Franklin County Data Center
Job Posting

$66,851-$86,907 **Excellent Benefits Package

JOB TITLE: IT Security Operation Supervisor

SUMMARY

The IT Security Operation Supervisor, reporting to the Director of Information Security, is responsible for leading various IT security operational activities, performing technical administration of IT security systems, as well as various team supervision duties. This role is responsible for overseeing the daily operations of key IT security systems and processes, leads responses to new security threats, incident responses, and investigations of potential breaches. Will also track work progress and report key metrics to senior management for strategic planning and decision making. Must successfully complete 180-day probationary period.

ESSENTIAL DUTIES AND RESPONSIBILITIES

- Manages the team that performs security operational administration on designated systems and applications, in accordance with the defined policies, standards and procedures of the organization.
- Ensures that customer service requests, break-fix incidents, and questions are addressed within the defined service level agreement.
- Spends significant time monitoring daily operations of the group, ensuring uptime, reliability, and effectiveness of security system.
- Plans the work, delegating effectively and following up with staff on deliverables. Provides continual support and guidance.
- Manages data outputs of security monitoring tools and proactively drives appropriate security measures to protect the enterprise and end users.
- Mitigates escalations of client incidents and issues. Assesses and troubleshoots, consults with vendors, and coordinates with other teams for problem resolution.
- Oversees patching activities where appropriate and remove or mitigate known control weaknesses, such as unnecessary services or applications or redundant user accounts, as a means of hardening systems in accordance with security policies and standards. Overall, facilitate the location and repair security problems and failures.
- Monitors and routinely audits compliance to all information security procedures and policies, and ensures consistency of internal controls across departments.
- Creates and maintains information system and software security certificate activities, including oversight for PCI and HIPAA compliance.
- Manages security vendor performance for products and services including, but not limited to, anti-virus software, intrusion prevention and intrusion detection systems, identity management, enterprise file transfer systems, and vulnerability management systems, administering products for staff as needed.
- Participates in threat and vulnerability assessments, in some cases followed by appropriate remedial action, to ensure that systems are protected from known and potential threats and are free from known vulnerabilities.

- Assists in the analyses and selection of security tools and other security measures.
- Develops and implement tests of computer systems to monitor effectiveness of security.
- Presents security concepts, technologies and plans to broad audience groups including Senior Leadership.
- Coordinates, documents, and reports on internal investigations of possible security violations, working with Director of Information Security, the FCDC's CIO/CISO, law enforcement and/or legal representatives in investigations of possible security violations.
- Performs other duties may be assigned.

SUPERVISORY RESPONSIBILITIES

Directly supervises security operation team members including FTEs, contractors, and/or vendors. Provides oversight and guidance for security enforcement and governance.

QUALIFICATIONS

- To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.
- Must possess at least five years of information security experience.
- Strong working knowledge and hands-on experience in one or more specific technical areas, such as Active Directory, Single Sign-on, intrusion detection and prevention systems, vulnerability management systems, device certification program, anti-virus systems, web content filtering systems, incident response, or access control management.
- Demonstrated experience implementing security initiatives that require partnership with other IT areas and business units.
- Strong analytical and problem solving skills.
- Working knowledge of generally accepted change, problem and incident management principles
- Excellent oral and written communication skills.
- Excellent team player with a proven track record of working across a large distributed enterprise.
- Strong ability to work effectively with external vendors and all levels of technical staff, management, and stakeholders.
- Must demonstrate strong discretion when handling confidential information.

EDUCATION and/or EXPERIENCE

Must possess a college degree; or five years related experience and/or training; or equivalent combination of education and experience.

CERTIFICATES, LICENSES, REGISTRATIONS

CISSP, CISA or equivalent certification preferred.

LANGUAGE SKILLS

Ability to read, analyze, and interpret general business periodicals, professional journals, technical procedures, or governmental regulations. Ability to write reports, business correspondence, and procedure manuals. Ability to effectively present information and respond to questions from groups of managers, clients, customers, and the general public.

REASONING ABILITY

Ability to define problems, collect data, establish facts, and draw valid conclusions. Ability to interpret an extensive variety of technical instructions in mathematical or diagram form and deal with several abstract and concrete variables.

PHYSICAL DEMANDS

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.
While performing the duties of this job, the employee is regularly required to sit; use hands to finger, handle, or feel; reach with hands and arms; and talk or hear. The employee frequently is required to walk. The employee is occasionally required to stand. The employee must frequently lift and/or move up to 10 pounds and occasionally lift and/or move up to 25 pounds. Specific vision abilities required by this job include close vision, distance vision, peripheral vision, depth perception, and ability to adjust focus.

WORK ENVIRONMENT

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is occasionally exposed to risk of electrical shock. The noise level in the work environment is usually moderate.

Data Center Benefits Summary:
Medical, Vision, Life, Mental Health, Direct Deposit, Credit Union, Deferred Comp, Retirement, Sick and Vacation Accrual, Tuition Reimbursement
EEO No fees