



REBA AND SAM SANDLER FAMILY CAMPUS
of the Tidewater Jewish Community

DIRECTOR, INFORMATION TECHNOLOGY SECURITY

Direct Report: Facility Director
Indirect Report: Chief Financial Officer (CFO)
Classification: Full-Time Exempt

Position Overview:

The Director of Information Technology (IT) Security is responsible for developing, implementing and monitoring a strategic, comprehensive enterprise cybersecurity and IT risk management program for the Sandler Family Campus and affiliate agencies. The Director, IT Security will provide the vision and leadership necessary to manage the risk to the organization and will ensure business alignment, effective governance, system and product availability, integrity and confidentiality.

Qualifications:

- Bachelor's degree from an accredited institution, with degree preferred in Computer Science or Information technology systems security or related field. Master's degree preferred.
- Minimum of ten (10) years within the last twelve (12) years of experience in the field related to the title of the position.
- Certified Information Security Manager (CISM) or Certified Information Systems Security Professional (CISSP) Certification.
- Knowledge of Information technology infrastructure library (ITIL) (certification preferred) with respect to security administration and information technology governance in a multi- platform environment.
- Knowledge and experience in audio-visual, multimedia operations
- Experience in establishing cybersecurity and risk metrics for reporting
- Strong Emotional Intelligence with demonstrated sustained leadership in a large organization involving multiple stakeholders.
- Demonstrated management skills, e.g., budget development and administration, policy development and implementation, personnel administration, staff training and development.
- Demonstrated ability to work with diverse people; effective oral and written communication skills.

Performance Responsibilities:

Essential Functions:

- Provides the direction for Campus data and cybersecurity protection, and oversee Technology governance and policies.
- Develops Campus security strategy, security awareness programs, security architecture, and security incident response.
- Provides strategic risk guidance for IT projects, including evaluation and recommendation of technical controls.
- Educates IT users on appropriate security risk and mitigation strategies
- Collaborates as needed, and coordinates the IT component of both internal and external audits, federal and state examinations to ensure security programs are in compliance with relevant laws, regulations and policies.

- Develops, maintains and publishes up-to-date security policies, standards and guidelines. Oversees training and dissemination of IT security policies and practices.
- Manages system acquisitions plans and procurement approaches
- Collaborates with UJFT/JCC CFO, and executives of affiliate agencies to maintain consistency within IT budgets
- Evaluates new cybersecurity threats and IT trends and develops effective security controls. Oversees development of security awareness programs.
- Develops and oversees effective IT disaster recovery policies and standards to align with company business continuity management program goals. Coordinates development of implementation plans and procedures to ensure business critical services are recovered in the event of disasters or other incidents, and provides direction, support and in-house consulting in these areas.
- Evaluates potential security breaches, coordinates response, and recommend corrective actions.
- Supervises the IT Coordinator as assigned in the performance of the job duties.
- Define and report on information security metrics.
- Provides project management and leadership to staff and external resources in support of established goals and objectives, improved efficiencies, and problem resolution.
- Ensures accomplishment of all objectives in accordance each affiliate agency's policies, procedures, and strategic direction, as well as regulatory standards governing the SFC.
- Maintains current knowledge of industry and regulatory trends and developments for the enterprise technology
- Capable of lifting/carrying 20 lbs. and occasionally up to 50 lbs.; some physical activity, such as standing, bending required
- Manages all CCTV cameras and servers
- Manages Offsite disaster recovery
- Building access systems /card readers
- Maintains all audio and visual equipment
- Maintains all physical and virtual servers.
- Maintains all hardware software licensing and warranties
- Performs other duties as assigned

GENERAL RESPONSIBILITIES:

- Responsible for all assigned items, keys etc.
- Follow all Campus safety procedures; use appropriate safety gear; use caution when operating electrical equipment; immediately report accidents and injuries to the supervisor.
- Maintain assigned IT closet in a clean orderly manner.
- Keep track of assigned equipment, and ensure that it is properly maintained. Replace worn cables keypads etc. Secure equipment at all times when it is unattended. Immediately report missing or worn equipment to the IT Director.
- Report any building maintenance or pest control problems to the supervisor.
- Cooperate at all times with Security; assist Security and maintenance personnel during emergencies.
- Must be sensitive to the needs and programs of faculty, students, staff and visitors.
- Ability to work effectively in an environment subject to frequently changing priorities, and the ability to remain flexible based upon those needs and priorities of the Campus and affiliate agencies.
- Other duties may be assigned, as necessary.

To Apply For This Position

Submit cover letter, resume and salary requirements to: resumes@ujft.org

Review of applications will begin immediately, and continue until the position is filled.