

## Franklin County Data Center Job Posting

### **JOB TITLE: DIRECTOR, INFORMATION SECURITY**

#### **SUMMARY**

Under the direction of the FCDC CIO and in strong collaboration with FCDC and county-wide technology leaders, the Information Security Director is responsible for the comprehensive information security policies and practices for the Franklin County Data Network. The position requires a technically competent security leader with depth of experience in systems, network, applications, and device security capable of continuously monitoring and assessing the Franklin County Data Network's security posture, communicating and managing risk, and evolving the strategic security planning and execution for Franklin County. The scope of this role includes information in electronic, print and other formats. The purpose of this position includes: assure that information created, acquired or maintained on the FCDN is available, accessible by only authorized users, and used in accordance with its intended purpose; to protect FCDN information and its infrastructure from external or internal threats; and to assure that FCDN users complies with all statutory, regulatory, or governing policies regarding information access, security, and privacy; to implement best security practices. The Information Security Director is responsible for preserving the availability, integrity, and confidentiality of County information resources through security leadership and governance, managing risks through explicit security control practices. The Information Security Director develops, coordinates, and oversees the implementation, and execution of, security policies and procedures to safeguard equipment, software, and information in computer files against accidental or unauthorized modification, destruction, or disclosure. Must successfully complete 180-day probationary period.

**ESSENTIAL DUTIES AND RESPONSIBILITIES** Other duties may be assigned.

#### **Policy**

Coordinate the documentation, distribution, and enforcement of FCDN security policies, standards, and procedures. Work with key IT offices in the development of such policies. Oversee the dissemination of policies, standards and procedures to FCDN users.

#### **Education and Training**

Coordinate the development and delivery of education and training on the information security and privacy matters for FCDN users and specialized training for systems owners and administrators.

#### **Compliance and Enforcement**

Serve as the FCDN audit and compliance lead. Prepare and submit required reports to internal and/or external stakeholders as a part of a comprehensive Certification and Accreditation program. Ensure systems are evaluated for security compliance on a regular basis, evaluate vulnerabilities and make recommendations based on current threat vectors, and document Information Assurance controls.

#### **Incident Response**

Develop and implement a Security Incident Reporting and Response protocol to address FCDN security incidents (breaches), respond to alleged policy violations. Correlate incidents and events across the network and disparate systems to detect and prevent attacks. Adapt the security posture, policy, and training based on current threat vectors and new systems.

#### **Risk Assessment and Incident Prevention**

Develop and implement an ongoing risk assessment program targeting information security matters; recommend methods for vulnerability detection and remediation, and oversee vulnerability testing.

### **Specialized Information Processing Oversight**

Protect, defend, secure, and ensure availability of Franklin County Information. Develop, oversee, and govern systems and processes in accordance with legal standards for all information and, in particular, Personally Identifiable Information, Payment Card Industry information, Health Insurance Portability and Accountability Act, and financial information.

### **Maintain Knowledgebase**

Maintain Security Technical Expertise in the Following Areas:

- Identity Management and Access Controls
- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Security Assessment and Training
- Security Operations and Training
- Software Development Security

### **Security Tools**

Serve as subject matter expert for the following security tools:

- Network Monitoring and Scanning
- Imaging and Vulnerability/Patch Management
- Firewall and Intrusion Prevention Systems
- Anti-virus
- Webfiltering
- Logging
- Security Incident and Event Management
- End Point and Mobile Device Management

Maintain familiarity with security tools, to include but not limited to:

Keep abreast of latest security legislation, regulations, advisories, alerts and vulnerabilities pertaining to FCDN.

- Develops and implements up-to-date security policies, procedures, and standards based on industry best practices, to protect the integrity, accuracy, confidentiality and recoverability of data and information across the County.
- Leads post-security risk assessment improvements including control implementation and staff education.
- Implements and oversees compliance monitoring activities.
- Interfaces with user community to understand their security needs and implement procedures to meet their requirements and applicable laws.
- Facilitates security awareness among staff so that information is treated as an asset and develops and supports training in multiple communities.
- Monitors internal control systems to ensure appropriate access levels are sustained.

- Researches, communicates and implements local, state and federal statutes as they relate to confidentiality and security of County information and other regulations that impact the hardcopy and online storage and protection of information.
- Provides recommendations for the selection of security software, physical and logical access control, and other security measures.
- Develops and implements tests of computer systems to monitor effectiveness of security.
- Distributes and maintains user access records including login and passwords.
- Reviews computer logs and messages to identify and report on possible violations of security.
- Coordinates, documents, and reports on internal investigations of possible security violations.
- Works with law enforcement and legal representatives in investigations of possible security violations.
- Conducts semi-annual computer access audits and takes appropriate measures based on the findings.
- Develops, coordinates, and implements disaster or emergency recovery procedures for information systems and computer environment.

Perform other duties as assigned.

### **SUPERVISORY RESPONSIBILITIES**

May supervise security team members and others in their performance of related tasks, including performance management and development.

### **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.

- Excellent oral and written communication skills.
- Highly skilled at managing large-scale projects simultaneously.
- Proven ability to collaborate with a broad range of constituencies.
- Strong ability to influence growth and positive change.
- Proven trustworthiness.
- Strong commitment to hold confidentiality to the highest regard, reinforcing for others the importance of upholding confidentiality.

### **EDUCATION and/or EXPERIENCE**

Bachelor's degree (B. A.) from four-year college or university; and ten to twelve years of related experience and/or training; or equivalent combination of education and 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, 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.

## **CONFIDENTIALITY AND NON-DISCLOSURE**

The Director of Information Security is responsible for protecting sensitive information related to the security posture of the Franklin County Data Network and has elevated systems privileges. As such, special faith and trust is placed in this position. Violation of this trust, through abuse of elevated privileges, or releasing security posture information to any unauthorized individuals or those without a mandated need to know, will result in termination.

## **CERTIFICATES, LICENSES, REGISTRATIONS**

Acquired CISSP, CISM, or CISA.

## **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.

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**

**Send resume, references, and salary requirements to:**

**Jessica Wilkins-Bibbs- Director, Human Resources**

**[jrwilkin@franklincountyohio.gov](mailto:jrwilkin@franklincountyohio.gov)**

**(614) 525-5984**

**No Fees EOE**