DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY BRANCH
TECH RECOVERY UNIT

DUTY STATEMENT

JOB TITLE: Information Technology Specialist I **POSITION #:** 472-508-1402-XXX

WORKING TITLE: Security Operations Specialist (Central)

EMPLOYEE:

POSITION DESCRIPTION: Under direction of the Vulnerability Management Unit, Information Technology Supervisor II, the Information Technology Specialist I, provides technical expertise and oversight in the security and protection of the Department of Developmental Services' (Department) information assets, and has responsibility to ensure that the Departments information technology assets, and endpoints are protected against the latest published vulnerabilities and hardened to state standards. As part of the Information Security Office (ISO), the incumbent provides monitoring of network activity, system operations and communications to support the Chief Information Security Officer (CISO) and IT management at the local facilities in their mission to ensure compliance with state and federal requirements. The incumbent will be expected to provide knowledge and support to all Department staff for device configuration, installation, patching, and best practices of state issued equipment and to protect Department resources.

SUPERVISION EXERCISED: None.

SUPERVISION RECEIVED: Reports to and under the direction of the ISO Vulnerability Management Supervisor (ITS II) under the Chief Information Security Officer.

EXAMPLES OF DUTIES:

<u>Essential Job Functions</u>:

35% Administer and Maintain vulnerability management technologies and processes to continuously identify and report vulnerabilities affecting Department IT assets. Ensure vulnerability management technologies satisfy SIMM 5345-A standards. Maintain active scanning schedule to ensure accuracy of results and full coverage of all potentially managed assets, including devices located at Department Headquarters, Developmental Centers, and managed cloud environments. Analyze and test veracity of identified vulnerabilities and generate corrective action plans to remediate potential risks. Work with ISO staff to ingest vulnerability management

logs into third-party systems, such as Security Information and Event Management (SIEM) and service request systems.

35% Collaborate with local technical support staff to communicate critical remediation guidance. Notify relevant team members of potential corrective actions to take, and work with them to verify corrective actions are implemented correctly. Conduct follow up activities to detect regressions in remediations and unintentional changes in the Department network. Develop reports to summarize vulnerability management effectiveness and assist in identifying process inefficiencies and gaps.

15% Participate in annual risk and technical standards compliance reviews for Department Systems and IT projects as needed. Conduct quality assurance monitoring of all system changes. Review network status to ensure production changes do not have a negative impact on the network. Validate production changes have been through the “change management process”.

10% Provide regular status briefings of security issues to the CIO, CISO, and local IT Management. Regularly monitor and provide preliminary analysis and categorization of Common Vulnerabilities and Exposures (CVE) and informational alerts from external agencies to the ISO team and coordinates with local IT staff regarding required patches.

Marginal Job Functions:

5% Complete other required duties within the scope of the classification.

WORKING CONDITIONS: Open-spaced partitioned offices; Prolonged periods on a computer a majority of the time. May require 24/7 on call support as well as weekend support. Occasional travel including overnight stays or day trips.

DESIRABLE QUALIFICATIONS:

Knowledge of: Windows Desktop (Win10/Win11) and Server Administration; Familiarity with a variety of system log file types; Hands on experience managing active vulnerability scans and patch management; Strong working knowledge IT networking/infrastructure; Functional knowledge of infrastructure components and the roles they serve; Experience with Cloud based auditing and monitoring (O365, AWS, Azure) a plus.

Ability to: Create scripts using PowerShell, Batch, SQL, and Regular Expressions. Develop and maintain cooperative and harmonious relationships with Department staff and colleagues; analyze situations accurately and take effective action; communicate effectively; reason logically and creatively; analyze data and present ideas and information effectively; review and edit written reports**;** present in front of small and medium sized audiences.

CERTIFICATION OR LICENSE: None.

Employee Name (Print)	Employee Signature	Date

Supervisor Name (Print)	Supervisor Signature	Date

Employee and Supervisor acknowledge that by signing this Duty Statement that they have discussed and agree to the expectations of the position.