Position Summary

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

Position Code: DEPTMGR4D50N

Civil Service Class and Level: Departmental Manager-4

Working Title (What the agency calls the position): Security, Compliance, Access, & Network Section Manager / Information System Security Officer (ISSO)

Name and Position Code Description of Direct Supervisor: LARRISON, RYAN M; STATE ADMINISTRATIVE MANAGER-2

Department/Agency: STATE POLICE

Bureau (Institution, Board, or Commission): Information and Technology Bureau

Division: Information Technology Division

Section: Security, Compliance, Access, and Network Section

Unit:

Work Location (City and Address)/Hours of Work: 7150 Harris Drive, Dimondale, MI 48821 / Monday - Friday 8 a.m. to 5 p.m.

General Summary of Function/Purpose of Position: This position functions as the Information Systems Security Officer (ISSO) for Michigan State Police (MSP) internal information systems responsible for maintaining the operational security posture and regulatory compliance of MSP internal information systems. This position is responsible for performing routine risk assessments, enforcing security policies, and managing system authorization documentation.
This position ensures that MSP's internal information systems meet appropriate security standards (e.g. CJIS, 28CFR, NIST, and State of Michigan/Department of Technology, Management and Budget (DTMB) policies). The position is responsible for defining security standards on all internal MSP information technology systems and for coordinating with security partners (The Criminal Justice Information Center (CJIC), DTMB, Michigan Cyber Security (MCS), etc.). This position evaluates data, privacy, and security posture, making recommendations to division command on risk management strategies and risk/reward scenarios related to them, weighing the benefit to MSP members vs. the risk of a data breach. This position also may be called upon to create policies to ensure compliance for securing internal MSP database and application environments, thereby ensuring regulatory and other best practices are maintained and followed. The position is required to perform all duties in a bias free manner.
This position will function as a second-line professional manager of professional positions in a complex work area.

Assigned duties and tasks for each duty.

Duty 1: Supervise Staff and Manage the Section

- Write section strategic plan, maintain records, prepare reports and perform other routine tasks associated with the position.
- Set goals and objectives for the section and ensure they are aligned with division and department goals and objectives.
- Hire and train personnel and organize the section as needed.
- Monitor work flow, set priorities and make work assignments.
- Monitor employee work performances, provide guidance, and take disciplinary action as necessary.
- Set section operating policies and procedures and ensure documentation is in place and adhered to.
- Conduct staff meetings and inform employees of changes in procedures, polices or workflows, etc.
- Identify training needs of staff and ensure the needs are met.
- Assign specialized tasks or special projects to staff based on the employee's strengths, experience and work performance.
- Other duties as assigned.

Duty 2: Policy Development and Training

- Ensure the development and delivery of training programs for MSP personnel.
- Oversee development of security policies affecting internal MSP systems.
- Oversee communications regarding policy changes and security advisories for the MSP relative to internal MSP and State of Michigan (SOM) systems.
- Oversee and coordinate outreach regarding security issues to all MSP divisions and districts regarding internal MSP and SOM systems.
- Provide guidance for staff performing research and development to identify potential security solutions or issues.
- Oversee Security Awareness Training development, delivery, and completion for MSP personnel.
- Develop security policy for internal MSP data following state and federal policies (CJIS, 28 CFR, etc.)
- Ensure technical compliance with CJIS Security Policy for internal MSP systems.

Duty 3: Oversee Network Access and Threat Assessment

- Manage the process for firewall rule changes impacting internal MSP systems.
- Oversee the process for agencies to connect via LGNet or Gateway to Gateway VPN when there is a MSP nexus.
- Oversee the SecurID token and Client VPN ordering and approval process for MSP and DTMB vendors working on MSP systems.
- Oversee the approval process for Gateway to Gateway Requests.
- Administer the process for requesting, creating and distributing client VPNs.
- Oversee the evaluation of vendor solutions for internal MSP systems in cooperation with the CJIS Systems Officer (CSO) and CJIS Information Security Officer (ISO) for compliance with CJIS and other Security Policy.
- Oversee and direct access control management for systems department wide.
- Establish and maintain department-wide policy and procedure for creating, modifying and terminating access as well as audit procedures to assure compliance.
- Establish and communicate processes for monitoring and reviewing user access for users of department systems.
- Oversight of the process to review hardware and software requests and ensure compliance with CJIS and other Security Policy.
- Manage the process to request, implement, and evaluate SOM Information Technology Policy Exception requests for the agency.

Duty 4: Act as the Information Systems Security Officer for the MSP on Internal MSP Systems

- Act as a privacy policy liaison, developing, implementing and maintaining policies and procedures to ensure protection of department's internal IT assets and data.
- Review SOM and CJIS Policy and work with the CJIS CSO and CJIS ISO to resolve issues/concerns ensuring federal requirements are also met.
- Ensure that security incident responses involving MSP personnel are documented, and reporting procedures followed.
- Represent the MSP at conferences.
- Act as a point of contact between divisions, districts, and the DTMB when technical assistance is required

Duty 5: Act as the department Privacy Protection Officer

- Oversee the development and maintenance of the agency privacy notice for applications.
- Oversee the development of policies and procedures related to data usage inside the department.
- Coordinate, develop and manage policies, procedures, and approval paths to determine authorized access to department applications and data where applicable to regulation and law.
- Act as liaison to the DTMB and appropriate business owners to classify data.

Duty 6: Other duties as assigned

- Other duties as assigned by the division commander.
- Serve as the alternate LEIN TAC Officer when necessary.
- Serve on committees and attend meetings as needed.
- Provide assistance and support to other division and district personnel.
- Independently provide analysis and testing of other applications within the division's charge.
- Work with division and bureau leadership on innovations in Security, Access, and the Single Sign on Portal.
- Represent the department during audits when related to job duties.

Types of decisions made independently and whom or what those decisions affect: Assigning work to subordinates, performance review, system maintenance, security and data classification, evaluation, and approvals. Policy development and implementation. This affects all members of the department and affects procedures for IT asset and data protection.

Types of decisions that require the supervisor's review: Consultation with the supervisor is necessary when an unwritten policy or past practice requires clarification or when a new policy will create a change to a data classification or security requirement.

Physical effort used to perform this job and environmental conditions of this position: Occasional travel.

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

MAINZ, RYAN M	DEPARTMENTAL SPECIALIST-2 13
SMITH, TARA L	DEPARTMENTAL MANAGER-3 14
INGHAM, BRYAN	DEPARTMENTAL SPECIALIST-2 13
TWIGG, THOMAS J	DEPARTMENTAL SPECIALIST-2 13

The essential functions of this position: This position functions as the Information Systems Security Officer (ISSO) for Michigan State Police (MSP) internal information systems responsible for maintaining the operational security posture and regulatory compliance of MSP internal information systems. This position is responsible for performing routine risk assessments, enforcing security policies, and managing system authorization documentation.
This position ensures that MSP's internal information systems meet appropriate security standards (e.g. CJIS, 28CFR, NIST, and State of Michigan/Department of Technology, Management and Budget (DTMB) policies). The position is responsible for defining security standards on all internal MSP information technology systems and for coordinating with security partners (The Criminal Justice Information Center (CJIC), DTMB, Michigan Cyber Security (MCS), etc.). This position evaluates data, privacy, and security posture, making recommendations to division command on risk management strategies and risk/reward scenarios related to them, weighing the benefit to MSP members vs. the risk of a data breach. This position also may be called upon to create policies to ensure compliance for securing internal MSP database and application environments, thereby ensuring regulatory and other best practices are maintained and followed. The position is required to perform all duties in a bias free manner.

The function of the position's work area and how it fits into that function: This position is responsible for monitoring compliance with the laws, policies, and procedures that impact data integrity and the security of the system used to communicate information to and from the MSP.

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 Manager 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.

Alternate Education and Experience

Department Manager 15
Education level typically acquired through completion of high school and two years of safety and regulatory or law enforcement experience at the 14 level; or, one year of safety and regulatory or law enforcement experience at the 15 level, may be substituted for the education and experience requirements.

KNOWLEDGE, SKILLS, AND ABILITIES:
Working knowledge of best practices in cyber security.

CERTIFICATES, LICENSES, REGISTRATIONS:
N/A