DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY BRANCH
SECURITY OPERATIONS UNIT

DUTY STATEMENT

JOB TITLE: Information Technology Associate **POSITION #:** 472-508-1401-XXX

WORKING TITLE: Security Operations Associate **EMPLOYEE**:

POSITION DESCRIPTION: Under the general supervision of the Information Technology Supervisor II, the Information Technology Associate (ITA) serves as the Security Operations Associate. The ITA assists in the implementation, administration, configuration, operation, and maintenance of security technologies and processes. The incumbent helps monitor and protect technology systems and networks, identifies potential risks, and supports routine security tasks necessary for maintaining an effective security posture. Work is performed in alignment with Department of Developmental Services (Department) policies and Statewide standards.

SUPERVISION EXERCISED: None.

SUPERVISION RECEIVED: Under the general supervision of the Information Security Operations Supervisor II.

EXAMPLES OF DUTIES:

DOMAIN(S):	Business Technology Management:	Basic skills
	Client Services:	Basic skills
	Information Security Engineering:	Moderate skills
	IT Project Management:	Basic skills
	Software Engineering:	Basic skills
	System Engineering:	Moderate skills

Essential Job Functions:

35% The incumbent assists in monitoring and operating security tools, analyzing alerts and logs to identify potential threats, and performing initial triage on low-complexity security incidents. Responsible for documenting incident information, supporting routine vulnerability scanning and remediation tracking, and helping maintain secure system configurations and access controls. The role also involves basic forensic data collection under supervision, organizing information for risk and compliance activities, and contributing to the evaluation of new security tools and methods. Additionally, the incumbent supports the

creation and maintenance of security documentation such as runbooks, procedures, and system inventories.

35% The incumbent supports asset management activities by helping maintain accurate inventories of hardware, software, and cloud assets that inform security controls, system configuration, vulnerability management, and event correlation. Ensures Security Operations has the asset data needed to assess risks, support policy and lifecycle planning, and make informed decisions that protect the Department's systems.

20% The incumbent assists in planning and organizing small tasks or workstreams within security-related projects, coordinating schedules, meetings, and project documentation as needed. Responsibilities include tracking assigned action items, reporting progress to supervisory staff, and supporting cross-team communication by preparing notes, summaries, and basic status updates. The role also helps maintain project artifacts, follow established project-management processes, and ensure assigned tasks are completed on time.

Marginal Job Functions:

5% The incumbent is responsible for managing the Department badge process, including coordinating photo collection, producing badges, and ensuring timely distribution to designated areas. This role also includes processing badge-related requests, maintaining accurate records, and ensuring all procedures are completed in accordance with established security and administrative requirements.

5% Other duties as assigned within the scope of the classification.

WORKING CONDITIONS: Work is performed in an open-office environment with partitioned workspaces. Extended use of computer systems and related technology. Availability for 24/7 on-call and weekend support as required. Occasional travel for business-related activities. This position is a hybrid, in-office/telework position, and may be subject to change. Incumbent can be required to report to the office, or any designated location at any time. Telework agreements can be modified and/or cancelled at any time.

DESIRABLE QUALIFICATIONS:

Knowledge of: Core security operations tools and processes, including monitoring and triaging alerts within platforms such as Cortex XDR, Microsoft SIEM/Sentinel, Proofpoint, and ServiceNow; vulnerability management; Tenable One; asset tracking to support security controls and basic configuration and access-control hygiene; cloud environments such as AWS and the ability to support forensic data collection, risk and compliance documentation, and security runbook development is also important; project coordination, maintaining accurate asset inventories, and support physical security tasks such as badge administration.

Ability to: Understand core security operations, including monitoring alerts, performing initial incident triage, supporting vulnerability and configuration management, and maintaining accurate asset inventories; assist with documentation, support project coordination tasks, conduct basic forensic data collection under guidance, and contribute to process improvements.

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.