Franklin County
Data Center

FRANKLIN COUNTY DATA CENTER
Job Posting: Director of Information Security

ANNUAL SALARY: $106,198 - $138,057 **EXCELLENT BENEFITS PACKAGE

SUMMARY

The Director of Information Security is responsible for the design, implementation and oversight of the information security program and framework for the Franklin County Data Network (FCDN). This will be under the guidance of the Chief Information Officer (CIO) or Chief Information Security Officer (CISO). This individual possesses vast experience in information security practices, secure network architecture, Internet Protocol (IP), firewalls, encryption, intrusion detection systems, web filtering, authentication, and authorization methodologies. The Director of Information Security will assist the CIO/CISO with the preservation of confidentiality, integrity, availability, and non-repudiation of County information resources through the development, deployment and embedding of information security architecture, policies and standards. The Director of Information Security must demonstrate effective communication skills as well as the ability to train others on security policies and practices. S/he must be able to manage onsite staff, contractors and services, providing technical direction as necessary. This position will play a major role in the development of a dedicated Security Operations Center (SOC) and Secure Managed Services. Must successfully complete a 180-day probationary period.

ESSENTIAL DUTIES AND RESPONSIBILITIES

Include the following. Other duties may be assigned.

- Perform complex IT architecture projects with competency to preserve the confidentiality, integrity, availability, and non-repudiation of the FCDN.
- Responsible for the development, deployment and embedding of information security architecture, policies and standards for a dedicated Security Operations Center (SOC), as envisioned by the CIO/CISO.
- Coordinate the documentation, distribution, and enforcement of FCDN security policies, standards, and procedures, working in collaboration with key IT staff to develop and implement communication strategies for all cyber security policies and procedures.
- Create and maintain cyber risk management methodologies.
- Develop effective security risk and control metrics.
- Responsible for the execution of day-to-day security operations.
- Regularly collaborate with the Directors over Enterprise Architecture and Application Development, to ensure cohesion of planning, implementation and communication strategies.
- Keep abreast on the latest security legislation, regulations, advisories, alerts and vulnerabilities pertaining to FCDN.
- Serve as the FCDN security audit and governance lead. Prepare and submit required reports to internal and/or external stakeholders, ensuring that systems, software, networks, and information are evaluated for security compliance.
- Regularly evaluate vulnerabilities, document, and implement controls.
- Develop and implement a comprehensive Identity, Access and Authentication program that defines and provides appropriate secure access to FCDN technology assets.
- Develop and implement a vulnerability management program that encompasses the external network, internal network, servers, PCs, applications and all endpoint devices.

- Develop and implement 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.
- Develop and implement an ongoing security and 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
- Access and Authentication technology and tools
- General and privileged access methodologies
- 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

Directly manages the team members of the security program. Will be required to provide coaching and guidance to employees relating to process and governance. Will be required to provide oversight to contract employees and services. 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.
- 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

- CISSP or CISM certification is required.
- CISSA certification is preferred.
- A college degree with courses in computer science, cyber security, application programming languages, development tools, systems analysis and systems design; or equivalent combination of education and experience.
- NIST 800-53 knowledge
- Prior demonstrated experience with FTI preferred.
- 10+ years of hands-on experience in IT security.
- 5+ years of experience with security staff management.
- Project management certification is 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, 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
fcdcjobs@franklincountyohio.gov
EOE No Fees ERP Eligible