OFFICE OF THE COOK COUNTY CLERK

Human Resources
118 N. Clark Street, Room 230
Chicago, Illinois 60602
(312) 603-5656

STANDARD JOB DESCRIPTION

Director of Cybersecurity

Job Code: 7058
Job Title: Director of Cybersecurity
Salary Grade: 24

Position I.D. No.: 0005349
Status: Shakman Exempt
Division: Information Technology

Job Summary

The Director of Cybersecurity reports directly to the Deputy Clerk of Information Technology and is responsible for managing and maintaining multiple Cook County Clerk's Office (CCCO) security technologies and the associated procedures and processes. The Director of Cybersecurity will detect, identify, analyze, correlate security incidents within the CCCO and escalate security incidents to the Deputy Clerk of Information Technology. The Director of Cybersecurity will also lead investigation and remediation of cyber security incidents as well as manage and maintain the physical security and physical access control systems within CCCO. Lastly, the Directory of Cybersecurity will collaborate with the Assistant Deputy Clerk of Elections to develop the policy for election security and develop the strategy to respond to security breaches. This role will brief the Cook County Clerk and Chief Deputy Clerk on security breaches, points of vulnerability and advise on possible solutions.

This position will have access to confidential and sensitive information as a part of crisis/issue management and will participate in "Confidential" meetings, communications and "Policymaking" related items, the position shall be selected by the Clerk of Cook County, or her or his designee.

Essential Job Duties

- Facilitate and review security technologies, hardware, and software; develop key metrics and performance goals.
- Collaborate with Deputy Clerks and management to develop and implement facility security best practices, coordinate and plan to proactively identify, mitigate, and manage risks within CCCO.
- CERT, Test, Exercise and Conduct Drills of Response Plans, Problem Management, Root Cause Analysis, and After-Action Reports.
- Collaborate with a range of functions including Compliance, Privacy and the enterprise to monitor developments in the areas of legal, regulatory, Cook County requirements, technological developments, and best practices in the information and cyber security governance and compliance field.
- Assess the impact or potential impact of change management initiatives of various sizes and degrees of complexities CCCO performance and productivity

- Stay current with technology trends by researching new methods that will effectively protect networks, databases, and applications and keep abreast of latest security and privacy legislation, regulations, advisories, alerts and vulnerabilities pertaining to all of the CCCO.
- Identify problems and security risks with network infrastructure and recommend corrective actions, troubleshoot and resolve performance or functional errors.
- Investigate cyber security incidents, escalate issues to the Deputy Clerk of Information Technology, if necessary, and recommend changes to network infrastructure based on outcome of incident.
- Work directly with other agencies to maintain security initiatives to protect CCCO infrastructure.
- Provide support for Election Day activities including, but not limited to deployment of special tools, participation in special election related projects, travel to and from the Elections Operations Center, participation in election preparation procedures including, but not limited to Pre-LAT, e-pollbook preparation, or other equipment, process or procedural tasks.

Minimum Qualifications

- Bachelor's degree in Computer Science, Information Technology, Information Systems, or closely related field.
- Certified Information Systems Security Professional (CISSP) or Certified Information Systems Auditor (CISA)
- Three (3) years of full-time project management experience.

Knowledge, Skills and Abilities

- Strong interpersonal, communication, project management, and leadership skills, including the ability to effectively communicate to both technical and non-technical audiences
- Knowledge of enterprise software (I.e. Absolute computrace, teamviewer and Votesafe).
- Ability to operate SAN/NAS (EMC/Clarion/VNX) and Cisco UCS.
- Ability to operate VMWare ESX 6.0 or higher.
- Ability to operate EMC Avamar backup solution.
- Ability to configure and manage MS SCOM/SCCM.
- Knowledge of Linux and SQL 2012/2016.
- Familiarity with Kace 1000 ticketing system.
- Ability to operate Windows server 2008/2016 with highly available network and system architecture.
- Highly self-motivated.
- Excellent self-management skills with high level of accuracy and reliability.
- Strong attention to detail.
- Strong analytical and problem-solving skills.
- Ability to assess the impact or potential impact of change management initiatives of various sizes and degrees of complexities CCCO performance and productivity.
- Significant experience with enterprise security, enterprise back-up software (Veeam a plus) and email security tools.
- Solid understanding of standard business processes including Change Management, Problem Management, Work Prioritization, Quality Assurance, and Continuous Improvement best practices, etc.

- Partner with various teams to improve security and bring standard methodologies to our infrastructure, products, and services.
- Drive detection, response, investigation, and remediation of infrastructure security vulnerabilities.
- Ability to conduct technological analyses and research.

Physical Requirement

- Ability to stand, sit, and kneel for long periods of time.
- Ability to lift up to 30 lbs.