***This old UMB job description was created between 2000 and 2014 and is being provided as a template or guide in the preparation of a current job description. The essential functions are general in nature and may not accurately depict the duties of a specific unit. Managers are encourage to update and provide specific duties that are applicable to work being performed in the unit.***

Job Title: **Assistant Director, Identity Management & System Integration Planning**

Job Family: Information Technology

Sub Family: IT - Security Identity

**Job Summary:**

Responsible for the day-to-day administration of identity and access management initiatives for the campus. Collaborate with the Director and other IT staff to ensure multiple system security and integrity. Identify user identities within a network and/or an enterprise system and creates controls for accessing resources by associating user rights and restrictions with the established unique identities.

**Essential Functions:**

* Oversee administrative functions of identity and access management.
* Partner with upper level administrators to identify and evaluate complex business and technology risks, internal controls which mitigate risks, and relate opportunities for internal control improvement.
* Assist in designing and maintaining campus directory(s). Develop basic risk management approaches, and expand information technology management processes. Assist in develop policies and procedures for security of systems.
* Execute advanced services and supervise staff in delivering basic services.
* Assist in the selection and tailoring of approaches, methods and tools to support service offering or industry projects.
* Manage the use of technology-based tools or methodologies to review, design and/or implement products and services.
* Assist in maintaining mentoring relationships within identity management and systems integration practice.
* Represent the department by participating in campus discussions and meetings; communicate a broad range of University services; manage engagements including preparing concise, accurate documents and balancing project management with the occurrence of unan
* Performs other duties as assigned.

**Minimum Qualifications**

Education: Bachelors in Information Technology, Cybersecurity, Computer Science, Systems Administration, Computer Engineering or a related field.

Experience: Five (5) years experience with identity management developing identity management strategies, architectures, and implementation plans integrating identity and access management into infrastructure and applications

Supervisory: One (1) year of direct supervision or responsibility for training, work coordina tion, and monitoring the work of others

Licensure/Certification:

Other: No subsitution of experience for minimum education requirement.

**Knowledge, Skills, and Abilities**

*Managers may provide prefered knowledge, skills, and abilities as necessary.*

Job Code: E0771I

SOC Code: 113021 IPEDS: Computer

EEO6 Code: Executive/Admin/Managerial State Code: 9445011

USM eCode: E2407E AAP Code: 1C