STATE OF OREGON
POSITION DESCRIPTION

Position Revised Date:
January 7, 2026

This position is:

☐ Classified
☐ Unclassified
☐ Executive Service
☒ Mgmt Svc – Supervisory
☐ Mgmt Svc – Managerial
☐ Mgmt Svc - Confidential

Agency: The Department of Administrative Services

Division: Enterprise Information Services

☐ New ☒ Revised

SECTION 1. POSITION INFORMATION

a. Classification Title: IT Cyber Security Manager 2
b. Classification No:
c. Effective Date:
d. Position No: 26548
e. Working Title: SOC Manager
f. Agency No:
g. Section Title: Cyber Security Services
h. Budget Auth No:
i. Employee Name:
j. Repr. Code: OAS
k. Work Location (City – County): Salem / Marion
l. Supervisor Name: Les DeFoor (Security Operations Center Director)

m. Position: ☒ Permanent ☐ Seasonal ☐ Limited Duration ☐ Academic Year
☒ Full-Time ☐ Part-Time ☐ Intermittent ☐ Job Share

n. FLSA: ☒ Exempt ☐ Non-Exempt

If Exempt: ☒ Executive ☐ Professional ☐ Administrative

o. Eligible for Overtime: ☐ Yes ☒ No

SECTION 2. PROGRAM AND POSITION INFORMATION

a. Describe the program in which this position exists. Include program purpose, who's affected, size, and scope. Include relationship to agency mission.

The Department of Administrative Services (DAS) is the central administrative agency that leads state government to implement the policy and budget decisions of the Governor and Oregon Legislature. Employing an enterprise-wide perspective, DAS serves state government by developing and upholding accountability standards to ensure productive and efficient use of state government's financial, human and information resources.

DAS provides a stable management infrastructure and essential business services including technology, financial, procurement, publishing/distribution, human resources and facility asset management. These services support and enable state and local government agencies to carry out their missions, benefiting all Oregonians.

Enterprise Information Services (EIS) is a state government-wide information technology (IT) organization led by Oregon's State Chief Information Officer (CIO). The State CIO is a statutory position, appointed by the Governor, and works closely with the State Chief Operating Officer (COO) and state leadership on adoption of statewide IT policies, standards, and governance. EIS has independent statutory authority and is aligned with the Department of Administrative Services (DAS) budget. EIS has over 300 FTE and is funded by assessment and rates charged for the services provided.

EIS provides centralized oversight for enterprise-wide IT resource management, planning, policy, program development, project delivery and the establishment and maintenance of statewide IT standards. EIS provides training, and direction to ensure IT integrity, security, and consistency across state agencies by working closely with elected officials, political subdivisions, state agencies and IT leadership. The EIS team is built on collaboration, support, and accountability. We work together to ensure our customer agencies receive the highest quality of service. We take pride in our work and look for ways to innovate.

EIS is committed to hiring highly skilled, diverse, and dedicated employees who will bring a unique skill set to the team. EIS is comprised of the following programs: Administrative Services, Cyber Security Services, Data Center Services, Data Governance and Transparency, Project Portfolio Performance, Shared Services, and Strategy and Design.

Cyber Security Services brings together enterprise security - governance, policy, procedure, and operations - under a single, accountable enterprise organization. This allows for end-to-end direction setting and execution for enterprise security.

The team is comprised of a cybersecurity risk governance policy and standards section for setting enterprise security policy and the associated controls to ensure compliance to standards and best practices, a solutions section driving enterprise security architecture, a network security services section to deliver on day-to-day enterprise network security provisioning, and a security operations center – providing dedicated, real-time security monitoring and incident response across enterprise. Cyber Security Services staff maintain certifications in multiple cyber disciplines and work collaboratively with key local and federal partners, EIS teams to deliver secure solutions to our statutory customers.

This position is designated as an "Essential Position" (State Policy #60.015.01) in all cases of official state office closures. The incumbent in this position is required to report to work in all cases of official notification of state office closures. Exceptions: previously approved vacation and absences. This position may be assigned tasks outside the normal position duties to respond to the special conditions of the closures. If reporting to your normal work location is deemed too dangerous, then you must contact your supervisor to be reassigned to an alternate and/or remote location.

b. Describe the primary purpose of this position, and how it functions within this program. Complete this statement. The primary purpose of this position is to:

The primary purpose of this position is to manage the day-to-day operations of the State of Oregon's Security Operations Center (SOC), ensuring continuous monitoring, detection, analysis, and response to cybersecurity threats impacting enterprise systems and agency services.

This position functions as the operational manager for SOC services, translating enterprise cybersecurity strategy, policy, and priorities established by Cyber Security Services leadership into effective, repeatable, and measurable security operations outcomes.

Operating within a Team of Teams model, the SOC Manager 2 coordinates people, processes, and technology across Security Operations, Network Security, Cloud Security, Governance Risk and Compliance, Data Center Services, and agency IT teams to ensure timely threat detection, incident response, and vulnerability remediation. Rather than owning enterprise-wide strategy, this role focuses on execution, operational alignment, and service reliability across interconnected teams.

The SOC Manager 2 is accountable for supervising SOC analysts and operational staff, maintaining 24x7 SOC readiness and response capability, ensuring SOC tools, workflows, and escalation paths function effectively, and supporting agency partners during incidents through coordinated response efforts.

Through strong operational leadership and cross-team collaboration, this position helps reduce enterprise cyber risk, improve incident response outcomes, and strengthen statewide security posture.

SECTION 3. DESCRIPTION OF DUTIES

List the major duties of the position. State the percentage of time for each duty. Mark "N" for new duties, "R" for revised duties or "NC" for no change in duties. Indicate whether the duty is an "Essential" (E) or "Non-Essential" (NE) function.

Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*

% of Time	N/R/NC	E/NE	DUTIES
35%	R	E	**SOC Operational Leadership and Management** Lead and manages the day-to-day operations of the State of Oregon's Security Operations Center, ensuring continuous monitoring, detection, analysis, and response to cybersecurity threats impacting enterprise systems and agency services. This position provides operational leadership for SOC functions including Security Information and Event Management (SIEM), threat detection, threat response, vulnerability management, cybersecurity incident response, and services that support agency secure configuration requirements. Ensures established SOC processes, procedures, playbooks, and escalation paths are consistently executed and aligned with enterprise security policies and standards. The position oversees alert triage, incident prioritization, and response activities, exercising judgment based on risk, potential impact, and available resources. Establishes and maintains the people, processes, and technologies required to deliver reliable and effective security operations services. Operational performance is monitored through defined metrics and service indicators, and the manager implements adjustments to improve efficiency, effectiveness, and service quality. This role is accountable for maintaining 24x7 SOC operational readiness, including shift scheduling, on-call coverage, and workload balancing, to ensure uninterrupted security monitoring and response capabilities.
30%	R	E	**Staff Supervision and Workforce Leadership** Provides direct supervision and leadership to professional, technical, and support staff assigned to the Security Operations Center. Supervisory responsibilities include interviewing and selecting staff, onboarding, assigning and planning work, evaluating performance, resolving conflicts and grievances, and initiating disciplinary actions when necessary. Ensure recruitment, selection, and retention practices support affirmative action, equal employment opportunity, and diversity goals. Mentors SOC staff and supports professional development by identifying training needs, recommending curriculum, and assisting with implementation.

			Fosters a collaborative, respectful, and accountable work environment that supports high performance in a high-pressure, incident-driven operational setting. Ensures staffing levels, skill coverage, and shift assignments align with operational demand and emerging threat conditions and communicates workforce risks or gaps to SOC leadership as appropriate.
20%	R	E	**Incident Response Coordination** Serves as the operational lead for security incident response activities within the Security Operations Center. Operating within a Team of Teams model, the position coordinates SOC activities with Network Security, Cloud Security, Governance Risk and Compliance, Data Center Services, and agency IT teams to ensure effective detection, containment, escalation, and recovery during cybersecurity incidents. Collaborate with other cybersecurity teams, state agencies, and external partners to coordinate incident response efforts. Coordinate activation of the cyber command teams and work to mobilize resources. Ensure effective communication and reporting during significant cybersecurity incidents. Ensures shared situational awareness across participating teams, facilitates timely and accurate communications, and supports leadership briefings during active incidents. Decisions related to incident escalation, response actions, and coordination are made in alignment with established policies and the strategic direction provided by SOC and CSS leadership. Lead incident response activities, including containment, eradication, and recovery efforts Following incidents, the manager supports post-incident reviews and root cause analysis by ensuring timelines, findings, and lessons learned are documented and shared. These insights are used to improve SOC processes, strengthen response capabilities, and reduce the likelihood of recurrence.
10%	R	E	**Tools, Processes, and Service Improvement** Provides operational oversight for systems and tools used to deliver security operations services, including SIEM, threat detection, and incident response platforms. The position evaluates the effectiveness of SOC tools, workflows, and procedures, and identifies opportunities for improvement related to alert quality, automation, response consistency, and operational efficiency.

			Recommends process, tooling, or staffing adjustments to SOC leadership and supports implementation of approved enhancements. Manage and optimize security tools and technologies within the SOC to maximize threat detection and response capabilities. Ensure that security tools are updated, configured correctly, and integrated effectively. Ensure staff are trained and operationally prepared to adopt new tools or workflows with minimal disruption to services. Utilizes threat intelligence to enhance the SOC's capabilities in detecting and mitigating emerging cyber threats.
5%	R	NE	**Outreach, Collaboration, and Other Duties** Works collaboratively with information security teams and other technical organizations within state government to build strong working relationships, share operational information, and improve collective readiness. Works with agency IT leaders and technical staff to support incident coordination, operational planning, and understanding of SOC services, response expectations, and escalation procedures. Participates in cross-functional working groups, training exercises, and operational planning activities related to security operations, and performs other related duties as assigned.
100%			

SECTION 4. WORKING CONDITIONS

Describe any on-going working conditions. Include any physical, sensory, and environmental demands. State the frequency of exposure to these conditions.

This position is suitable for remote or hybrid work options, subject to business and operational needs.

Requires extended use of computer equipment, including desktop or laptop computers, multiple monitors, keyboards, and other peripheral devices.

The employee will spend significant portions of the workday typing, viewing, analyzing, and interpreting information displayed on electronic screens.

May require prolonged periods of sitting or standing while performing tasks, with limited opportunities for movement during active incidents or operational monitoring periods.

Work is performed in an office or remote environment that may be highly dynamic and distracting, requiring frequent task switching, sustained concentration, and the ability to rapidly refocus attention in response to alerts, incidents, or operational demands.

The employee must be able to function effectively in a fast-paced, incident-driven environment where interruptions are common, and priorities may change quickly. The position requires the ability to analyze complex information, make timely decisions, and communicate clearly during high-pressure situations.

Duties are primarily performed in an office or remote environment working at a computer terminal for extended periods of time. The position may involve working in or around noisy equipment or environments when coordinating with technical teams or during on-site response activities.

Business needs require availability outside of standard business hours. This may include working irregular hours, evenings, weekends, holidays, or overnight shifts in support of 24x7 Security Operations Center activities, incident response, maintenance, or system changes that cannot be performed during standard hours of 6:00 a.m. to 6:00 p.m.

Business needs may require reassignment to one of three shifts (day, swing, or graveyard), sometimes with limited advance notice, to ensure continuous SOC operations and adequate management coverage during incidents or staffing shortages.

Requires the ability to respond promptly to urgent incidents, including after-hours notifications.

Driver's license is required or satisfactory means of transportation.

SECTION 5. GUIDELINES

a. List any established guidelines used in this position, such as state or federal laws or regulations, policies, manuals, or desk procedures.

This position is designated as an "Essential Position" (State Policy #60.015.01) in all cases of official state office closures. The incumbent in this position is required to report to work in all cases of official notification of state office closures.

Exceptions: previously approved vacation and absences. This position may be assigned tasks outside the normal position duties to respond to the special conditions of the closures. If reporting to your normal work location is deemed too dangerous, then you must contact your supervisor to be reassigned to an alternate and/or remote location.

Oregon Revised Statutes

- Oregon Administrative Rules
- Department of Administrative Services Policies and Procedures
- Enterprise Information Security Strategy
- EIS Strategic and Section Plans
- Statewide Information Security Plan & Standards
- Center for Internet Security (CIS)
- NIST SP 800-53 R5 Security and Privacy Controls
- NIST SP 800-30 Risk Management Guide for Information Technology Systems
- NIST SP 800-37 Guide for Applying the Risk Management Framework
- All Other Applicable Statewide, DAS, and EIS Policies, Procedures and Standards
- Federal and State government regulations including:
    - Criminal Justice Information Services (CJIS)
    - Federal Information System Management Requirements (FISMA)
    - IRS Publication 1075
    - HIPAA Security and Privacy Rules
    - Oregon Consumer Information Protection Act

Other Best Practices Resources, such as ISO 27000 series, Common Criteria, National Institute for Standards and Technology (NIST SP-800 series), CIS Controls, etc…

b. How are these guidelines used?

The above guidelines provide general guidance and policy directions, and a framework that should be applied as necessary for each application. This includes decisions concerning the appropriate application and interpretation of policies and procedures that relate to highly sensitive confidential information.

They are used to determine correct operational procedures necessary for efficient and secure operation of statewide computer systems including work processes and procedures that ensure consistent quality of services.

SECTION 6. WORK CONTACTS

With whom, outside of co-workers in this work unit, must the employee in this position regularly come in contact?

Note: If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".

Who Contacted	How	Purpose	How Often?
Agency Customers	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily
Managers/co-workers	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily
Vendors	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries, coordination	Daily
Other State Employees	In person, phone, email, by letter or electronic means	Problem solving, disputes, requests, and inquiries	Daily
Outside Governmental Officials	In person, phone, email, by letter or electronic means	Program overview, problem solving, dispute resolution, incident command, planning and other inquiries	Frequently

SECTION 7. POSITION RELATED DECISION MAKING

Describe the typical decisions of this position. Explain the direct effect of these decisions.

Exercises independent judgment in managing day-to-day Security Operations Center activities, including prioritizing alerts, incidents, and response actions based on risk, potential impact, and available resources.

Makes operational decisions regarding incident escalation, containment strategies, and coordination with internal agencies and external partners, while ensuring alignment with established policies and the strategic direction set by SOC and Cyber Security Services leadership.

Determines staffing assignments, shift coverage, and workload distribution to maintain continuous SOC operations and effective response capabilities.

Makes operational decisions related to SOC staffing levels, tool utilization, and service delivery priorities within approved budgets, and recommends budget adjustments or funding needs to SOC and Cyber Security Services leadership.

Evaluates the operational effectiveness of SOC tools, processes, and procedures, and recommends adjustments or improvements to enhance detection, response, and efficiency.

Balances competing operational demands, regulatory requirements, and resource constraints, making timely decisions during high-pressure incidents that may affect multiple agencies or critical state services.

SECTION 8. REVIEW OF WORK

Who reviews the work of the position?

Classification Title	Position Number	How	How Often	Purpose of Review
IT Cyber Security Manager 3		In person, phone, email, by letter or electronic means	Daily/Weekly/Quarterly	To determine if corrective actions or directions are needed. To stay informed of active threats. Performance reviews

SECTION 9. OVERSIGHT FUNCTIONS THIS SECTION IS FOR SUPERVISORY POSITIONS ONLY

a. How many employees are directly supervised by this position? 11

How many employees are supervised through a subordinate supervisor? 0

b. Which of the following activities does this position do?

☒ Plan work
☒ Assigns work
☒ Approves work
☒ Responds to grievances
☒ Disciplines and rewards

☒ Coordinates schedules
☒ Hires and discharges
☒ Recommends hiring
☒ Gives input for performance evaluations
☒ Prepares & signs performance evaluations

SECTION 10. ADDITIONAL POSITION-RELATED INFORMATION

ADDITIONAL REQUIREMENTS: List any knowledge and skills needed at time of hire that are not already required in the classification specification:

This position is subject to a criminal records check, which may require fingerprints. If you are offered employment, the offer will be contingent upon the outcome of a criminal records check (FBI). Any history of criminal activity will be reviewed and could result in the withdrawal of the offer or termination of employment.

This position is required to maintain an active Criminal Justice Information Services (CJIS) background clearance and must successfully complete annual CJIS security awareness training to retain access to sensitive systems and data.

You are responsible for promoting and fostering a diverse and discrimination/harassment-free workplace; establish and maintain professional and collaborative working relationships with all contacts; contribute to a positive, respectful and productive work environment; maintain regular and punctual attendance; perform all duties in a safe manner; and comply with all policies and procedures.

Working in a team-oriented environment requires participative decision making and cooperative interactions among staff and management. You are to be aware of Affirmative Action and the department's Diversity strategies and goals.

Additional skills, abilities and requirements:

Technical and Operational Competencies

- Employee is required to possess and maintain a valid driver's license issued by the state where the employee resides or provide an acceptable alternate mode of transportation.
- Demonstrated knowledge of IT service management and operational practices such as ITIL, including incident management, problem management, change coordination, and service delivery in a 24x7 environment.
- Strong technical foundation in cybersecurity operations, including threat detection, incident response, vulnerability management, and security monitoring across on-premises, cloud, and hybrid environments.
- Working knowledge of SOC technologies such as Security Information and Event Management (SIEM) platforms, endpoint detection and response tools, log management, and alerting systems.
- Experience managing or supporting systems administration and operational support functions, with an understanding of how infrastructure, applications, and security controls interact in enterprise environments.
- Ability to work with and protect highly sensitive, confidential, or proprietary information in accordance with state policy, legal requirements, and regulatory obligations.
- Demonstrated ability to build, motivate, and sustain effective operational teams, including fostering teamwork, accountability, and resilience in high-pressure environments.
- Strong analytical and problem-solving skills, including the ability to assess complex technical and operational issues and drive corrective actions across multiple teams or organizations.
- Excellent written and verbal communication skills, including the ability to document incidents, operational decisions, and lessons learned in a clear and professional manner.
- Ability to establish and maintain effective working relationships with supervisors, peers, subordinates, agency partners, vendors, and the public.
- Ability to explain complex cybersecurity and technical issues to non-technical audiences in a clear, concise, and actionable manner.
- Regular and reliable attendance is required to meet the operational demands of a 24x7 Security Operations Center and to provide necessary services.

Behavioral Expectations

- Prepare for meetings by identifying operational issues, risks, and proposed solutions, and actively contribute to team decision-making.
- Share in leadership responsibilities and actively support decisions made by Cyber Security Services and SOC leadership.
- Participate in cross-functional, operational, or problem-solving teams as needed to support security operations and incident response objectives.
- Demonstrate accountability, professionalism, and sound judgment in all interactions, particularly during high-impact or time-sensitive incidents.

Problem Solving and Decision-Making

- Ability to analyze complex security incidents and determine appropriate response actions under time-sensitive and high-pressure conditions.
- Skill in prioritizing competing incidents, alerts, and operational demands based on risk, potential impact, service criticality, and available resources.
- Ability to identify gaps in SOC processes, tooling, staffing, or procedures and develop practical, operationally focused corrective actions.
- Skill in applying cybersecurity frameworks, policies, standards, and procedures to novel, ambiguous, or rapidly evolving situations.
- Ability to evaluate operational data, metrics, and trends to inform decisions, improve SOC performance, and support continuous improvement.
- Capacity to exercise sound judgment during incidents affecting critical systems, essential services, or multiple state agencies.
- Ability to balance operational effectiveness with compliance, legal, regulatory, and policy requirements.

Interpersonal and Communication Skills

- Ability to supervise, coach, and motivate technical staff in a 24x7 operational SOC environment.
- Skill in building trust, credibility, and effective working relationships with SOC analysts, agency security staff, leadership, and external partners.
- Ability to manage conflict and resolve issues among staff or between participating teams and agencies in a constructive manner.
- Ability to foster collaboration across diverse technical teams, organizations, and stakeholders using a Team of Teams operating model.
- Skill in mentoring staff and supporting professional development, knowledge sharing, and succession planning.
- Ability to adapt leadership and communication style to varying experience levels, operational conditions, and incident severity.
- Demonstrated emotional intelligence, professionalism, and composure during stressful or high-impact incidents.
- Ability to prepare concise, accurate written reports, incident summaries, and operational briefings for technical and non-technical audiences.
- Ability to deliver clear verbal briefings to leadership during active incidents and post-incident reviews.
- Skill in translating threat intelligence, operational findings, and technical data into actionable risk information.
- Ability to clearly communicate expectations, priorities, and performance feedback to staff.
- Ability to coordinate communications across agencies and with external partners during incidents and recovery activities.
- Skill in documenting decisions, actions, and outcomes in accordance with policy, audit, and legal requirements.

BUDGET AUTHORITY: If this position has authority to commit agency operating money, indicate the following:

Operating Area	Biennial Amount ($00000.00)	Fund Type
N/A	N/A	N/A

Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*

SECTION 11. ORGANIZATIONAL CHART

Attach a current organizational chart. Be sure the following information is shown on the chart for each position: classification title, classification number, salary range, employee name and position number.

SECTION 12. SIGNATURES

Employee Signature Date Supervisor Signature Date

Appointing Authority Signature Date