Municipal Authority of the City of Sunbury
Job Description
General Manager

Job Summary: The General Manager of the Municipal Authority City of Sunbury shall serve as the chief administrator of all Authority functions including Wastewater, MIPP, Water, Solid Waste, Recycling and Flood control. This individual will be appointed by the Board of Directors of the Municipal Authority City of Sunbury.

Education / Qualifications:

1. Bachelor's Degree in Business Administration or Management.
2. Comprehensive knowledge of Federal and State regulations governing Municipal Operations
3. Minimum of five (5) years' experience in Management in the Water and Wastewater field.
4. Minimum of five (5) years' supervisory experience.
5. Computer experience - Must have a working knowledge of Windows and Microsoft Office Programs.
6. Strong financial background.
7. Strong Communication Skills.

Reporting Responsibility: Board of Directors, Municipal Authority of the City of Sunbury.

Job Responsibilities:

1. Administer the financial affairs of the Authority including the handling of all funds, accounting, and reporting procedures.
2. Long range organizational planning.
3. Maintain and preserve accounting and business records as required by any law, government agencies, and Authority policies.
4. Administer the collection of fees.
5. Responsible for all bidding functions of the Authority.
6. Manage Authority benefits and insurances.
7. Maintain an up-to-date inventory of capital purchases.
8. Advise and assist in investments of Authority funds.
9. Coordinate the general operation of all departments, including retained engineer, office, wastewater, MIPP, water, solid waste, recycling and flood control.
10. Prepare the annual financial budget with assistance from department managers.
11. Prepare and submit grant and permit applications with assistance from department managers as necessary.
12. Develop department and personnel policies with input from the department managers. Implement all policies and procedures adopted by the Authority Board of Directors.
13. Administer and monitor an employee-training program.
14. Ensure that staff are informed and updated on Authority policies and procedures.
15. Prepare board reports and present updated information at all Authority board meetings.
16. Prepare all internal financial reports and present this information at board meetings.

17. Immediately inform the Board of Directors of all sensitive issues that may arise related to the Authority.
18. Make recommendations to the Authority Board of Directors on staffing needs and requirements of Authority.
19. Maintain a professional image in the presence of the public.
20. Communicate effectively with public officials and the media during major events of the Authority.
21. Pursue relevant continuing education on an ongoing basis.
22. Maintain employee performance data and complete periodic performance evaluations.
23. Expected to always be available when needed by the Authority.
24. All other duties and responsibilities as assigned by the Authority Board of Directors.

Privacy Official Job Responsibilities

The Privacy Official is responsible for developing and implementing the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in connection with the group health plan sponsored by the Employer, developing employee training programs relating to the privacy of group health plan information, publishing and distributing the Notice of Privacy Practices for the group health plan and serving as the designated decision maker for issues and questions involving interpretation of the privacy rules as they relate to the group health plan in coordination with legal counsel as needed. The Privacy Official will be responsible for the following tasks:

1. Inventorying the uses and disclosures of Protected Health Information by the company.
2. Working with management to determine the individuals and classes of individuals who need access to PHI.
3. Implementing a training program.
4. Ensuring that compliance documents are drafted, implemented, and delivered, as applicable. The documents include amendments to plan documents, changes to business associate contracts, Privacy Policy, and the Notice of Privacy Practices.
5. Developing authorizations, complaint forms, logs and other documents to be used to comply with HIPAA's privacy requirements.
6. Establishing and administering the process for receiving, documenting, tracking, investigating and acting on all complaints concerning the Company's uses and disclosures of Protected Health Information.
7. Developing and implementing procedures for providing plan participants with an accounting, requesting amendments, accessing, and requesting restrictions on uses and disclosures of Protected Health Information.
8. Maintaining documentation in accordance with the record retention provisions of the Privacy Policy.
9. Notifying or overseeing the notification of individuals, the media and the Department of Health and Human Services of any breach of unsecured PHI, in accordance with the provisions of the HITECH Act.
10. Understanding and advising staff about privacy requirements, minimum necessary uses and disclosures and future changes in laws or regulations related to privacy; and
11. Auditing and monitoring the privacy program.

Security Officer Job Description

The Security Officer is responsible for implementing the security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in connection with the group health plan sponsored by the Employer in coordination with legal counsel as needed.

The Security Officer will be responsible for the following tasks:

1. Maintaining current knowledge of applicable federal and state security laws that relate to the company's group health plan.
2. Conducting an initial inventory of the types of electronic Protected Health Information received, maintained or transmitted by the company.
3. Certifying that the Company does not create, receive or maintain any electronic Protected Health Information by conducting a Risk Assessment.
4. Adopting a Security Policy that establishes the Company's position with respect to Protected Health Information and the Company's intent to avoid creating or receiving any Protected Health Information in an electronic format.
5. Notifying vendors, and, if appropriate, employees, that the Company does not intend to create or receive any Protected Health Information in an electronic format.
6. Maintaining documentation in accordance with the record retention provisions of the Security Policy.
7. Understanding and advising staff about security requirements and future changes in laws or regulations related to security; and
8. Auditing and monitoring the security program, making changes as appropriate and notifying the staff of any changes.

Submit an application and resume to Jennifer Kremer.