known as the Buckley Amendment. A federal law that protects the privacy of student academic records.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a federal law that protects the security of individually-identifiable health information.

Identity and Access Management (IAM). An integrated system of policies, business processes, and technologies that enable UCF to both facilitate and control user access to IT resources and applications. IAM incorporates the process of identifying individuals in a system such as a computer or network and controlling their access to resources within that

system by associating user rights and restrictions with a person's established identity. Credentials that uniquely identify one and only one person represent an identity.

Institutional Data. All data created, collected, maintained, recorded, or managed by the university, its staff, and agents working on its behalf, in the course of conducting university business.

Resource Owner. An owner of a resource or application that consumes directory services.

Restricted Data. Any confidential or personal data that are protected by law or policy and that require the highest level of access control and security protection while in storage or in transit.

Unrestricted Data. Data that are not protected by law or contract, and the disclosure of which would cause no harm to the university or to the affected parties. Examples of unrestricted data include employee names, dates of hire, rate of pay, title, office address or phone number. Student names, years, majors, or other directory information not blocked by a student within the scope of FERPA, can be considered unrestricted data.

ENTERPRISE DIRECTORY GOVERNANCE COMMITTEE RESPONSIBILITIES

The Enterprise Directory Governance Committee, formed by UCF IT, includes stakeholders from across the campus community. The committee's mission is to:

- Govern all directory services across the institution
- Develop procedures to review proposed directory service use cases
- Recommend changes and improvements to university directory services
- Govern a standardized directory structure that meets university policies, standards, and regulatory requirements
- Establish procedures to review and audit adherence to account and authorization standards and practices
- Minimize the use of redundant directory services across the university

UCF IT RESPONSIBILITIES

UCF IT shall establish, administer, and maintain the Enterprise Directory, including:

- Establish business processes to manage the Enterprise Directory
- Maintain the technical infrastructure necessary to operate the Enterprise Directory
- Implement Enterprise Directory Governance Committee standards and recommendations

PROCEDURES

- All applications that require user authentication, where technically feasible, must first consider an Enterprise Directory approach for authentication, authorization, accounting and auditing purposes
- Resource owners are responsible for adhering to the policies, procedures, and standards set forth by this document and the Enterprise Directory Governance Committee
    - Resource owners seeking to propose Enterprise Directory architecture changes or modify services (e.g., implement or change current services) that depend on the enterprise directory shall work through the Enterprise Directory Governance Committee
    - Resource owners of distributed directories shall work through the Enterprise Directory Governance Committee to obtain approval for any architectural, business process, or regulatory changes that affect the directory
- Any exceptions to the use of the Enterprise Directory shall be reviewed and approved by the Enterprise Directory Governance Committee
    - All distributed directories are subject to the same policies, procedures, and standards that apply to the Enterprise Directory

RELATED DOCUMENTS

2.100.5 *Florida Public Records Act—Scope and Compliance* policy
http://policies.ucf.edu/documents/2-100.5FloridaPublicRecordsActScopeAndCompliance.pdf

4-007.1 *Security of Mobile Computing, Data Storage, and Communication Devices* policy
http://policies.ucf.edu/documents/4-007.1SecurityOfMobileDevices.pdf

4-008.1 *Data Classification and Protection Policy*
http://policies.ucf.edu/documents/4-008.1DataClassificationAndProtection.pdf

4-002.2 *Use of Information Technologies & Resources Policy*
http://policies.ucf.edu/documents/4-002.2UseOfInformationTechnologiesAndResources.pdf

4-209 *Export Control Policy*
http://policies.ucf.edu/documents/4-209ExportControlPolicy.pdf

Records retention schedule:
http://dos.myflorida.com/media/693588/gs05.pdf

UCF password standards:
http://www.cst.ucf.edu/wp-content/uploads/501-101-Password-Standards.pdf

Florida Information Protection Act of 2014:
http://www.flsenate.gov/Session/Bill/2014/1524/BillText/er/PDF

CONTACTS
UCF Chief Information Security Officer, 407-823-3863

INITIATING AUTHORITY
Vice President for Information Technologies & Resources and Chief Information Officer

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-017

Initiating Authority: Joel L. Hartman Date: 1-31-18

University Policies and Procedures Committee Chair: Rhonda L Bishop Date: 1/29/2018

President or Designee: John C. Hitt Date: 2/1/18