Senior Identity and Access Management Analyst

Job Code: 340032	**FLSA Status: Exempt**	**Mgt. Approval: P. Verhage**	**Date: March 2022**
Department: 1007422 IS - Risk & Compliance		**HR Approval: N. Lazaro**	**Date: March 2022**

JOB SUMMARY

The UW Health Information Security (IS) Senior Identity and Access Management Analyst is the guardian of staff identity and access and is responsible for safeguarding critical and confidential information belonging to UW Health or for which UW Health is the custodian.

The Senior Identity and Access Management Analyst is responsible for account life cycle management and auditing as appropriate. The Senior Identity and Access Management Analyst participates in the development of workflows, system configuration, change documentation, optimization and support related to access, while working with application teams to deploy new applications and functionality.

The Senior Identity and Access Management Analyst leads and assists in the development of department and organization wide policies and procedures, while effectively communicating policies and procedures impacting Identity and Access management to end users, leadership, and peers to ensure compliant practices. The Senior Identity and Access Management Analyst provides guidance on optimizing security build based on appropriate minimum necessary standards. The Senior Analyst is responsible for the on-going maintenance, testing, support and optimization of Identity Governance and Role Based Access Controls (RBAC).

The Senior Identity and Access Management Analyst is highly independent holding organization level responsibilities and leads large scale projects. The Senior Identity and Access Management Analyst team member mentors and trains team members demonstrating leadership characteristics in line with UW Health Way. They lead and implement continuous improvements to improve efficiency and accuracy of work performed.

MAJOR RESPONSIBILITIES

- Provide user account life cycle management, including creating, provisioning, securing, and inactivation of access.
- Lead and participate in projects and production support operations focused on implementing Identity and Access Management (IAM) integrations and Role Based Access Control (RBAC) strategies and integrations.
- Lead and collaborate in the design, implementation, and support of the IAM technologies.
- Lead and participate in projects to ensure standard processes and procedures are implemented when rolling out new provisioning and role management points.
- Plan, build, test, manage, and update security for the protection of and access to UW Health systems.
- Lead the development, implementation, and support of RBAC.
- Ensure all evidence of authorization is documented and archived according to internal standards.
- Manage directory account permissions via RBAC.
- Act as the subject matter expert for Identity Governance and RBAC.
- For systems and software applications in scope for IAM Team, identify and reconcile discrepancies between access rights assigned and access rights required for users to perform job duties.
- Assist IAM Engineers in troubleshooting issues with IAM tools and processes.
- Lead application upgrades, evaluation of new technology, settings, and functionality related to IAM.
- Troubleshoot security and workflow issues independently or in collaboration with other Information Systems teams and/or stakeholders, while adhering to internal service standards.
- Enforce organizational policies and procedures to ensure only authorized personnel have access to information in compliance with the Minimum Necessary Rules.
- Participate in ongoing auditing and risk assessments, and implementation of audit recommendations.
- Identify and ensure dormant accounts/records are disabled; eliminate access for those who no longer need applicable information.
- Develop system access and security implementation plans derived from operational customer needs and requests.
- Develop, validate, and maintain detailed documentation on standard operating procedures, system configurations, and technical settings for internal team use, end user support, and other IS teams as needed.
- Write and generate reports to perform in-depth analysis and data collection for issues associated with IAM using PowerShell or other reporting methods.
- Provide Microsoft O365 Shared Resource Management and Support (Distribution Lists, Shared Calendars, Shared Mailboxes, Mail Contacts, and Resource Calendars).
- Support the enrollment of Multifactor Authentication (MFA), Single Sign-on (SSO), Electronic Prescribing of Controlled Substances (EPCS), and Mobile Device Management (MDM).
- Lead efficiency improvements by recommending process changes as well as developing solutions to automate and orchestrate repeatable tasks for IAM.
- Conduct account quality checks.

- Staff a 24x7 on-call rotation 365 days a year to ensure ongoing operations and security for a facility that operates continuously to provide the best possible care to the patients we serve.

ALL DUTIES AND REQUIREMENTS MUST BE PERFORMED CONSISTENT WITH THE UW HEALTH PERFORMANCE STANDARDS.

JOB REQUIREMENTS

Education	Minimum	Associate Degree in Healthcare, Information Technology, Business, or related field (2 years of relevant experience may be considered in lieu of degree in addition to experience below)
	Preferred	Bachelor's degree in Healthcare, Information Technology, Business, or related field
Work Experience	Minimum	• Demonstrated success training and mentoring others on Active Directory and Identity and Access management tools • Demonstrated success using analytical tools and skills for the development of workflows, system configuration and documentation related to identity and access management • Demonstrated success designing and administrating Identity Management and Access • Demonstrated success leading large scale projects and processes
	Preferred	7 years relevant work experience and Software experience: Active Directory, Microsoft O365, ServiceNow or Identity and Access management applications
Licenses & Certifications	Minimum	None
	Preferred	Systems Security Certified Practitioner (SSCP), Microsoft Outlook or Azure, or other IAM tools
Required Skills, Knowledge, and Abilities		**Intermediate competency in the following areas:** • Leadership including leads with integrity, maintains strategic orientation, demonstrates business & financial acumen, champions innovation, manages execution, leads & develops people • Technical leadership of applicable products or platforms • Leading highly empowered, self-directed teams including cross-functional teams • Communication • Effective team member • Critical thinking • Applying lean management tools • Applying agile methodologies • Mentoring and teaching **Advanced competency in the following areas:** • Identity Management • Technology Awareness and Management **Other Knowledge, Skills and Abilities** • Advanced ability to analyze data and information with a detailed understanding of regulatory requirements that impact the healthcare industry, as well as security frameworks and methodologies • Meticulous attention to detail • Advanced problem-solving skills • Ability to work comfortably under pressure and deliver on tight deadlines • Ability to maintain the highest standards of confidentiality, integrity, and personal accountability when working with sensitive and restricted data, including Protected Health Information (PHI)

PHYSICAL REQUIREMENTS

Indicate the appropriate physical requirements of this job in the course of a shift. *Note: reasonable accommodation may be made available for individuals with disabilities to perform the essential functions of this position.*

Physical Demand Level	Occasional	Frequent	Constant

		Up to 33% of the time	34%-66% of the time	67%-100% of the time
X	**Sedentary:** Ability to lift up to 10 pounds maximum and occasionally lifting and/or carrying such articles as dockets, ledgers and small tools. Although a sedentary job is defined as one which involves sitting, a certain amount of walking and standing is often necessary in carrying out job duties. Jobs are sedentary if walking and standing are required only occasionally, and other sedentary criteria are met.	**Up to 10#**	**Negligible**	**Negligible**
	Light: Ability to lift up to 20 pounds maximum with frequent lifting and/or carrying of objects weighing up to 10 pounds. Even though the weight lifted may only be a negligible amount, a job is in this category when it requires walking or standing to a significant degree.	**Up to 20#**	**Up to 10#** or requires significant walking or standing, or requires pushing/pulling of arm/leg controls	**Negligible** or constant push/pull of items of negligible weight
	Medium: Ability to lift up to 50 pounds maximum with frequent lifting/and or carrying objects weighing up to 25 pounds.	**20-50#**	**10-25#**	**Negligible-10#**
	Heavy: Ability to lift up to 100 pounds maximum with frequent lifting and/or carrying objects weighing up to 50 pounds.	**50-100#**	**25-50#**	**10-20#**
	Very Heavy: Ability to lift over 100 pounds with frequent lifting and/or carrying objects weighing over 50 pounds.	**Over 100#**	**Over 50#**	**Over 20#**
List any other physical requirements or bona fide occupational qualifications:				

Work/Environmental: Moderate noise level consistent with an office environment