ORANGE COUNTY CLASS SPECIFICATION

TITLE: CYBERSECURITY ANALYST **GRADE:** 16

TITLE ABBREVIATION: CYBERSECURITY ANALYST **TITLE NO.:** 568650

JURIS.CL: C **SALARY CODE:** 01 **EEO CODE:** PR **FLSA CODE:** NE

DEPARTMENT: INFORMATION TECHNOLOGY SERVICES **DIVISION:**

SUPERVISOR'S TITLE: DIRECTOR OF CYBERSECURITY

DISTINGUISHING FEATURES OF THE CLASS: This position performs both technical and administrative work involving policy and procedure development regarding data integrity and security. The incumbent monitors security systems and software to ensure the safekeeping and protection of data from unauthorized modification or destruction. The position also monitors, assesses and modifies the disaster recovery program, performs network intrusion testing, application vulnerability assessment scans, and risk assessment reviews. The work is performed under the general supervision of a higher-level manager. Supervision is not a function of this class, The incumbent does related work as required.

TYPICAL WORK ACTIVITIES:

Monitors and advises on information security issues related to both systems and workflow to ensure that internal security controls are appropriate and operating as intended;

Audits and monitors both electronic and physical security of IT systems and networks;

Coordinates a response to information security incidents;

Assists in developing information security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements;

Conducts data classification assessment and security audits and recommends remediation plans;

Keeps abreast of latest security issues;

Reviews findings of vulnerability assessments and works to address the issues;

Audits and monitors security policies for workstations and servers;

Coordinates the reporting of security issues;

Creates, manages and maintains user security awareness;

Works with the Information Technology Management team on developing information security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements;

Provides education on security related matters;

Creates maintains, and tests the County Incident Response Plan;

Conducts and documents both internal and external intrusion and penetration testing;

Collaborates with IT management, the County Attorney, the County Administrator, and law enforcement agencies to manage security vulnerabilities;

Prepares and maintains information security documentation, including department policies and procedures, county-wide notifications, and ITS alerts;

May perform security vulnerability, remediation as required;

Responds to Insurance security risk guest questionnaires.

FULL PERFORMANCE KNOWLEDGE, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS: Thorough knowledge of the principles and practices of computer system security administration; thorough knowledge of accepted information technology practices with regard to data integrity and security; thorough knowledge of firewall management; thorough knowledge of web filtering software and hard, Thorough knowledge of the principles and practices of computer system security administration; thorough knowledge of accepted information technology practices with regard to data integrity and security; thorough knowledge of firewall management; thorough knowledge of web filtering software and hardware; good knowledge of logical operations of data communications devices; good knowledge of local and wide area network administration; working knowledge of data processing methodology and techniques including documentation of data security; working knowledge of data processing methodology and techniques including documentation of data security; ability to implement and maintain computer security policies and procedures; ability to communicate effectively, both orally and in writing; ability to understand and interpret complex technical material; ability to prepare written material, especially system security documentation; ability to define and recommend computer documentation of data security; ability to establish and maintain effective working relationships.

MINIMUM QUALIFICATIONS: Either

(A) Bachelor's degree in computer science, computer technology, data processing, management information systems, information resource management, or related field AND two (2) years of experience in information security systems administration; OR

(B) Associate's degree in computer science, computer technology, data processing, management information systems, information resource management, or related field AND four (4) years of experience in information security systems administration; OR

(C) Graduation from high school or possession of a high school equivalency diploma AND six (6) years of experience in information security systems administration.

SPECIAL REQUIREMENTS: Posses and maintain a valid driver's license. Ability to lift and carry fifty (50) pounds.

Note: Your degree or credits must have been awarded by a college or university accredited by a regional, national, or specialized agency recognized as an accrediting agency by the U.S. Department of Education/U.S. Secretary of Education. If your degree or credits were awarded by an educational institution outside the United States and its territories, you must provide independent verification of equivalency. A list of acceptable companies who provide this service can be found on the Internet at http://www.cs.ny.gov/jobseeker/degrees.cfm. You must pay the required evaluation fee.

ADOPTED 06/15/24