Job Profile: Data Privacy Manager

Job Code: XXXXX

Proposed Pay Grade: 34

Job Classifications: 600

Job Family: XXXX

Job Profile Summary: The Data Privacy Manager will play a crucial role in ensuring compliance with new state laws regarding data privacy within IMS and City departments. Incumbent will oversee the implementation of privacy programs, monitor ongoing dataset examination, coordinate customer notification in the event of data breaches, and manage reporting requirements. Compliance with these laws will be a key performance metric for this role.

Job Description

TYPICAL DUTIES:

- Develop and implement privacy programs to ensure compliance with state laws and regulations.
- Collaborate with IMS and City departments to assess current data processing activities and identify areas of non-compliance.
- Document non-compliant processing activities and develop strategies for bringing them into compliance.
- Oversee ongoing dataset examination to ensure that only the minimum amount of personal data necessary is being processed.
- Coordinate with legal and IT teams to provide notice to individuals affected by data breaches, in accordance with state law requirements.
- Conduct privacy training programs for employees and monitor completion to ensure compliance with training requirements.
- Serve as a liaison between the organization and regulatory agencies on privacy matters.
- Stay up to date on changes in privacy laws and regulations and assess their impact on the organization.
- Prepare and submit annual reports on data sharing and processing activities to the relevant state privacy officer or chief privacy officer.
- Collaborate with contractors to ensure compliance with data privacy requirements in contractual agreements.
- Performs additional duties as assigned.

MINIMUM QUALIFICATIONS:

- Bachelor's degree in Information Technology, Computer Science, Law, Business Administration, or a related field.
- At least 3 years of experience in data privacy management, compliance, or a related field.
- Familiarity with relevant state laws and regulations regarding data privacy, including Utah state code 63A-19-401.
- Strong understanding of privacy principles, including data minimization, notice requirements, and breach notification procedures.
- Experience developing and implementing privacy policies, practices, and procedures.

- Excellent communication and interpersonal skills, with the ability to effectively collaborate with cross-functional teams.
- Demonstrated ability to manage projects, prioritize tasks, and meet deadlines in a fast-paced environment.
- Experience conducting privacy training programs for employees.

PREFERRED QUALIFICATIONS:

- Master's degree in Information Technology, Cybersecurity, Law, or a related field.
- Certified Information Privacy Professional (CIPP) or other relevant certifications.
- Experience working in a governmental or public sector environment.
- Knowledge of data protection technologies and tools.
- Experience conducting privacy impact assessments and risk assessments.
- Familiarity with data governance frameworks and best practices.
- Experience managing data breach response and mitigation efforts.
- Ability to interpret and apply complex legal requirements to practical business situations.
- Strong analytical and problem-solving skills, with attention to detail.

WORKING CONDITIONS:

- Light physical effort. Intermittent sitting, standing, and walking. Comfortable working conditions.
- Considerable exposure to stress resulting from complex problem solving and stringent project deadlines.

The above statements are intended to describe the general nature and level of work being performed by persons assigned to this job. They are not intended to be an exhaustive list of all duties, responsibilities and skills required of personnel so classified. All requirements are subject to possible modification to reasonably accommodate individuals with disabilities.