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

DUTY STATEMENT

JOB TITLE: Information Technology Specialist I **POSITION #:** 472-508-1402-017

WORKING TITLE: Identity and Access Management Specialist

EMPLOYEE:

POSITION DESCRIPTION: Under direction of the Security Operations Supervisor (Information Technology Supervisor II), the Information Technology Specialist I (ITS I) supports identity and access management controls and monitoring across Department systems and data. The incumbent administers access-related processes and tools, review's anomalous identity activity, and coordinates corrective actions to reduce unauthorized access and disclosure risk.

SUPERVISION EXERCISED: None.

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

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

EXAMPLES OF DUTIES:

Essential Job Functions:

35% Support approved provisioning, modification and deprovisioning workflows across Entra ID, Active Directory, Microsoft 365, SaaS and departmental applications. Maintain access assignments and privileged access records according to least privilege and separation-of-duties requirements.

30% Monitor authentication events, access changes, elevated privileges and identity anomalies using departmental security tools, including Varonis capabilities. Investigate exceptions with security operations and coordinate documented remediation.

20% Support multifactor authentication, single sign-on, Conditional Access and directory-based authorization controls; troubleshoot access-related issues and coordinate with system owners.

10% Support identity platform administration, integration with SIEM and ticketing, periodic access reviews, privilege audits and documentation of findings for compliance and remediation tracking. Maintain IAM workflows, exception procedures, access review records and operational documentation; identify opportunities for controlled automation.

Marginal Job Functions:

5% Perform other duties within the scope of the classification, including collaboration with IT operations, Human Resources, application owners and ISO teams.

WORKING CONDITIONS: Work is performed in an office or approved telework environment requiring prolonged computer use, analysis of security events, careful handling of sensitive information, and communication during time-sensitive incidents. Availability for after-hours incident response and occasional travel may be required. 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: Identity and access security, including Microsoft Entra ID, Active Directory, multifactor authentication (MFA), single sign-on (SSO), Conditional Access, privileged access, least privilege, identity lifecycle controls, access certification, and separation of duties; Varonis or comparable platforms to monitor sensitive-data permissions, anomalous access, privilege changes, and potential data exposure; Tenable Identity Exposure or similar identity posture assessment, Microsoft Purview, Microsoft 365, Varonis DSPM/DAM/DLP capabilities, audit logs, Microsoft Sentinel or comparable SIEM integration, and incident case documentation; scripting and automation (such as PowerShell or Python), GitHub/DevOps concepts, secure data handling, NIST-aligned identity controls, HIPAA-sensitive environments, and responsible generative AI use.

Ability to: Analyze access patterns, distinguish approved access from suspicious activity, prepare clear investigative findings, coordinate remediation with account and application owners, and maintain defensible 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.