

|  |  |
| --- | --- |
| **Job Title:** *The formal title of the position*  **Identity and Integration Analyst** | **FLSA Classification:** *(FLSA Federal Law GUIDELINES)*  xExempt ☐Nonexempt |
| **Reports to:** *Title of the position that the job incumbent reports to* | **Location:**  **SEU Main Campus (or remote)** |
| **Department: Enterprise Information Systems** | **Division: Office of Information Technology** |
| **Employment Category:**  xFull-Time ☐ Part-Time | **Paygrade:** |

**PRIMARY PURPOSE OF POSITION**

The Identity and Integration Analyst works within the university’s Identity and Access Management (IAM) framework to ensure the university successfully manages access to critical information and systems within the organization. The person in this position will **analyze the identity life cycle, articulate access requirements and define enterprise identity records** using a full set of IAM competencies and skills to design, deploy, and support systems that verify appropriate user privileges and manage credentials for accessing our most valuable assets.

**ESSENTIAL DUTIES AND RESPONSIBILITIES**

**Identity Management Responsibilities**

* Manage identities across platforms serving as the area expert
* Deliver a variety of technical work across Okta, SSO (SAML and CAS protocols), and the identity system of record (Banner) including use/development of Okta Workflows, Banner Enterprise Identity Service (BEIS), and custom scripts
* Attend to the identity management lifecycle and optimization using Okta flows and custom scripts
* Advance the university’s IAM offerings by implementing new functionality such as password-less authentication
* Resolve major incidents and any minor issues escalated to EIS related to IAM
* Document and understand flow of data from source system(s) to identity manager as well as the university’s identity architecture

**Access Management Responsibilities**

* Work with business stakeholders as well as product owner(s) to capture IAM use cases and define IAM processes
* Deliver an access architecture/philosophy that focuses on data access rather than application access
* Continually assess both user provisioning and user access/permissions to software and systems to ensure standard, effective processes are in place
* Document and understand flow of data from identity manager to target applications

**Integration Management Responsibilities**

* Integrate university software and systems using standard tools such as API’s, native functionality available in identity management software/platform, or integration platform software ensuring standard and consistent identity lifecycle management
* Assist in the development of a rubric or flowchart to establish when to use identity management software for integrations versus other source databases/software

**Technical and Problem-Solving Responsibilities**

* Serve as the technical authority and champion for all services managed by the Identity and Access team.
* Conduct analysis of user and permission data, and the development of test cases for applications, file shares and other identified entitlements repositories that have been re-permissioned
* Foster a practice of collaboration and continuous improvement within the Identity and Access areas
* Demonstrate excellent Identity and Access troubleshooting skills and knowledge of problem resolution methodologies and root cause analysis
* Participate in IT operational planning and execution as well as policy, procedure and standards development
* Demonstrate expertise in the Identity and access field and recommend changes to our identity platform and ecosystem as the field changes and as best practice dictates
* Use standard tools for managing and communicating work
* Demonstrate knowledge of technical trends in IT security and risk management to include security and risk control frameworks - especially as related to Identity and Access Management
* Analyze and document functional and nonfunctional requirements for various IAM domains (identity lifecycle management, access management, integration management, privileged access management, reporting and analytics)
* Write test cases, regression test, and ensure that upgrades to cloud or on-premise software do not negatively impact campus identity operations

**QUALIFICATIONS**

* Bachelor’s degree in computer science or related field
* 2 years of experience with any IAM product and/or identity and access management job responsibilities
* Strong technical skills – especially in programming (groovy or Java, preferred) and technical in troubleshooting
* *(Alternate wording)*
* *Strong Technical Skills*
  + *Programming: groovy and Java programming preferred*
  + *Troubleshooting: identification(network, server, application), quick fix, long-term solution*
  + *DevOps: GitHub, Ansible, Puppet, Bamboo, Jenkins*
* Experience with Okta or other identity management software, AD, LDAP as well as an in-depth understanding of SAML2.0 and CAS
* Experience using APIs and other integration techniques to integrate data/software applications
* Ability to self-manage as well as ability to do basic project management tasks such as estimating task duration, planning and executing a set of tasks, and understanding task dependencies
* Ability to collaborate with technical and non-technical members of the university community

**WORKING CONDITIONS**

* Some (rare) weekend/off-hour work is required in this position.
* Hybrid or remote work available, if desired (as is working on-premise).
* Ability to participate in occasional in-person training, team building or other team/university events.

**PHYSICAL REQUIREMENTS**

* Physically able to lift various materials up to 25 pounds on an occasional basis.
* While performing required job tasks, physically able to bend, crouch and reach continuously.
* While performing required job tasks, physically able to remain seated, frequently to continuously.
* While performing required job tasks, physically able to remain standing up to 15% of the time.
* Possesses dexterity abilities required to operate a computer and other office equipment to perform related job responsibilities.
* Possesses physical abilities to remain at a computer workspace for long periods, frequently continuously during the working hours.

**SUPERVISORY RESPONSIBILITIES**

May occasionally lead projects where coordinating other workers’ tasks is required. May occasionally supervise student workers’ tasks.



*This document describes the general purpose, duties and essential functions associated with this job and is not an exhaustive list of all duties that may be assigned or skills that may be required.*

*I have read and understand my job description and acknowledge that management reserves the right to change or reassign job duties or combine jobs at any time.*

Employee (Print Name): Date:

Employee (Signature): Date:

|  |  |  |
| --- | --- | --- |
|  | HR OFFICE USE ONLY: | |
| **Approved by:** | | *Signature of the person with the authority to approve the job*  *description* |
| **Printed Name of**  **Approver:** | | *Printed name of the person with the authority to approve the job*  *description.* |
| **Date**  **approved:** | | *Date upon which the job description was approved* |
| **Reviewed:** | | *Date when the job description was last reviewed* |