ORANGE COUNTY OCERS EMPLOYEES RETIREMENT SYSTEM

Job Description

Director of Cyber Security

DEPARTMENT	Executive	**REPORTS TO**	Assistant CEO Finance & Internal Operations
TITLE CODE	8029MR	**DATE**	02/23/18
POSITION CODE	R1803750	**ADMINISTRATIVE REVISION**	

Job Summary

Under general direction, establish and maintain an enterprise-wide security management program, which includes procedures and policies designed to protect the agency's information, systems and technology assets from both internal and external threats;

Distinguishing Characteristics

The Director of Cyber Security is an upper management position that reports directly to the Assistant CEO of Finance and Internal Operations and acts as the agency's Information Security Officer. OCERS management staff is expected to uphold the highest standards of accountability, plan sponsor focus, and system efficiency. The Director of Cyber Security is responsible for identifying, evaluating and reporting on cyber security risks, leading agency-wide information security efforts that integrate all aspects of information assurance, providing protection of computer systems, networks and member, financial and confidential data from internal and external threats. The Director of Cyber Security also coordinates, investigates, reports on and leads the recovery efforts of cyber security incidents should they occur.

The Director of Cyber Security position requires a strategic thinker and highly effective leader with knowledge of business management and specific practical knowledge, hands-on skills and technical depth related to information security technology. The Director of Cyber Security is forward thinking and is tasked with anticipating new threats and actively working to prevent them from occurring. The Director of Cyber Security must work with executives and upper management across multiple departments to ensure the security program is working smoothly and effectively.

Performance Attributes

Include but are not limited to the following:

- Lead an information security planning process that establishes an inclusive and comprehensive information security program for OCERS that includes a framework that aligns with OCERS Mission, Vision and Values;
- Establish the security management program goals, objectives, metrics and reporting mechanisms that can measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation and create a roadmap for continual program improvements;
- Develop, implement and maintain security policies, procedures, and practices based on industry best practices and in compliance with agency policies and regulatory requirements and enforce adherence to security practices;
- Develop and implement security projects that address identified risks and business security requirements

- Responsible for safeguarding OCERS information and intellectual property, ensure that the integrity, confidentiality and availability of information is owned, controlled or processed by the agency, and ensure proper privacy protection measures and procedures are followed and updated according to applicable regulations and requirements;
- Lead efforts to assess and evaluate the adequacy of the security controls for OCERS information and technology systems and the impact of new technologies on OCERS overall information security, identifying methods to enhance existing security services and provide direction and guidance and make recommendations to executives as appropriate;
- Monitor security vulnerabilities, threats and events in network and host systems, anticipate new security threats and stay up-to-date with evolving infrastructures;
- Create a framework for roles and responsibilities regarding information ownership, classification, accountability and protection;
- Develop, implement and manage the Computer Security Incident Response Plan and conduct electronic discovery and digital forensic investigations as necessary;
- Develop and manage security talent, engaging/managing third parties as needed to ensure the required capabilities are available either internally or externally;
- Work as a liaison with vendors, legal and contract administration staff to establish mutually acceptable contracts and service level agreements
- Prepare and present reports related to cyber security matters, policies or programs to OCERS Audit Committee and Board of Retirement, making recommendations as appropriate and following through with direction received;
- Prepare and manage the Information Security division's annual budget to reflect information security strategic and operating initiatives;
- Conduct information security risk assessments and risk management processes, providing security risk evaluation, mitigation and solutions to projects and initiatives and work with stakeholders throughout the agency on identifying acceptable levels of residual risk;
- Consult with IT staff to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software;
- Manage and conduct agency-wide cybersecurity training program;
- Design, coordinate and oversee security testing procedures to verify the security of systems, networks and applications, and manage the remediation of identified risks;
- Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and are in compliance with policies and audit requirements;
- Implement procedures to monitor and ensure security patches on the agency's systems are up-to-date.

Qualifications

The minimum qualifications required for entry into the classification are as follows:

Education and/or Experience

- Bachelor's degree from an accredited college or university with a major in Computer Science or related field, a MBA or MS is highly desireable and;
- Eight years of increasingly responsible experience in cybersecurity application and infrastructure, technology management including five years of supervisory and project management experience and;
- Hands on experience with current IT security technologies.

Special Notes, Licenses or Requirements

- Professional information security certifications such as:
    - Certified Information Systems Security Professional (CISSP),
    - Certified Information Systems Auditor (CISA)
    - Certified Information Security Manager (CISM)
    - Similar industry certifications
- Demonstrated understanding of security standards and information security and compliance frameworks, controls and best practices: (i.e. SSAE 16, SOC 2 and SOC3, OWASP Top 10, SANS, NIST)
- Must be an intelligent, articulate and persuasive leader who can serve as an effective member of the upper management team and who is able to communicate complex information technology solutions, computer services and security-related concepts to a broad range of technical and non-technical staff.

Knowledge/Skills/Abilities

The following lists the knowledge, skills, and abilities necessary to perform the essential duties of the position.

Knowledge of:

- Principles, concepts, practices, methods and techniques of effective leadership, information technology management and public administration pertaining to the planning, directing and monitoring of information and systems security;
- Risk management frameworks, processes and best practices related to the management of information and technology risks;
- Security protocols, concepts and best practices as well;
- Cloud and wireless security;
- Remote access protocols;
- Anit-virus, anti-spam, internet filtering and patch management tools
- Intrusion detection/prevention systems
- System technology security testing (vulnerability scanning and penetration testing)

- Developing and documenting security architecture and plans, including strategic, tactical and project plans;
- Effective supervision, training and employee motivation principles, practices and techniques;
- Telephone, office and online etiquette;
- Computer applications and hardware related to the performance of the essential functions of the job;
- Use and support of end user applications (e.g. Microsoft Office) and the ability to document and provide end user training.

SKILLS/ABILITY TO:

- Strong leadership skills the ability to lead cybersecurity operations designed to prevent, detect and respond to a wide range of threats both internally and externally;
- Implement and utilize management theories and principles; project management best practices; work planning and scheduling practices; supervisory and motivation practices;
- Critical thinking with strong problem solving skills and ability to adapt to technological advancements within the industry;
- Establish and maintain strong and effective working relationships with all levels of OCERS personnel, consultants, contractors, vendors, plan sponsors, board members and others regarding a variety of OCERS policies, procedures, and practices;
- Communicate effectively both orally and in writing;
- High level of personal integrity as well as the ability to professionally handle confidential matters and show an appropriate level of judgement;
- Manage technical and professional staff by interviewing, selecting, training, evaluating, and communicating with employees;
- Work with other employees, supervisors, managers and executives to move concepts, projects, and work assignments toward successful completion in a timely manner;
- Work independently and;
- Operate personal computer and word processing, database, and spreadsheet application programs.

Physical, Mental and Environmental Conditions

The physical and mental demands described here are representative of those that are customarily required to successfully perform the essential functions of this class.

Physical and Mental Demands

- Speak and hear well enough to communicate in English clearly and understandably in person, over the telephone, and in small or large groups;
- Manual dexterity sufficient to use hands, arms and shoulders repetitively to operate a telephone, keyboard, mouse and write;

- Mental stamina to interact professionally with members of the Board of Retirement, Plan Sponsors, peers and retirement system members;
- Vision sufficient to read fine print and a computer monitor;
- Independent body mobility, agility, and stamina to stand, walk, stoop, bend, and twist, to access a standard office environment;
- Ability to sit for prolonged periods of time and;
- Body strength sufficient to lift up to 20 pounds.

Mental Demands

- Use written and oral communication skills;
- Read and interpret data, information, and documents;
- Analyze and solve problems;
- Observe and interpret situations and have the poise and ability to act calmly and competently in high-pressure, high stress situations;
- Learn and apply new information or skills and;
- Perform highly detailed work on multiple, concurrent tasks; work under intensive deadlines; and interact with vendors and staff in the course of work.

Environmental Conditions

- The primary work place is in an office environment work with standard office equipment.
- Peripheral office equipment generates to moderate noise level.
- Operates in an environment that includes elected officials, non-elected officials, government agencies, community interest groups and the general public in the development and coordination of OCERS affairs.
- Out of area travel may be required to attend professional conferences and meetings.

ACKNOWLEDGEMENT

By signing below, I acknowledge I have reviewed and discussed the contents, requirements, and expectations included in this job description with my supervisor and a copy has been provided to me.

Employee Signature	Date
Supervisor Signature	Date
HR Signature	Date