Director of IT & Enterprise Systems Management

FLSA Classification: Exempt
Reports to: Chief Operating Officer
Salary Range: $97,633 - $112,132
To Apply, please visit: https://www.healthymatsu.org/employment
Application Deadline: Open Until Filled

JOB DESCRIPTION

About the Foundation

Mat-Su Health Foundation (MSHF) is the official business name of Valley Hospital Association, Inc., which shares ownership in Mat-Su Regional Medical Center. In this capacity, MSHF board members and representatives actively participate in the governance of Mat-Su's community hospital to protect the community's interest in this important healthcare institution. The MSHF mission is to improve the health and wellness of Alaskans living in the Mat-Su and the tools it uses include grantmaking, convening of local partners, and policy change. MSHF's work has resulted in significant improvements in systems that support the health of Mat-Su residents in areas such as behavioral health, child welfare, crisis response, community connections, workforce development, transportation, housing, and senior services.

Position Summary

The Director of Information Technology and Enterprise Security is a critical role within the Mat-Su Health Foundation, responsible for developing, implementing, and maintaining robust technological operations and security measures to safeguard the Foundation's assets.

These assets include but are not limited to: employee systems and records; grantee information; financial data and digital banking relationships, IT infrastructure hardware (e.g. servers, workstations, mobile devices, network equipment, routers, switches and firewalls); software (e.g. operating systems, apps, databases, etc.); network resources (e.g. internet connectivity, intranet systems, VPNs and, Wi-Fi networks); cloud resources; physical assets (e.g. server rooms and office spaces containing IT equipment); communication systems (e.g. email, VoIP, instant messaging platforms and video conferencing tools; access credentials (user accounts, passwords, authentication tokens and, digital certificates) and; backup and recovery systems (e.g. data backups, disaster recovery and business continuity plans).

This position will lead the organization's IT strategy, oversee cybersecurity initiatives, and drive the integration of innovative technologies, including Artificial Intelligence, to enhance operational efficiency and protect against cyber threats.

Job Responsibilities

Leadership

- Develop and execute a comprehensive IT and cybersecurity strategy aligned with the Foundation's mission and objectives.
- Lead the planning and implementation of new technologies and systems upgrades to enhance organizational efficiency and security.
- Collaborate with the executive leadership team (ELT) to establish IT governance policies, internal standard operating procedures (SOPs), and best practices.
- Supervise and manage relationships with external IT vendors and consultants.
- Provide regular reports and updates to the Chief Operating Officer and ELT on IT initiatives, security status, and risk assessments.

- Foster a culture of innovation and continuous improvement within the Foundation.
- Create and implement a long-term technology roadmap aligned with the Foundation's growth objectives.
- Implement cost monitoring capabilities to track and optimize IT expenditures.
- Develop and maintain a strategic recapitalization plan for IT infrastructure and systems.
- Conduct regular cost-benefit analyses for major IT investments and initiatives.

Cybersecurity

- Design and implement robust cybersecurity measures to protect against threats such as data breaches, malware, and social engineering attacks.
- Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the Foundation's IT infrastructure.
- Develop and maintain an incident response plan to effectively manage and mitigate cyber-attacks.
- Implement and manage advanced threat detection and prevention systems.
- Oversee the Foundation's data backup and disaster recovery processes to ensure business continuity.
- Establish and enforce security governance policies and internal SOPs for Foundation Board of Directors, employees, and contractors.
- Implement a comprehensive identity and access management system.
- Develop and maintain a cybersecurity awareness program for the Board of Directors and employees.

Management and Administration

- Create and manage the IT department budget, ensuring cost-effective allocation of resources and implementing cost monitoring capabilities.
- Oversee the Foundation's data lifecycle management program, including data governance, security, and compliance with relevant regulations.
- Implement and maintain IT service level agreements (SLAs) for internal departments and external stakeholders.
- Develop and execute a strategic recapitalization plan for IT infrastructure and systems to ensure long-term sustainability.

Infrastructure and Systems Management

- Direct the management and maintenance of all IT systems, including networks, servers, databases, and end-user devices.
- Identify comprehensive cloud-based solutions to enhance and reduce on-premises infrastructure. and execute a cloud-based migration strategy informed by industry best practices including but not limited to desktop tiles, shared drives, data applications, digital assets, and IT processes. Develop and maintain a comprehensive IT asset management system.
- Oversee information security processes to ensure data integrity, system availability, and access management.
- Manage technology procurement and maintenance to provide optimal, efficient, and cost-effective IT support for Foundation operations.
- Provide technical direction for SharePoint and database management systems.
- Establish and maintain IT service level agreements (SLAs) for internal and external stakeholders.
- Partner with foundation departmental leaders to help secure, safeguard and optimize internal systems i (e.g., Director’s Desk, Salesforce, Giving Data, Sage, Stamplii, etc.)
- Partner with foundation departmental leaders to evaluate current software and/or select new software systems.

Artificial Intelligence Integration

- Develop and implement a comprehensive AI strategy for the Foundation, including use cases, ethical guidelines, and integration roadmap.
- Create and maintain AI internal SOPs to guide the ethical and effective use of AI technologies within the organization.
- Design and deliver educational programs to inform employees about AI capabilities, limitations, and best practices for integration into everyday work.
- Evaluate and implement AI-powered tools to enhance cybersecurity, data analysis, and operational efficiency.
- Establish partnerships with AI research institutions and industry leaders to stay at the forefront of AI advancements.
- Develop and implement AI-driven predictive analytics for grant-making and program evaluation.
- As a part of the Foundation's Operations Convening, create an AI ethics though partner group to oversee the responsible use of AI technologies within the Foundation.

Vendor and Contract Management

- Manage relationships with IT service providers and other third-party vendors.
- Negotiate and oversee contracts for IT services, software licenses, and hardware procurement.
- Ensure vendors adhere to the Foundation's security standards and compliance requirements.
- Develop and maintain a vendor performance evaluation system.
- Implement a vendor risk assessment process to mitigate potential security and operational risks.
- Establish and maintain a vendor diversity program to support the Foundation's commitment to equity.

Staff Training and Support

- Develop and implement comprehensive IT and cybersecurity training programs for all Foundation employees.
- Oversee the delivery of employee training programs to enhance cybersecurity awareness and reduce human error-related risks.
- Assess IT related employee training programs to determine the most appropriate training programs for Foundation staff.
- Provide end-user support and ensure timely resolution of IT issues for Foundation employees and Board members.
- As a part of the Foundation's internal professional growth and development plan, outline an education program to develop, enhance and evolve IT skills among non-technical staff members.
- Create and maintain a knowledge base of common IT issues and solutions for staff reference.
- Develop and deliver specialized training for executive leadership and staff on emerging technologies, cybersecurity awareness, and their potential impact on the Foundation's mission.

Compliance

- Ensure compliance with relevant data protection regulations and industry standards.
- Develop and maintain IT governance frameworks to align IT initiatives with organizational goals.
- Implement and manage access control systems to protect sensitive information and ensure appropriate user permissions.
- Conduct regular IT governance policy and internal SOP reviews and updates to maintain alignment with industry best practices.
- Develop and maintain a comprehensive IT risk register and mitigation strategies.
- Implement and oversee an IT audit program to ensure ongoing compliance and identify areas for improvement.

Innovation and Continuous Improvement

- Stay informed about emerging technologies and industry trends to identify opportunities for innovation within the Foundation.
- Implement a continuous improvement process for IT services and infrastructure.
- Explore and make recommendations to implement cloud-based solutions to enhance scalability and reduce on-premises infrastructure costs.
- Establish an innovation lab to test and evaluate new technologies for potential Foundation use.
- Develop and maintain partnerships with technology incubators and startups to access innovative solutions.
- Implement a suggestion system for staff to contribute ideas for IT improvements and innovations.

Internal and External Relations

- Collaborate with foundation departmental leaders to secure, safeguard, and optimize internal systems
- Become a part of a regional thought partner group of IT leaders (e.g., Technology Association of Grantmakers) to stay current on existing and emerging IT trends.
- Develop and maintain strong relationships with technology vendors, service providers, and industry partners to ensure the Foundation receives optimal support and value.
- Serve as the primary liaison between the IT department and other foundation departments, ensuring effective communication and alignment of IT initiatives with organizational goals.
- Develop and maintain strategic partnerships with technology providers and industry leaders.

Health Equity Promotion

- Embrace and support the Foundation’s commitment to diversity, equity, and inclusion (DEI) by leading Foundation-wide strategies as jointly determined and prioritized by the Foundation’s Chief Operating Officer and Chief Community Impact Officer.
- Advance personal and professional growth in cultural competency and equity.

Competencies

- Exceptional leadership skills with the ability to inspire and motivate others.
- Strong strategic thinking and problem-solving abilities.
- Excellent verbal and written communication skills, with the ability to explain complex technical concepts to non-technical stakeholders.
- In-depth knowledge of cybersecurity best practices, threat landscapes, and mitigation strategies.
- Proficiency in project management methodologies and experience leading large-scale IT initiatives.
- Strong vendor management skills and ability to negotiate favorable contracts.
- Expertise in data analytics and the ability to leverage data for decision-making.
- Thorough understanding of IT governance frameworks and compliance requirements.
- Ability to build relationships and trust with internal and external stakeholders.
- Demonstrated experience in crisis management and incident response.
- Innovative mindset with the ability to identify and implement emerging technologies.
- Strong financial acumen and budget management skills.

Education, Experience and Certification(s)

- Bachelor’s degree in information technology, Computer Science, Cybersecurity, or a related field; or equivalent combination of education and experience.
- Minimum of 5 - 10 years of progressive IT leadership experience,
- Proven track record of successfully implementing enterprise-wide IT strategies and cybersecurity initiatives.
- Extensive experience in risk management and compliance within the nonprofit or healthcare sectors.
- Demonstrated expertise in AI technologies and their application in organizational settings.
- Relevant industry certifications such as CISSP, CISM, CRISC, or CGEIT are highly desirable.
- Experience working with foundations, nonprofit leadership, or corporate boards is preferred.

Other Duties

- Willingness to work flexible hours and be on-call for emergency situations.
- Ability to travel occasionally for conferences, training, or vendor meetings.
- Commitment to ongoing professional development and staying current with emerging IT trends and best practices.

Supervisory Responsibilities

This position requires experience in positively managing personnel and or vendor relationships to achieve objectives.

Work Location

Wasilla, Alaska

Work Environment

Employee will be working in a typical office environment with offices, moderate temperature, and equipment noise.

Physical Demands

Employee will be spending considerable time at a desk using a computer terminal and will occasionally be required to use personal vehicle to travel to various locations in the community.

EEO Statement

Mat-Su Health Foundation is an equal employment opportunity employer. We celebrate diversity and are committed to creating an inclusive environment for all employees.