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

DUTY STATEMENT

JOB TITLE: Information Technology Supervisor II **POSITION #:** 472-508-1404-005

WORKING TITLE: Technology Recovery Unit Supervisor

EMPLOYEE:

POSITION DESCRIPTION: Under general direction of the Information Technology Manager I, Information Security Officer, the Information Technology Supervisor II (ITS II) serves as the working supervisor of the Technology Recovery Unit (TRU) at the Department of Developmental Services (Department). The position provides direct supervisory leadership and performs substantive enterprise technology recovery planning, information system security planning, risk analysis, and program coordination duties.

SUPERVISION EXERCISED: A number of rank-and-file staff/professional staff.

SUPERVISION RECEIVED: Under general direction of the Information Technology Manager I, Information Security Officer.

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% The incumbent leads the Department's Technology Recovery Plan (TRP) and Disaster Recovery Plan (DRP) programs, ensuring enterprise recovery plans are maintained, updated, and coordinated with Department programs, Information Technology Division (ITD) branches, and remote locations. The incumbent provides direct supervision of assigned staff, including workload management, performance evaluations, coaching, training, and quality oversight. The incumbent collaborates with the California Department of Technology (CDT) and departmental stakeholders to identify recovery requirements, manage dependencies, and prioritize remediation efforts.

30% The incumbent is responsible for maintaining the Enterprise System Risk Profile Dashboard, supported by validated Information System Security Plan (ISSP) workbooks, including their Business Impact Analysis (BIA) tabs. The incumbent oversees the Enterprise System Risk Profile Dashboard, ensuring the accuracy, integrity, maintenance, and controlled publication of recovery and risk information. The incumbent establishes data standards and validation

processes for ISSP Phase 1 and Phase 2 workbooks and ensures system criticality, recovery objectives, dependencies, risk findings, and BIA data are accurately maintained. The incumbent reviews enterprise risk trends and prepares management reports to support recovery readiness and informed decision-making.

20% The incumbent oversees the maintenance and reporting of ISO-approved software and hardware records, including approved, denied, pilot, and sunsetting technologies. The incumbent coordinates with the Data Protection Unit (DPU), Privacy Coordination Unit (PCU), and Security Operations (SecOps) to support technology review processes and compliance activities. Responsibilities include maintaining audit-ready documentation, tracking approval status, and ensuring ISO records remain separate from asset inventory and CMDB ownership functions.

10% The incumbent coordinates disaster recovery exercises, tabletop activities, and recovery testing to validate departmental preparedness. Responsibilities include documenting lessons learned, tracking corrective actions, and monitoring progress toward remediation. The incumbent also oversees incremental BIA activities to ensure recovery priorities and objectives remain current and aligned with operational needs.

Marginal Job Functions:

5% The incumbent performs other duties consistent with the mission of the TRU, including participation in special projects and emergency response activities. The incumbent provides coordination and leadership during technology disruptions, recovery events, and other situations requiring recovery support.

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; supporting compliance initiatives, audit activities, documentation governance, and records management processes; supervising staff, assigning and monitoring workloads, conducting performance evaluations, and fostering employee development and accountability.

Ability to: Collaborate effectively with executive leadership, business stakeholders, technical teams, and external partners in achieving organizational objectives and advancing program maturity; communicate effectively, communicate technical, recovery, and risk-related information to both technical and non-technical audiences.

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.