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

DUTY STATEMENT

JOB TITLE: Information Technology Specialist I **POSITION #:** 472-508-1402-011

WORKING TITLE: Technology Recovery Specialist HQ

EMPLOYEE:

POSITION DESCRIPTION: Under direction of the Information Technology Supervisor II, the Information Technology Specialist I (ITS I), performs complex analytical and technical documentation duties supporting the Department of Developmental Services' (Department) enterprise Technology Recovery Program. The incumbent reviews and updates ISSP Phase 1 and Phase 2 workbooks, evaluates system risks and dependencies, coordinates recovery documentation with system owners and technical teams, supports incremental system-level BIAs recorded in ISSP workbooks, and assists with enterprise TRP/DRP updates, recovery exercises, and evidence collection. The position supports Department programs and remote locations.

SUPERVISION EXERCISED: None.

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

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

EXAMPLES OF DUTIES:

Essential Job Functions:

35% Coordinate with system owners, custodians, and technical subject matter experts to review, validate, and maintain Information Security Strategy Plan (ISSP) Phase 1 and Phase 2 workbooks. Ensure system architecture, ownership information, recovery objectives, controls, dependencies, and recovery planning data remain accurate, complete, and current. Identify documentation gaps, recovery planning concerns, and potential recovery risks, while supporting enterprise recovery risk reporting, dashboard metrics, and documentation compliance activities. Apply applicable state requirements and federal contingency-planning concepts, including NIST SP 800-34, NIST SP 800-53, FIPS 199/200, and HIPAA where applicable.

30% Support the development, annual review, maintenance, and continuous improvement of enterprise Technology Recovery Plans (TRPs) and system-level Disaster Recovery Plans (DRPs). Collaborate with business and technical stakeholders to document recovery procedures, recovery requirements, system dependencies, technical recovery assumptions, and vendor support needs. Maintain controlled documentation, approvals, version histories, and supporting evidence necessary to demonstrate recovery readiness and compliance with departmental standards.

20% Support the planning, coordination, execution, and documentation of disaster recovery exercises, tabletop exercises, and recovery testing activities. Assist in developing realistic recovery scenarios, capturing exercise outcomes, identifying gaps, preparing after-action reports, and tracking corrective actions through completion. Coordinate with system owners and technical teams to validate recovery procedures, restoration dependencies, and testing results to improve organizational recovery readiness.

10% Coordinate the development and validation of system-level Business Impact Analyses (BIAs) within ISSP workbooks by gathering and documenting recovery requirements, business criticality, downtime tolerance, recovery priorities, and system dependencies. Work with business and technical stakeholders to verify recovery assumptions, identify potential risks, and elevate unresolved issues for management review and risk-based decision-making.

Marginal Job Functions:

5% Perform related recovery planning, documentation management, audit support, compliance tracking, reporting, and coordination activities in support of Technology Recovery Unit objectives. Participate in special projects, process improvement initiatives, training activities, and other assignments as required to support departmental continuity and recovery programs. Other duties as assigned within the scope of the classification.

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: Information Security Strategy Plans (ISSPs), Business Impact Analyses (BIAs), Technology Recovery Plans (TRPs), Disaster Recovery Plans (DRPs), and applicable industry frameworks and standards, including NIST Special Publication 800-34, NIST Special Publication 800-53, FIPS 199, FIPS 200, and State of California information security requirements; developing and maintaining management dashboards, analyzing risk-related information, and administering access controls for sensitive reports and program data; compliance initiatives, audit activities, documentation governance, and records management processes.

Ability to: Collaborate effectively with executive leadership, business stakeholders, technical teams, and external partners in achieving organizational objectives and advancing program maturity.

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.