STATE OF OREGON
POSITION DESCRIPTION

Position Revised Date:
January 2025

Agency: Department of Administrative Services

Division: Enterprise Information Services (EIS)

☐ New ☒ Revised

This position is:
☐ Classified
☐ Unclassified
☐ Executive Service
☐ Mgmt Svc – Supervisory
☒ Mgmt Svc – Managerial
☐ Mgmt Svc - Confidential

SECTION 1. POSITION INFORMATION

a. Classification Title:	Operations and Policy Analyst 4	**b.** Classification No.:	X0873
c. Effective Date:	1/1/2025	**d.** Position No:	1987201
e. Working Title:	Information Security Awareness & Training Program Coordinator	**f.** Agency No:	10700
g. Section Title:	Cyber Security Services (CSS)	**h.** Budget Auth	001300500
i. Employee Name:		**j.** Repr. Code:	MMN
k. Work Location (City – County):	Salem - Marion		
l. Supervisor Name (Optional):	Ryan Mikesh		

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, benefitting all Oregonians.

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

The EIS provides centralized oversight for enterprise-wide IT resource management, planning, policy, program development, project delivery and the setting of statewide IT standards. The 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 and support. 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. The Office is comprised of the following sections: Data Center Services, Project Portfolio Performance, Cyber Security Services, Data Governance and Transparency, Strategy and Design, and Enterprise Shared Services.

Cyber Security Services ("CSS") is an information security management section within the EIS. It acts as a shared information security resource for the state of Oregon. EIS's mission: Mature enterprise technology governance, optimize investments, ensure transparency, provide oversight, and deliver secure and innovative solutions. CSS comprised of the following Teams:

- Enterprise Security Services: This team's focus will be on execution of core security services delivered by CSS for the entire enterprise. Services to be included in the catalog will be developed over time, as will allocation of resources to this team.
- Enterprise Security Operations Center: This team will deliver on the Rapid Detection, Response, & Recovery strategic objective of the Enterprise Information Security Strategy. This team includes 3 main disciplines: Detection, Vulnerability Management, and Incident Response.
- Governance, Risk, and Compliance: This team's focus is on the Open, Empowered Culture of Security and Proactive, Holistic Risk Management objectives of the Enterprise Information Security Strategy. This team includes a number of key disciplines: Governance, Risk Management, Compliance Strategy, Business Enabling Team, Security Awareness and Training.

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:

This position is responsible to build, maintain and measure the statewide enterprise cyber security information awareness and training program services for all state employees with the goal of securing the workforce's behaviors and ultimately creating a secure culture. Under the direction of the State Chief Information Security Officer ("CISO") and Section Program Manager, perform complex research and analysis in the area of information security. This position is responsible for developing, disseminating and communicating the annual security training, monthly awareness campaigns and the phishing simulation program for the State of Oregon. Develop and maintain in the creation and management of the section's metrics program that provides an overall measure of the effectiveness of the awareness and training program. Coordinate outreach to division, agency, and enterprise-partner users on security and awareness initiatives. Maintain and support federal and state security compliance regulations, requirements and standards as they pertain to statewide security training; develops long-range plans, goals, objectives and milestones; determines and implements security awareness policies and training activities. This position also provides consultative advice to division, agency, and enterprise-partners on the administrative, policy, programmatic and management aspects of the security awareness and training program.

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.

% of Time	N/R/NC	E/NE	DUTIES

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

50%	NC	E	<u>Program Management, Analysis and Organization</u>
			• Statewide Information Security Awareness and Training Program management
			• Statewide Phishing Simulation Program management
			  ○ Develop stakeholder communications templates and roadmaps
			  ○ Coordination of stakeholders
			• Design and execution of training and awareness curriculum
			• Assist with Security & Disaster Recovery (DR)Tabletop exercises
			• Creation of instructional and explanatory materials (e.g. presentations, processes, standards) to provide guidance to stakeholders and workforce
			• Delivery methods may include on-line sessions, materials for classroom delivery, or written vectors (or a combination as needed).
			• Create policy and process documentation related to information security training, education, and awareness programs as needed.
			• Develop the strategy, goals, and objectives for the Information Security Awareness and Training Program.
			• Develop Information Security Awareness and Training events and activities (e.g. Cybersecurity Awareness Month, in-person presentations, advanced technical training, speaking events, etc.)
			• Consultant to division, agency, and enterprise-partners on training requirements related to regulated data and other protected information, as well as state and agency requirements
			• Develop training courses tailored to audience and environment
			• Evaluate the effectiveness of existing Information Security Awareness and Training Program/activities.
			• Develop and manage Workforce Development Program based on NIST NICE Framework
			• Develop Information Security Awareness and Training Ambassador Program for agencies
			• Work with external vendors and agency partners as needed to establish quotes, production schedules, delivery, and implementation of materials.
			• Collaborate with information security technical experts as needed to augment or further develop information security training, education, and awareness activities appropriate for regulatory requirements.
			• Coordinate Statewide Information Security Awareness & Training Advisory Board

30%	NC	E	<u>Research and Evaluation</u> • Research and analyze adult learning techniques • Develop detailed plans, goals and objectives for long-range implementation and administration of CSS Information Security Awareness and Training initiatives.

			• Develop and Monitor Program metrics by monitoring and tracking the success of the program and operation data. Use data to implement awareness programs for state employees, vendors, and contractors. Create and maintain a metrics framework that can effectively measure and communicate the impact of the program. • Monitor and manage efforts to ensure all state employees comply with mandatory annual security training. Ensure new employees undergo training within first 30 days of employment.
15%	NC	E	Project Management • Develop the yearly strategic plan for the annual enterprise security training and monthly awareness program. • Manage the annual security awareness and training program initiatives as an annual project by planning and developing the annual mandatory statewide information security training for all state employees to complete. Identify project scope for the required training and resources. Recommend annual project budget and spending plan to stakeholders. Create and implement the communication plan for the annual awareness and training program. • Lead cross collaboration workgroups to obtain new vendor contracts for training and awareness material for state agencies to utilize. Follow contracting guidelines to develop contractor statement(s) of work for training materials. Obtain quotes from contractors. Monitor and track project budget, schedule and performance of the Information Security Awareness and Training Program. Coordinate project activities with internal and external units. • Administer security training project contracts; monitor and evaluate contractor performance. Recommend changes to the annual project plan in response to unforeseen changes or unexpected results. Obtain approvals to proposed changes in project scope, quality, budget, or schedule from sponsor. • Validate quality of project deliverables. Create and maintain performance metrics for the enterprise and assist in individual agency metric creation. • Plan, implement and coordinate the enterprise annual October Cyber Security Awareness Month weekly activities and awareness training forum.
5%	NC	NE	Other duties as assigned

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.

Office environment with extensive use of office equipment including personal computers. Duties are performed in a cubicle office design resulting in on-going audible distractions. Requires extended time working at a computer terminal with frequent use of common office technology, including phones, computers, printers, copy machines,

fax machines, etc. Work may include long periods of sitting and standing. Involves working with highly sensitive and/or politically sensitive agency information. Requires high level of professional integrity with regard to agency customer information. Deadlines and department requirements may create stressful situation. This position requires the ability to work on multiple tasks simultaneously and within a short time frame, and interface with customers. Occasional overtime may be required to meet deadlines.

Frequent travel required to agency customers mostly within the local area (Salem). Requires driver's license or alternative means of transportation. May include overnight travel.

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.

- 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
- NIST SP 800-53 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?

They provide general guidance and policy directions, and framework to the incumbent who must interpret and apply them as necessary for each application. Used to determine correct operational procedures necessary for efficient operation of statewide computer systems and work processes and procedures to

ensure a consistent quality of services. Assures compliance with correct rules and procedures in performing daily work assignments.

SECTION 6. WORK CONTACTS

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

Who Contacted	How	Purpose	How Often?

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

DAS CSS	In person, by telephone, electronically	Discuss agency enterprise security plans, projects, training, contracts	Daily
Division staff	In person, by telephone, electronically	Provide information, resolve problems, process daily workload – information technology plans and projects, business planning and analysis, consulting services	Frequently
Agency staff	In person, by telephone, electronically	Provide information, resolve problems, direct visitors, direct calls, schedule meetings and resources – discuss agency enterprise security training plans, projects, contracts, consulting. Discuss agency enterprise security training plans, projects contracts	Frequently
Enterprise-wide staff	In person, in writing, by telephone, electronically	Provide information, direct calls, schedule meetings and resources	Frequently
Vendors	In person, by telephone, electronically	Obtain product information and bid requirements – identify, discuss CSS technology implementation, quality assurance, contract issues	Frequently
General public	In person, by telephone, electronically	Respond to incoming communication and direct callers	Frequently
Government officials	In person, by telephone	Information technology plans and projects, presentations, status updates	On occasion
Attorney General staff	In person, by telephone, electronically	Discuss training contract issues	As required
Department of Justice	In person, by telephone, electronically	Discuss agency enterprise security plans, projects, training, contracts	As required

SECTION 7. POSITION RELATED DECISION MAKING

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

This position makes security policy and procedure decisions. It sets the standards and develops long-range plans, goals, and objectives for cyber security information training. Direct and independent decisions are made on state-wide training, testing, configuration, installation and operation of awareness, training and

tools. Less-than-optimal decisions can affect availability of resources necessary for state agencies to meet their goals in meeting the enterprise training services and metrics.

The decisions of this position are critical to the success of the enterprise Information Security Awareness and Training Program for the state. The work is complicated by the need to deal with subjective concepts such as value judgments to coordinate security awareness activities across state agencies. The work is also complicated by the need to develop data that is currently unavailable such as developing training, surveys, conducting analysis of course testing failure and success rates. The position takes into account and gives weight to uncertainties about the data and other variables that affect long-range program performance. It develops detailed plans, goals and objectives for long-range implementation and administration of statewide awareness & training initiatives.

This position has major significance to the enterprise from a security and awareness perspective, and often serves as the basis for new administrative systems, legislation, regulations or programs by evaluating training requirements to meet security standards; results upon implementation may significantly change major administrative aspects of programs, or substantially affect the quality and quantity of benefits and services provided to customers by ensuring that people, technology and processes are meeting the statewide security standards through information security awareness and training.

Current operational measurements are typically ambiguous and susceptible to widely varying interpretations (constant changes to information privacy and security risk prevention, training regulations and compliance); research is complicated by conflicting operational or service goals and objectives (statewide).

SECTION 8. REVIEW OF WORK

Who reviews the work of the position?

Classification Title	Position Number	How	How Often	Purpose of Review
Note: *If additional rows of the below table are needed, place curser at end of a row (outside table) and hit "Enter".*				
IT Cyber Security Manager 2	1914802	Written / In-Person	As need / Quarterly	Ensure program goals are met. / Performance Eval

SECTION 9. OVERSIGHT FUNCTIONS

THIS SECTION IS FOR SUPERVISORY POSITIONS ONLY

a. How many employees are directly supervised by this position? N/A

How many employees are supervised through a subordinate supervisor? _____

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.

You are responsible to promote and foster 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:

- Employee is required to possess and maintain a valid driver's license issued by the state where the employee actually resides or provide an acceptable alternate mode of transportation
- Desired Attributes for the Enterprise Security & Awareness Training Coordinator position:
    - Excellent skills in communicating effectively with technical and business partners in writing and in oral expression including making presentations.
    - Leading state-wide security awareness & training events, materials
    - Ability to create course content
    - Ability to work collaboratively with technical and business partners.
    - Skilled in establishing and maintaining effective working relationships with superiors, subordinates, peers and other agencies and the public.
    - Employee must remain current with cyber security assessment practices as well as other aspects of the profession by attending training/education sessions.
    - Ability to practice critical thinking skills, including scientific methodology, analyzing technical methodologies, business practices and technical reports.
    - The capability to be completely and comprehensively accountable for performance and results.
    - Experience with Microsoft Word, Excel, Access, and Outlook
    - Strong attention to detail.
    - Experience communicating effectively with people over the telephone, in writing and in person to answer questions and explaining information or decisions
    - Experience delivering training in a classroom setting or work experience that included presenting information to groups.
    - Ability to coordinate diverse activities and ensure completion of projects and assignments.
    - Skill managing multiple and competing priorities with short deadlines including the ability to use sound judgment and critical thinking to interpret, prioritize and follow policy direction.
    - Adept at managing conflict and difficult conversations with colleagues to support a positive workplace culture and promote shared ownership of work.
    - Ability to communicate and market complex messages in a simple, clear and engaging manner within our organization, division, agency, and enterprise-partners.
    - The ability to plan, manage and maintain a complex, enterprise-wide program over the long term.
    - Understand the concepts of behavior, culture and how culture impacts how people behave, learn and interact with others.
    - Extensive experience in cybersecurity or information technology is not required. However, you will be expected to continually work with and learn from our security team and stay current with the latest cybersecurity concepts and risks.
    - SANS Security Awareness Professional (SSAP) credential or any certifications in Organizational Change, Marketing, Instructional Design, Adult Education or Communications will be considered a plus.

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

Operating Area	Biennial Amount ($00000.00)	Fund Type

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

N/A		

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