# Cyber Information Security Officer 1927

**Grade: 11**

**FLSA: Exempt**

**Date: 11/22**

**Job Summary:** The Information Security Officer (ISO) is responsible for assisting with the day-to-day operations of securing the county’s various information systems. Reporting to the Deputy Director of Information Technology, the ISO is tasked with providing technical expertise in all areas of network, system, and application security for the entire county network including supported sub-agencies. The ISO works closely with the various teams in the Information Technology department, county departments, and allied agencies (Metcom, St. Mary’s County Health Department, St. Mary’s County Libraries, St. Mary’s County Public Schools, etc.) that utilized county infrastructure to ensure that systems and networks are always designed, developed, deployed, and managed with an emphasis on strong, effective security and risk management controls. The ISO leads the county-wide Cyber Security Planning Committee with county, state, and federal Cybersecurity compliance for all county and county allied agencies. Assesses the vulnerability management program, reviews annual cybersecurity assessments and penetration tests, and research and reports on emerging threats, to take pre-emptive risk mitigation steps for multiple county agencies. The ISO effectively correlates and analyzes security events within the county’s unique network environment to proactively detect threats and mitigate attacks before they occur by establishing policies and procedures which defend against remote attacks of the county infrastructure.

**Essential Functions:**

1. Monitor online security-related resources for new and emerging cyber threats;
2. Ensure compliance with county, state, and federal cybersecurity laws and policies;
3. Proactively monitor the network environment to detect and implement steps to mitigate cyber-attacks before they occur;
4. Provides technical expertise regarding security-related concepts to operational teams within the Information Technology Department and the entire county government network;
5. Assesses new security technologies and threats to determine potential value to protect and defend the enterprise;
6. Prepare for, review, investigate, report, and respond to real-time alerts within the environment;
7. Review real-time and historical reports for security and/or compliance violations;
8. Reviews vulnerability assessments of the county’s systems and networks and implements corrective actions and polices to improve cyber posture.

**Required Knowledge, Skills, and Abilities:**

1. Technical knowledge of enterprise-class technologies such as firewalls, routers, switches,

 wireless access points, VPNs, and desktop and server operating systems;

1. Demonstrate experience implementing and/or enforcing security and compliance
2. Strong writing skills, as well as the ability to articulate security-related concepts to a broad

 range of technical and non-technical staff;

1. Working experience with creating, implementing, and managing a threat hunting program within a corporate environment;
2. Understanding of Microsoft’s enterprise technology platform, including Azure,

 Active Directory, SQL, IIS, Office365, MFA / 2FA authentication, and the Windows server

 and desktop operating systems;

 frameworks such as NIST, Cobit, and ISO;

1. Must be a proficient problem-solver that can work autonomously.

**Education and Experience:**

1. Four-year college degree or equivalent industry training and certifications;
2. Three to five years of experience in a security analyst or related position;
3. One or more of the following certifications: CEH, CISM, CompTIA Security+, CISSP, GSEC
4. Experience with managing and securing both on-premise and hosted systems and

 applications;

1. Experience with application, website, and database security.

**Physical and Environmental Conditions:**

Work demands occasional strenuous effort. For example, handling of moderately heavy boxes, moderately heavy tools, equipment, or materials of up to 30 to 60 pounds.

Work environment involves everyday risks or discomforts which require normal safety precautions typical of such places as offices, meeting or training rooms, residences, or commercial vehicles, e.g., use of safe workplace practices with office equipment, avoidance of trips and falls, observance of fire regulations and traffic signals, and/or working in moderate outdoor weather conditions.

The above job description is not intended as, nor should it be construed as, exhaustive of all responsibilities, skills, efforts, or working conditions associated with this job.

Reasonable accommodations may be made to enable qualified individuals with disabilities to perform the essential functions of this job.

I certify that this is an accurate statement of the essential functions and responsibilities of this position.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

HR Representative Date

Your signature below indicates that you have received a copy of this position description.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature Date