# Position Summary

This summary describes the organization, duties, and requirements of a State of Michigan vacancy.

**Position Code:** DEPSPL2P49N

**Civil Service Class and Level:** DEPARTMENTAL SPECIALIST-2

**Working Title (What the agency calls the position):** Privacy and Information Security Officer, (PISO), Agency Security Officer (ASO)

**Name and Position Code Description of Direct Supervisor:** DOWLING, ARIC W; STATE ADMINISTRATIVE MANAGER-1

**Department/Agency:** LEO-LABOR AND ECON OPPORTUNITY

**Bureau (Institution, Board, or Commission):** Employment and Training

**Division:** Operations - Communications, Experience and Support Services

**Section:** Information & Technology Support

**Unit:**

**Work Location (City and Address)/Hours of Work:** 320 S. Walnut St., Lansing, MI 48933 / Monday – Friday 8:00 am to 5:00 pm

**General Summary of Function/Purpose of Position:** This position will serve as LEO-Employment and Training's (LEO-E&T) Privacy and Information Security Officer (PISO), Agency Security Officer (ASO) and Continuity Coordinator. The PISO and ASO roles are in compliance with the Enterprise Information Management Program (Governor's Executive Directive 2016-14). This position will lead IT security for LEO-E&T including the development, implementation and management of all security policies and procedures and monitoring of information systems to ensure full compliance with state and federal privacy laws and any State of Michigan enterprise-wide privacy framework. Responsibilities are to adopt, advise and support all activities from a data and information standpoint. As the Continuity Coordinator, this position will manage the LEO-E&T Continuity Plan to ensure the continuity of essential functions under all conditions. This work includes maintenance and testing of the plan at least annually.

**Assigned duties and tasks for each duty.**

**Duty 1:** Serves as LEO-E&T's Privacy and Information Security Officer and Agency Security Officer directing the development, implementation and management of all LEO-E&T information security resources.

- Coordinates compliance with state and federal privacy laws and any State of Michigan enterprise-wide privacy framework, and coordinates functions and needs with DTMB and the LEO-E&T Chief Data Steward.
- Advises on best practices related to data privacy and security.
- Provides guidance and information security consultation to LEO-E&T's Chief Data Steward as part of Data Sharing Agreement/Memorandum of Understanding development and maintenance.
- Liaises with Michigan Cyber Security to ensure consistency between enterprise policies and LEO-E&T policies and work to strengthen LEO-E&T's overall security program.
- Shapes privacy strategies across LEO-E&T to address the risk related to the unauthorized use or loss of customer information.
- Creates and/or reviews policies, standards and procedures related to IT security.
- Ensures delivery of initial and subsequent privacy training and orientation to all employees, contractors and other business partners or third parties as applicable.
- Initiates, facilitates and promotes activities to foster information privacy awareness within LEO-E&T and keeps staff informed through regular communications.
- Performs periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the department's other compliance and operational assessment functions.
- Establishes and maintains the LEO-E&T critical systems and functions list and develop and implement methods to ensure protection of private information.
- Coordinates the IT portion of the Internal Control Process (ICE).
- Develops and maintains LEO-E&Ts SSP development guide and its components.

    - Ensures LEO-E&T System Security Plans (SSPs) are in alignment with system continuity plans.
    - Reviews system-related information security plans to ensure alignment between security and privacy practices.
- Facilitates the completion of SSPs, providing guidance to information system owners and business owners and advising on appropriate responses to privacy and information security controls and risk mitigation.
- Responsible for establishing plans for SSP development, reviews and renewals.
- Develops and maintains LEO-E&T's Incident Response Plan and its components.
- Oversee incident response planning and coordination, along with other Departmental personnel and counsel, as appropriate, including investigation of security breaches, complaints, breaches and errors and omissions relating to privacy policies and procedures.
- Serves as information privacy consultant to all divisions within LEO-E&T.
- Cooperates with Human Resources, Civil Rights, Attorney General's Office and other applicable parties in compliance reviews or investigations.
- Coordinates information security policies and information access with LEO-E&T's FOIA coordinator.
- Maintains a high level of ethics, confidentiality and objectivity when performing all job responsibilities.
- Maintains a high level of awareness and understanding of applicable laws, policies, procedures and trends in information security.
- Keeps up to date on the latest information security trends, emerging technology and best practices.

**Duty 2:** Serves as LEO-E&T's Continuity Coordinator, responsible for developing and maintaining a comprehensive business process that incorporates Mission Essential Functions.

- Manages the LEO-E&T Continuity Plan, ensuring the continuity of essential functions under all conditions.
- Coordinates activities within the LEO-E&T Continuity Plan.
- Provides guidance on the security of LEO-E&T essential equipment, services and systems.
- Supports departmental continuity strategies by identifying mission essential functions (MEF) and associated business processes.
- Documents the actions that will be taken to prevent, minimize or restore those MEFs during an emergency or outage.
- Facilitates annual Test, Train & Exercise activities for all of LEO-E&T and details results to support annual updates to the Continuity Plan and supportive resources.

**Duty 3:** Supports bureau continuity functions related to FOIA, Legislative Reporting and Records Management and other duties as assigned.

- Responsible for developing and maintaining Standard Operating Procedures (SOPs) for position-specific tasks, ensuring documentation is accurate, accessible and aligned with current practice.
- Serves on workgroups, councils or committees related to privacy/security.
- Serves as designated continuity backup for FOIA, Litigation, Records Management, Regulatory Rules, Legislative Reporting and eSignature functions.
- Maintains cross-training and familiarity with associated SOPs, systems and reporting cycles to ensure uninterrupted administrative and compliance operations. Coordinates with the FOIA / Records Management Officer to sustain transparency, records retention, and regulatory documentation during coverage periods.
- Performs other related duties as directed.

**Types of decisions made independently and whom or what those decisions affect:** Project, policy and governance execution decisions, and knowing when to escalate them to leadership.
Exercises independent judgment in selecting a course of action to address customer requests, issues and complaints.
Extensive, independent judgment is required. Independently determines key concerns and selects the appropriate methods of response, gathers and reports complex information in the most appropriate manner for the situation, and prioritizes multiple competing inquiries.

**Types of decisions that require the supervisor's review:** New initiatives and those impacting strategic goals regarding privacy and information security.
Resolving significant conflicting privacy and information security priorities across LEO-E&T.
All audit responses related to privacy and information security.
Guidance is sought, when priorities of assignments conflict, executive direction is not clear, policy/procedures are unclear, any activities that will set precedence or have (major) impact on the department or other state agencies, issues are politically sensitive, or issues that are sensitive in nature.

**Physical effort used to perform this job and environmental conditions of this position:** Normal office environment with extended periods of time using a personal computer. Physical effort normally associated with office work/environment. Occasional driving to meetings or training would be required. Some occasional travel within the United States may be required, including overnight stays. May require lifting/moving of files and boxes.

**Names and classes and levels of employees whom this position immediately supervises:**

**The essential functions of this position:** This position will serve as LEO-Employment and Training's (LEO-E&T) Privacy and Information Security Officer (PISO), Agency Security Officer (ASO) and Continuity Coordinator. The PISO and ASO roles are in compliance with the Enterprise Information Management Program (Governor's Executive Directive 2016-14). This position will lead IT security for LEO-E&T including the development, implementation and management of all security policies and procedures and monitoring of information systems to ensure full compliance with state and federal privacy laws and any State of Michigan enterprise-wide privacy framework. Responsibilities are to adopt, advise and support all activities from a data and information standpoint. As the Continuity Coordinator, this position will manage the LEO-E&T Continuity Plan to ensure the continuity of essential functions under all conditions. This work includes maintenance and testing of the plan at least annually.

**The function of the position's work area and how it fits into that function:** The function of the Information & Technology Support section is to develop and oversee the overall strategic and operational aspects of IT within LEO-E&T. This position coordinates the implementation of LEO-E&T privacy/security-related priorities. In consultation with leadership, they will serve as the specialist tasked to lead privacy/security framework efforts throughout LEO-E&T. The Specialist will be responsible for monitoring privacy/security efforts across LEO-E&T to ensure compliance with all agency policies and statewide best practices. This position entails tasks with a high level of complexity, detail, accountability and impact across LEO-E&T.

**Minimum education, experience, and credentials typically needed to perform the position's essential functions:**

**EDUCATION:**

Possession of a bachelor's degree in any major.

**EXPERIENCE:**

**Departmental Specialist 13 - 15**
Four years of professional experience, including two years equivalent to the experienced (P11) level or one year equivalent to the advanced (12) level.

**KNOWLEDGE, SKILLS, AND ABILITIES:**

- Strong knowledge of information security and technology functions, guidelines, best practices, principles and procedures.
- Knowledge of existing state and agency IT security policies and procedures.
- Knowledge of project management principles and practices.
- Ability to communicate effectively, build consensus, facilitate working sessions, and negotiate solutions and alternatives.
- Ability to work in a team environment involving matrix organizations.
- Ability to resolve conflicting high-priority requirements.
- Ability to gather and analyze facts, draw conclusions, define problems, and suggest solutions.
- High level of trust and integrity.
- Ability to prepare and present effective, clear and concise reports and presentations.
- Strong analytical, interpersonal, verbal and written communication skills to accurately document, interpret and explain complex information, and communicate / interface effectively across all staff levels, customers and vendors.
- Work on tasks that are complex in nature where judgment is required in analyzing, interpreting and making recommendations to resolve non-routine issues.

**CERTIFICATES, LICENSES, REGISTRATIONS:**
None