DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY BRANCH
PRIVACY COORDINATION UNIT

DUTY STATEMENT

JOB TITLE: IT Specialist I **POSITION #:** 472-508-1402-020

WORKING TITLE: GenAI Risk Analyst **EMPLOYEE:**

POSITION DESCRIPTION: Under direction of the Information Technology Supervisor II, the Information Technology Specialist I (ITS I) serves as a Generative AI Risk Analyst within the Information Security & Privacy Section. The incumbent performs technical and risk-based evaluations of proposed, existing, and modified GenAI tools, systems, and AI-enabled software capabilities used by the Department or Regional Centers. The ITS I investigates AI system architecture, model behavior, integrations, and data handling to identify privacy, security, and compliance risks; evaluates safeguards; documents findings and mitigation recommendations; and supports responsible use of GenAI. The ITS I collaborates with program staff, system owners, IT Acquisitions, Legal, and vendors.

SUPERVISION EXERCISED: None.

SUPERVISION RECEIVED: Reports to and under direction of the Information Technology Supervisor II.

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

EXAMPLES OF DUTIES:

Essential Job Functions:

35% Performs GenAI risk assessments, including assessments required under applicable State Administrative Manual and Statewide Information Management Manual requirements (including SIMM 5305-F, as applicable), for proposed GenAI tools, internally developed systems, and AI features introduced through software updates, renewals, modifications, or expanded integrations. Evaluates privacy, security, data governance, access control, data retention, model behavior, and regulatory impacts. Documents GenAI system risks, constraints,

and compliance requirements; Provides recommendations supporting responsible, safe deployment of GenAI within the Department. Serves as the liaison for GenAI-related security and privacy incidents, contributing AI-focused expertise to incident response activities. Contributes technical expertise to GenAI-related privacy and security incident reviews.

25% Reviews GenAI procurement documents, statements of work, and vendor responses for tools proposing deployment in Department and Regional Center environments; Determines alignment with statewide requirements, Department-wide policies, and AI governance rules; Coordinates with Procurement and Legal to address gaps, issues, or compliance concerns; Supports development of contract language related to responsible AI use. Coordinates DDS Headquarters and Regional Center GenAI procurement review processes and leads multi-agency consultations involving DDS, Regional Centers, vendors, CDT, and HHSA.

25% Develops and maintains GenAI risk scoring methodologies, job aids, and evaluation criteria; Creates GenAI system authorization documentation; Ensures consistent application of statewide GenAI governance frameworks: Participates in Department GenAI Governance activities. Manages the Dep0rtment and Regional Center GenAI risk register to ensure centralized tracking of statewide GenAI risks.

10% Advises programs when implementing approved GenAI solutions; Supports responsible use requirements, privacy protections, and security safeguards; Explains data-handling rules to ensure compliance with Department policies. Provides training and guidance to Regional Center staff on privacy-, security-, and compliance-related aspects of approved GenAI solutions.

Marginal Job Functions:

5% Assists in developing guidance, awareness materials, and procedures supporting privacy compliance; participates in project meetings, procurement reviews, and planning sessions to ensure privacy considerations are incorporated appropriately. Other duties as assigned within the scope of the classification.

WORKING CONDITIONS: 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: GenAI risk assessments for HIPAA-covered entities, including evaluation of PHI exposure, data handling controls, and HIPAA compliance; formal GenAI-related training or certification and background in HIPAA privacy/security requirements; developing or reviewing AI or software product documentation, such as architecture diagrams, API specifications, data flow diagrams, or risk/security documentation; applying AI governance, responsible AI principles, privacy/security regulatory requirements, and statewide or enterprise evaluation frameworks (e.g., SIMM 5305-F, SIMM 150, NIST AI RMF, ISO 42001); working with vendors, procurement teams, legal counsel, or product owners to evaluate and negotiate technical or compliance requirements for AI or complex software tools.

Ability to: Evaluate Generative AI or machine-learning systems at a technical level, including understanding model behavior, training data constraints, inference patterns, and system integration impacts; work in software engineering, machine learning engineering, product security, or technical roles, especially involving AI-enabled products or cloud-hosted SaaS platforms; translate AI system behavior, model limitations, and privacy/security risks into clear, actionable guidance for non-technical stakeholders; design or improve risk assessment methods, develop standardized documentation or templates, and maintain structured tracking systems or risk registers; utilize strong analytical skills, including the ability to identify subtle AI risks (hallucinations, data leakage, bias, model drift, retention risks, access misuse, prompt injection) and clearly document findings; serve as a liaison during technical investigations or security/privacy incidents involving AI or complex cloud systems.

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.