

DOA Data Manager
Department of Administration, Division of Enterprise Services

POSITION SUMMARY

Working in the Division of Enterprise Technologies (DET), under general direction, this position serves as the Department of Administration's (DOA's) Data Manager. This position is responsible for developing and guiding the overarching strategy and principles of DOA's and supported Customer data management program including being responsible for the collection, storage, and utilization of data within those organizations. The role should ensure that data is accurate, accessible, secure, and facilitate informed decision-making and planning. This will include things like developing data quality standards, performing classifications, assisting in DOA's and supported customer governance and interoperability. The position is also responsible for guiding the short- and long-term planning and continuous improvement efforts related to data management, including ensuring the department's investments in data are leveraged to their fullest potential and data risks are mitigated.

The position works closely with leaders and subject matter experts (e.g., division data stewards) from DOA divisions and supported customers to develop policies and procedures related to the collection, storage and use of data. This position also involves working with staff across DOA to create data literacy and training programs for staff. This position will also work closely with DOA Legal and Privacy areas on policy and governance.

GOALS AND WORKER ACTIVITIES

60% A. Management and strategic direction of the department and supported customer's data governance program.

1. Create a comprehensive data strategy that aligns with organization's goals. Provide information related to cost-effective uses of data and to improve risk management efforts related to data.
2. Develop and implement policies and procedures related to data management activities across the department. This includes consideration of data throughout its lifecycle, including data collection, analysis and usage.
3. Partner with DOA and supported customer data stewards to determine internal processes for divisions/offices to follow related to raising data quality/integrity issues and interoperability.
4. Create a leadership framework to make decisions about data-related programs and initiatives.
5. Review department programs to ensure there is compliance with regulations, data accuracy and security. This includes ensuring that data is accessible, safe and used for business processes effectively.
6. Provide updates to leadership on data management activities. Develop reports and present them to senior leaders, as directed.

7. Collaborate with DOA and supported customer data stewards to create standardized analytics and metrics related to data governance activities, as needed.
8. Act as a lead change agent to promote data management across the department and supported customers.
9. Educate employees across the department and supported customers about data security practices and expectations.
10. Develop training and/or review training completion reports related to privacy of data.
11. Consistently and regularly monitor and analyze information and data systems, to discover ways of enhancing them such as new technologies, upgrades, and integrations emerge.
12. Identify and resolve data-related problems, ensuring the integrity and reliability of data across DOA and supported customers.

20% B. Collaboration and facilitation of data management activities across the agency and our supported customers. This may also include collaborating with other state agencies (as needed).

1. Meet with division/office leaders across the department and supported customers to learn of their data issues and emerging initiatives/programs. This includes reviewing and making recommendations to those individuals to meet their data needs.
2. Analyze information from department and supported customers and make recommendations to leadership on ways to incorporate data management policies and processes into programs.
3. Develop a DOA Data Governance Group, including drafting agendas, presenting information, coordinating meeting attendance, etc.
4. Collaborate with the Bureau of Technical Architecture, Policy Team, and Bureau of Security within DET on policies, standards and procedures.
5. Collaborate with technical experts in the department to coordinate training and communication activities.
6. Partner with the Chief Financial Officer on any budget/procurement related requests, including changes with data infrastructure, security and management.
7. Coordinate Cyber-Security Initiatives and programs into Data management practices in coordination with the Chief Information Security Officer.
8. Coordinate Privacy initiatives and programs into data management practices in coordination with the Division of Legal Services.
9. Coordinate any data related procurement actions with the Division of Enterprise Operations.

15% C. Manage continuous improvement efforts related to data management and data integrity processes.

1. Collaborate with division and supported customer data stewards to develop long-term strategies and plans for using data.
2. Review processes across the department and supported customers using data for business programs and look for process improvement opportunities.
3. Develop internal processes for improving programs related to data management.
4. Investigate potential uses of Artificial Intelligence (AI) and machine learning into data management activities.
5. Provide recommendations for leadership on changes to data management efforts.

5% D. Demonstrate leadership in customer service and participate in special projects as assigned.

1. Facilitate knowledge sharing through documentation, presentations, and collaborative discussions.
2. Stay up to date on emerging data technologies, security trends, and best practices to continuously improve data management practices.
3. Apply the DOA Employee Core Competencies in all actions, interact with other DET staff and business customers in a professional manner, and maintain a positive, courteous, and open working environment following DET's Inspire model.
4. Develop and maintain coordination and problem resolution with other areas, partners, and DET to ensure responsive service to customers.
5. Create a work environment that demonstrates respect for everyone.

KNOWLEDGE, SKILLS AND ABILITIES

1. Significant knowledge of data management programs, functions, principles, practices, governance models, regulations, and standards. This should include things like managing data systems, ensuring data quality and appropriate safeguarding, integration, and data handling.
2. Experience in implementing data related policies, procedures, standards and guidelines.
3. Management skills including the ability to direct and organize program activities for projects.
4. Excellent leadership skills, including the ability to bring customers/users together to address issues.
5. Knowledge of information technology programs and functions.
6. Strong oral and written communications skills.
7. Excellent interpersonal skills including the ability to collaborate, negotiate, and partner with others.
8. Ability to develop programs and processes.
9. Strong skills in policy development.

10. Ability to manage controversial and sensitive information and issues using confidentiality and security practices.
11. Strong skills in strategic planning and management.
12. Ability to manage and guide changes in an organization.
13. Ability to effectively work with diverse teams within an organization.
14. Knowledge of contract administration and vendor management.
15. Knowledge of continuous improvement methods.
16. Strong skills using Microsoft Office tools.
17. Ability to diffuse conflicts and issues with tact and diplomacy.
18. Knowledge of data quality approaches and strategies.
19. Knowledge of data sharing and data security strategies.
20. Knowledge of classification strategies for sensitive and confidential data.
21. Familiarity with data technologies related to reporting, analytics and visualization tools and platforms.
22. Familiarity with modern database and information system technologies as it relates to data storage, usage, and management.
23. Experience in Cyber-Security principles and frameworks.
24. Certified Data Management Professional (CDMP) preferred but not required.