STATE OF OREGON
POSITION DESCRIPTION

Position Revised Date:
July 26, 2023

Agency: Department of Administrative Services

Facility: Enterprise Information Services

☐ 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:	IT Administrator 1	**b.** Classification	7014Z
c. Effective Date:	01/06/2024	**d.** Position No:	1900001
e. Working Title:	Chief Cybersecurity Technology Director	**f.** Agency No:	10700
g. Section Title:	Cyber Security Services	**h.** Budget Auth No:	672180
i. Employee Name:	Vacant	**j.** Repr. Code:	MESN

k. Work Location (City – County): Salem Marion County

l. Supervisor Name: Ben Gherezgiher

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

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

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 work collaboratively with key local and federal partners, EIS teams to deliver secure solutions to our statutory customers.

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 Chief Cybersecurity Technology Director is a senior leadership role responsible for assisting the State Chief Information Security Officer (CISO) in overseeing and managing the information security technologies and other cybersecurity initiatives of the state government. The Chief Cybersecurity Technology Director supports the state CISO in developing and implementing comprehensive security technology strategies, policies, and procedures to protect sensitive information and critical infrastructure across all state agencies, board and commissions. This position involves actively in the overall operational effectiveness of the division including participating in security governance, incident response, and continuous improvement efforts to enhance the state's overall 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.

% of Time	N/R/NC	E/NE	DUTIES
20%	R	E	• Provide leadership and direction for a diversified staff. Hire, monitor performance, develop, coach, discipline and provide direction to employees. Respond to and resolve employee grievances. Assign and plan work. Promote safety and wellness training and practices in performance of all work activities. Implement Affirmative action and Diversity strategies and goals. Responsible for promoting and fostering a diverse workforce and discrimination/harassment-free workplace. • Administer and maintain a high-performance customer focused organization, conducive to high levels of employee morale and productivity, employee growth and development through relevant training and skills building, diverse representation within the labor force, and equal and fair treatment of all employees, by all employees. Ensure the delivery process of timely employee performance evaluations. • Solves problems and addresses issues as identified by the staff and/or as assigned by State Chief Information Security Officer. • Collaborate with the State CISO in the development and execution of the state's information security strategy and vision. • Assist in the formulation, implementation, and maintenance of security policies, standards, and guidelines. • Collaborate with state executives and agency leaders to develop a comprehensive cybersecurity strategy aligned with the state's business goals. • Develop and manage cyber security services budget.
20%	N	E	• Provide leadership in management of current cyber technologies to ensure services meet expectations of security and risk. • Develop cybersecurity technology roadmap to include multi-cloud and on prem environments and communicate plan to cybersecurity teams and partners. • Working with state CISO establish cyber posture standard for state agencies, boards and commissions to meet.

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

15%	R	E	• Participate in governance meetings and security committees to monitor and evaluate the effectiveness of security measures. • Assist in ensuring compliance with relevant security regulations, laws, and standards across state agencies. • Contribute to security audits and assessments to identify potential risks and vulnerabilities.
15%	R	E	• Aid in the development and maintenance of the state's incident response plan to handle security incidents effectively. • Support incident response teams during security breaches and cyberattacks to mitigate their impact. • Assist in conducting post-incident analysis and recommend improvements to prevent future incidents.
15%	R	E	• Participate in division's operational and capital budget preparation, manage operational budget, review biennial budget requests, and assist State CISO to defend budget expenses. • Assist in evaluating security vendors and technologies to meet the state's security needs. • Participate in vendor contract reviews to ensure adherence to security requirements. • Participate in project activities and decisions to move forward cybersecurity support initiatives.
10%	R	E	• Collaborate with other state executives, government leaders, and security teams to communicate security risks and initiatives. • Lead and implement staff transformation with succession planning across all service verticals of the cybersecurity organization. • Encourage/implement team of teams' operational model across the cybersecurity service verticals. • Represent the State CISO in meetings and events when necessary.
5%	R	N	• 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.

This position involves frequent contact with executives, management, and staff both internal and external to the organization. It requires working with a variety of people and situations, which requires the incumbent to exercise diplomacy. Confidentiality of information must be maintained at all times. This position requires the ability to work on multiple tasks simultaneously, sometimes within short time frames, and interface effectively with business partners. It requires maintenance of tight deadlines and close coordination of a large number of tasks. Often travel to meetings is required with some travel to trainings. There can be frequent interruptions, demanding timeframes, and non-traditional working hours. At times, weekend and evening work is required to meet customer demands and department deadlines. This position requires significant use of a computer and video-conferencing.

Where an employee's duties can be successfully performed away from their central workplace, an employee is eligible for remote work, upon agency approval.

This position is suitable for remote work options.

There may be times that a position or an individual must be located full-time, on-site, within traditional business hours. Times when on-site presence can be required include but are not limited to training, performance, business alignment, accommodations, or resource availability.

To be eligible for remote work, staff must have a home workspace that meets all applicable technology, security and safety requirements including the ability to provide protection of confidential information. Staff are responsible for obtaining an appropriate broadband internet connection for working remotely.

Staff working remote shall:

- Meet all responsibilities and perform all duties as if their role was performed in a traditional work setting.
- Comply with all agency policies, guidelines, and management directives.
- Maintain a professional demeanor in the performance of all duties.
- Meet and maintain performance expectations.
- Be available each week during established work hours, as determined by the business need.

DAS is committed to diversity. Diversity efforts reinforce respectful treatment of others in the workplace. These efforts focus on identifying ways to work better together, reducing conflict by increasing understanding, improving collaboration, fostering teamwork, and increasing productivity and quality of services delivered by DAS. 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.

Working in a team-oriented environment requires participative decision making and cooperative interactions among staff and management. This includes maintaining regular and punctual attendance; performing all duties in a safe manner; and complying with all policies and procedures.

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 Administrative Rules
- Oregon Revised Statutes
- Department of Administrative Services rules, internal division policies and procedures
- Enterprise Information Services Strategy
- IT Standards Document and CIO business plans.
- Federal laws, policies and rules related to interoperability and geospatial data.

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. Position may recommend revisions to the above guidelines, including justification and need for the revision.

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".*			
State Legislators	Written or in person	Provide clarification or statutory reporting	Annual
Local Government Partners	Written or orally	Assist in cyber information sharing or advisories	As needed
Federal Partners	Written or orally	Assist in cyber information sharing or advisories	As needed
Managed Service Providers	Written or orally	Manage performance of managed service provisioning	As needed
Legislative Fiscal Office	Written or orally	Assist in cyber services budget proposals, incident clarifications and to collaborate in technology and cyber services	Quarterly

SECTION 7. POSITION RELATED DECISION MAKING

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

State information asset security, executing of service contracts, interagency agreements, cyber incident activity related decisions. Service denial related to cyber risk etc.

Impact, is related to optimization of cyber services for state agencies and partners.

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".

State Chief Information Security Officer	0485302	In person, virtually, phone, e-mail	Quarterly; Weekly or as needed.	Regular check ins; Review and progress of work
			Quarterly	Performance Evaluations

SECTION 9. OVERSIGHT FUNCTIONS

THIS SECTION IS FOR SUPERVISORY POSITIONS ONLY

a. How many employees are directly supervised by this position? 3

How many employees are supervised through a subordinate supervisor? 36

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. Also, you will be required to pass State Police CJIS Certification. 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 for this position:

- 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.
- Excellent written and oral communication skills.
- The ability to explain complex technical issues to non-technical customers.

- Bachelor's or master's degree in computer science, Cybersecurity, Information Technology, or a related field is desirable.
- Substantial experience (typically 10+ years) in information security and risk management, with prior experience in leadership or supervisory roles.
- Professional certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or Certified Ethical Hacker (CEH) are advantageous.
- Familiarity with information security strategies, policies, and procedures, as well as security frameworks, compliance regulations and budgets.
- Strong understanding of incident response planning and execution.
- Excellent communication and interpersonal skills to collaborate effectively with various stakeholders.
- Proficient in problem-solving and decision-making, especially in high-pressure situations.
- Knowledge and experience with cybersecurity technologies and tools, including firewalls, intrusion detection systems, type of encryption technologies, cloud-based security infrastructure and services.
- Familiarity with security frameworks such as NIST, ISO 27001, and CIS Controls.
- ITIL, LEAN Six Sigma training/certifications are advantageous.
- Ability to work independently and contribute effectively as part of a team.

Behavioral Expectations:

- Establish/maintain effective working relations w/other departments, divisions, contractors,
- Prepare for meetings, bringing issues and solutions for the team to resolve,
- Share in leadership, and actively support decisions made by the management team,
- Participate in cross-functional or problem-solving teams as needed, and
- Adhere to all statewide, DAS and EIS policies, processes, procedures, and safety practices.

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

Operating Area	Biennial Amount ($00000.00)	Fund Type
Cyber Security	$500,000.00	IT Operational Budget

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