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

DUTY STATEMENT

JOB TITLE: Information Technology Specialist I **POSITION #:** 472-508-1402-021

WORKING TITLE: Cloud Security Specialist **EMPLOYEE**:

POSITION DESCRIPTION: Under direction of the Security Operations Supervisor (Information Technology Supervisor II), the Information Technology Specialist I performs cloud security operations, security posture monitoring, and cloud telemetry assurance for Department of Developmental Services (Department) cloud-hosted systems. The incumbent evaluates cloud configuration and exposure findings, validates the availability and quality of security logs and alerts, coordinates integration of cloud telemetry with the Department Security Information and Event Management (SIEM) platform, and works with cloud service owners and the Security Operations Unit (SOU) to verify corrective actions. The position supports Amazon Web Services (AWS), Microsoft Azure, and related cloud services without assuming enterprise SIEM administration, digital forensic case ownership, or identity provisioning responsibilities.

SUPERVISION EXERCISED: None.

SUPERVISION RECEIVED: Reports to and under direction of the Security Operations Supervisor (Information Technology Supervisor II).

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

EXAMPLES OF DUTIES:

Essential Job Functions:

35% Cloud Security Posture and Configuration Monitoring. Evaluate AWS and Azure security posture findings, cloud service configurations, exposed services, encryption settings, network access rules, storage protections, and security baselines. Validate findings against approved Department requirements; assess potential impacts and recommend prioritized corrective actions to designated cloud infrastructure and application owners. Track disposition and verify remediation evidence without assuming ownership of production infrastructure changes.

30% Cloud Security Telemetry Monitoring, SIEM Integration, and Event Triage. Identify cloud-native audit, identity, network, workload, and security event sources needed for effective monitoring of AWS and Azure services. Assess whether required logs and alerts are enabled, complete, timely, appropriately retained, and attributable to cloud assets; identify

telemetry gaps and coordinate their correction with cloud service owners. Define cloud-specific monitoring requirements and assist the SIEM & Digital Evidence Analyst with onboarding, field mapping, validation, and use-case testing in Microsoft Sentinel or the designated Department SIEM. Review cloud-native security findings, correlate relevant cloud context, and escalate suspected incidents to the SIEM & Digital Evidence Analyst and incident response lead. Support containment and remediation verification without owning enterprise SIEM administration, correlation-rule maintenance, or forensic case management.

20% Cloud Vulnerability and Exposure Management. Review cloud workload vulnerability findings, externally exposed resources, insecure configurations, and service-specific security advisories. Correlate cloud inventory and asset ownership information; document affected resources, exposure paths, compensating controls, and remediation deadlines. Coordinate technical remediation with infrastructure teams and validate closure or formally documented exceptions.

10% Cloud Security Control Validation, Documentation, and Integration Support. Validate cloud security safeguards, including resource isolation, encryption, audit logging, backup protections, and configuration baselines; document control deficiencies and remediation evidence. Maintain operational procedures, cloud asset-to-owner mappings, technical diagrams, telemetry source inventories, logging coverage records, and response runbooks. Coordinate SIEM integration requirements with the SIEM & Digital Evidence Analyst and identity-related findings with the IAM Specialist. Support cloud service onboarding and technical security assessments without assuming enterprise architecture, policy ownership, or routine infrastructure administration.

Marginal Job Functions:

5% Other duties as assigned within the scope of the classification, including training, exercises, and temporary support during significant cloud security events.

WORKING CONDITIONS: Work is performed primarily in an office or approved telework environment and requires prolonged use of computer systems, analysis of detailed technical information, and coordination during time-sensitive security events. The incumbent may be required to provide after-hours, weekend, or on-call support during significant security incidents. Minimal travel may be required for departmental business including and not limited to, site visits, meetings, or training. 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: AWS and Azure cloud security services, including AWS CloudTrail, CloudWatch, Config, GuardDuty, Security Hub and VPC Flow Logs; Azure Monitor, Activity Logs, Azure Policy, and Microsoft Defender for Cloud, or comparable cloud security solutions; cloud security posture management, vulnerability and exposure assessment, secure cloud configuration, network segmentation, encryption, and cloud incident triage is advantageous; Kusto Query Language (KQL), Tenable or comparable vulnerability platforms, Palo Alto Networks/Panorama telemetry and APIs, ServiceNow, GitHub/DevOps, infrastructure as code, Python or other scripting, and responsible use of generative AI for security analysis.

Ability to: Assess the completeness, timeliness, retention, and asset attribution of cloud audit and security telemetry; coordinating cloud log onboarding, field mapping, and validation with a Microsoft Sentinel or comparable SIEM administrator; and interpreting cloud-native alerts; demonstrate technical writing, risk-based prioritization, collaboration with cloud service owners, and the ability to document defensible findings and remediation evidence.

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.