**Division of Enterprise Technology**
**Classification Title: Information Technology Manager**
**Functional Title: Deputy Chief Information Security Officer (DCISO), Deputy Director, Bureau of Security**

## Position Summary

The Deputy Chief Information Security Officer (DCISO), Deputy Director for the Bureau of Security, reports to the State CISO and is responsible for the daily operational management of the statewide security program. Serving as a strategic partner and operational counterpart to the CISO, the Deputy CISO executes the State's cybersecurity strategy through direct leadership of the Bureau of Security. This role enables the CISO to focus on statewide strategic planning and executive engagement by overseeing day-to-day security operations and program management.

The Deputy CISO's primary role is to convert the CISO's vision and strategy into actionable plans and to build and operate a platform of automated, self-service enterprise security solutions and services. This includes overseeing security operations, managing incident response, leading compliance and audit activities, and ensuring security controls, NSA and CISA guidance are integrated into all technology projects and systems, both on-premises and in the cloud.

The Deputy CISO is responsible for the direct management of Bureau staff, fostering a culture of excellence, collaboration, and innovation. This role ensures that security policies, standards, and procedures are effectively implemented, monitored, and maintained. The Deputy CISO will manage relationships with agency technical staff, vendors, and operational partners to ensure the seamless delivery of DET services and the robust protection against cyber threats.

Goals and Worker Activities

A. 40% Lead and manage the Bureau's day-to-day operations and staff. Provide direct leadership, management, and operational direction to Bureau and cross-divisional staff.

1. Instrument, measure, and continuously improve the daily operations of the Bureau of Security, ensuring alignment with the CISO's strategic objectives.
2. Manage project and operational teams to develop and execute detailed work plans to ensure the efficient and effective use of staff resources to meet Bureau, Division, and enterprise goals.
3. Establish and track operational metrics and objectives for the Bureau. Analyze resource allocation and performance, reporting progress and recommendations to the CISO.
4. Organize the resources and activities of the Bureau for maximum effectiveness, promoting a lean-agile operational model focused on delivery and continuous improvement.
5. Establish workload priorities, assign tasks, and provide clear instruction and direction to employees, removing impediments and enabling their success.

6. Act as the primary leader for Bureau staff, fostering open communication, counseling, and motivating the team to achieve a high level of performance and engagement.

7. Develop and manage staff performance standards, conduct regular performance evaluations, and create robust training and career development plans to ensure staff competency and growth.

8. Manage personnel actions (hiring, reclassification, etc.) in coordination with the CISO to ensure appropriate and effective allocation of staff resources.

9. Maintain clear and consistent channels of communication with all staff to ensure employees are informed of objectives, activities, and plans, and to encourage their input.

10. Cultivate professional, effective communications with subordinates, peers, and leaders across the enterprise to build and maintain a comprehensive cyber response organization based on trust and cooperation.

B. 25% Execute the enterprise security strategy and manage the security program.

1. Direct the implementation and operational management of the enterprise security program, ensuring the confidentiality, integrity, and availability of state information assets. Ensure all security controls and practices are aligned with and measured against established frameworks like NIST, CIS, and FedRAMP.

2. Execute the security strategy and manage the associated roadmaps and supporting documentation, translating high-level goals into concrete projects and initiatives.

3. Lead Bureau and cross-division teams to engineer and automate the continuous identification, assessment, and mitigation of internal and external threats, vulnerabilities, and risks. Leverage artificial intelligence (AI) and machine learning (ML) to enhance threat detection, incident correlation, and predictive analysis. Ensure robust monitoring, timely detection, containment, and incident response capabilities are in place and consistently tested.

4. Manage and coordinate state and federal compliance audits, report results to leadership, and oversee the development and execution of remediation plans.

5. Oversee regular reviews of access to all systems and direct the risk analysis and rating of all current and future systems and platforms. Reviews may include website approvals, cloud brokerages, license agreements, internation travel security reviews, and deviations from contract security riders.

6. Direct vulnerability assessments, penetration tests, and security reviews. Oversee the investigation of security violations and ensure policy violations are reported to management.

7. Develop, coordinate, and track remediation plans to address security vulnerabilities in a timely manner.

8. Manage and enhance the state's security awareness program to cultivate a security-conscious culture.

9. Direct the development, maintenance, and testing of incident response plans.

10. Analyze, forecast, and optimize the cost and performance of security tools and controls (e.g., logging, data ingestion, and scanning).

C. 20% Oversee the implementation and enforcement of security policies, standards, and project requirements.

1. Manage the development, publication, and review cycle of enterprise-wide information security policies, standards, and procedures.

2. Ensure security requirements and DevSecOps practices are integrated into infrastructure (IaC) and the System Development Life Cycle (SDLC).

3. Work closely with data, systems, network, and application development teams to ensure the integrity of information security procedures and the adoption of shared services and secure configurations.

4. Oversee staff and vendors who safeguard the state's assets, intellectual property, and computer systems, ensuring their activities align with state security policy.

5. Ensure that technologies and associated projects are appropriately monitored for security risks, with risk mitigation requirements being efficiently set, appropriately designed, and delivered.

D. 15% Oversee security incident response and manage tactical intelligence.

1. Direct the Incident Response Team during major security incidents, coordinating all phases of the incident response lifecycle.

2. Proactively monitor and integrate threat intelligence from Federal (CISA, NIST, NSA), State, trusted public/private sector partners, and commercial sources to identify potential threats to state systems.

3. Provide timely and actionable notification of new vulnerabilities and threats to agency security officers and technical staff and track mitigation efforts.

4. Coordinate anomaly and incident reporting to determine if potential threat activity is directed against a single agency or across the enterprise.

5. Manage incident reporting to outside organizations, including law enforcement and government-wide incident response bodies, as directed by the CISO.

6. Interact with the CISO to ensure that operational decisions and resource allocation maintain and enhance the State's information security posture.

Knowledge and Skills

1. Strong oral and written communication skills, with the ability to translate complex technical concepts into clear, actionable information for technical and non-technical audiences.
2. Exceptional interpersonal and leadership skills, with a proven ability to lead, motivate, and develop a diverse team of technical and non-technical professionals.
3. Strong project and program management skills, with experience in agile methodologies or other iterative approach with short feedback loops.
4. Proven ability to plan, organize, and direct complex technical work, with an in-depth understanding of cybersecurity operations and issues.
5. Experience in analyzing and resolving complex enterprise business and technology issues in a large government or corporate organization.
6. Demonstrated ability to establish credibility with staff, peers, and agency partners to garner support for security initiatives.
7. Demonstrated experience as an articulate and persuasive leader who can serve as an effective manager and communicate security-related concepts to a broad range of technical and non-technical staff.
8. Expert knowledge of cybersecurity with extensive experience in security operations, incident response, and risk management.
9. Expert knowledge of computer and network investigation with digital forensics knowledge.
10. Expert knowledge of security frameworks and standards, particularly NIST CSF, RMF, and 800-series publications, as well as CIS controls.
11. Deep knowledge of secure software development, DevSecOps, and cloud security (FedRAMP, GCP, Azure, AWS).
12. Demonstrated experience securing cloud-native services, including container platforms , data streaming, and serverless architectures.
13. Expert knowledge of security-as-code principles and embedding security into CI/CD pipelines and infrastructure-as-code (IaC) frameworks.
14. Extensive, hands-on knowledge of network, system, database, and application security.
15. Strong, practical understanding of modern IT operations, including Site Reliability Engineering (SRE), observability, and FinOps principles.

16. Demonstrated ability to work with management and staff at all levels of the organization to implement and enforce sound security practices.

17. Demonstrated experience leading business continuity planning, disaster recovery, and risk management programs.

18. Strong working knowledge of security principles (authentication, vulnerability management, penetration testing, auditing) and technologies (SIEM, EDR, firewalls, IAM).

19. Strong, practical understanding of AI applications in cybersecurity and the principles of AI Security and Governance to secure enterprise AI/ML systems.

20. Demonstrated ability to execute a documented strategy, manage supporting roadmaps, and work with teams and leadership to communicate progress and challenges.