Franklin County
Data Center

Franklin County Data Center
Job Posting

$129,806 - $166,748
****Excellent Benefits Package**

JOB TITLE: Chief Information Security Officer (CISO)

SUMMARY

The Franklin County Data Center is seeking an experienced Chief Information Security Officer (CISO) responsible to direct strategy, operations and the budget for the protection of the county's information assets. The scope of responsibility will encompass communications, applications and infrastructure, including the policies and procedures which apply. The ideal candidate will be a visionary leader for the Franklin County Data Center's total information security needs to ensure the security posture of Franklin County. The CISO will work closely with the CIO and other key stakeholders. This candidate must demonstrate outstanding interpersonal communication skills as well as the ability to train others on security policies and practices. Must successfully complete a 180-day probationary period.

ESSENTIAL DUTIES AND RESPONSIBILITIES

Include the following. Other duties may be assigned.

- Establish and provide strategic vision and leadership for the Franklin County Data Center's comprehensive security program.
- Direct and approve the design of security systems;
- Ensure that disaster recovery and business continuity plans are in place and tested;
- Ensure that security policies, controls and cyber incident response planning is in place;
- Approve identity and access policies;
- Review investigations after breaches or incidents, including impact analysis and recommendations for avoiding similar vulnerabilities;
- Maintain a current understanding the IT threat landscape;
- Ensure compliance with the changing laws and applicable regulations;
- Translate that knowledge to identification of risks and actionable plans to protect the county;
- Schedule periodic security audits, report on and address remediation's;
- Oversee identity and access management policies;
- Make sure that cyber security policies and procedures are communicated to all personnel and that compliance is enforced;
- Manage all teams, employees, contractors and vendors involved in IT security, which may include hiring;
- Provide training and mentoring to security team members;
- Constantly update the cyber security strategy to leverage new technology and threat information;
- Brief key stakeholders on status and risks, including taking the role of champion for the overall strategy and necessary budget; and
- Communicate best practices and risks to all parts of the business, not just IT.
- Establish security and compliance goals, metrics and reporting mechanisms. Create a maturity model and maintain a security roadmap for continual improvements.
- Oversee the development and implementation of an effective incident response program to address, control, and manage information security incidents, events, or security breaches. Ensure that the incident response program is aligned to the FCDN security program.

- Responsible for instituting security education and awareness. Oversee the development and implementation of an ongoing security awareness training program that can be expanded upon for all county agencies.

SECURITY TOOLS

Serve as subject matter expert for the following security tools and security areas:

- Intrusion detection and prevention tools
- Elevated account management tools
- Firewall systems
- Web and content filtering tools
- ITSM IT GRC
- Log correlation engines
- End point (anti-virus, malware, and related end point threats)
- Training classes and conferences
- Mobile Device Management (MDM) tools
- PHI, PII, PCI, and sensitive data

SUPERVISORY RESPONSIBILITIES

Will be required to manage all employees and contractors involved in IT security which may include; training, mentoring and hiring. Off-hours support is expected-must have the ability to respond to security events during non-traditional hours.

QUALIFICATIONS

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily and be a reliable presence on site, maintaining appropriate business hours. 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.

- Proven working experience building and maintaining security systems.
- Excellent analytical and problem-solving skills.
- Solid technical knowledge of security industry best practices and procedures.
- Experience with network technologies and with system, security, and network monitoring tools.
- Familiarity with web related technologies (Web applications, web services, service oriented architectures) and of network/web related protocols.
- Hands-on experience in security systems, including firewalls, intrusion detection systems, anti-virus software, authentication systems, log management, content filtering, etc.
- Problem solving skills and ability to work under pressure.
- Ability to be a strong leader and collaborate with all levels with credibility.
- Exemplify strong business partnering skills, leadership presence and organizational maturity.
- Understanding of the system hardening processes, tools, guidelines and benchmarks.
- Hands-on experience with vulnerability scanning, firewall, antivirus & malware analysis, proxy, IDS/IPS, log correlation tools, Data Privacy, SIEM, DLP, and other related tools.

EDUCATION and/or EXPERIENCE

- Bachelor's degree from four-year college or university with courses in computer science, cyber security, application programming languages, development tools, systems analysis and systems design; or equivalent combination of education and experience.
- Advance degree in the field of information security or risk management is preferred.
- CISSA, CISSP or CISM (at least one is required)
- NIST 800-53 knowledge
- Prior demonstrated experience with FTI.
- 10+ years of hands on experience in IT security.
- Demonstrated technical proficiency with PowerShell.
- 10+ years of security staff management.
- 3+ years of demonstrated CISO leadership experience.

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, agencies, elected officials, 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.

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.

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**