Draft Cybersecurity Framework and Risk Assessment

Identify the types of critical and sensitive data

Risk management program objectives

	Maintaining necessary access and control to the town's banking/accounting, utility billing, communications infrastructure as well as critical data.
Availability	***Availability of all information should be generally uninterrupted and able to be recovered within 72 hours in the case of server failure.***
Confidentiality	***Ensuring that data of a sensitive nature is protected from unauthorized access at all times.***
Integrity of data	***Verifying that the data is correct and can be recovered if in doubt or corrupted***
Integrity of Processing	***Protecting systems and controls from improper alteration to ensure correct processing and functionality***

How are objectives established, maintained, and approved?

What factors have a significant effect on the entity's inherent cybersecurity risks?

Characteristics of technologies

- ***A. Connection types***
- ***B. Frequency of backups***
- ***C. On-site and off-site backup storage***
- ***D. Firewall protections?***

Organizational and user characteristics

- ***A. User practices?***
- ***B. Password practices?***

Environmental, technological, organizational and other changes during the period

- ***A. Personnel changes?***
- ***B. Departmental changes?***
- ***C. Vendor changes?***
- ***D. New threats identified?***
- ***E. Changes in any of the techological characteristics or organizational/user characteristics listed above?***

Security incidents and response?

What security incidents were identified during the 12-month period immediately prior to the begin date of the period reviewed?

Who, what, when, where, why, how?

What steps were taken to mitigate the threat of their reoccurrence?

Cybersecurity Risk Governance Structure

What is the process for establishing, maintaining and communicating the principles of ethics and integrity as they relate to cybersecurity?

How does the town maintain internal and external oversight of the risk management program?

Cybersecurity Risk Assessment Process

How are current and potential cybersecurity risks identified?

How does the town assess the related risks and mitigate appropriately?

Cybersecurity Communications and Quality of Cybersecurity Information

What is the process for internally communicating relevant cybersecurity information, such as objectives/responsibilities, how to identify something unusual and of potential concern (and related consequences)?

What is the process for externally communicating relevant cybersecurity information, such as objectives/responsibilities, how to identify something unusual and of potential concern (and related consequences)?

Monitoring of the Cybersecurity Risk Management Program

What is the process for conducting ongoing and periodic evaluations of internal controls related to cybersecurity?

What is the process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities and control deficiencies to parties responsible for taking corrective actions?

Cybersecurity Control Activities

How are responses to assessed risks developed, including design and implementation of control processes?
Provide a summary of the entity's IT infrastructure and its network architectural characteristics.

What are the key security policies and processes implemented and operated to address the entity's cybersecurity risks, including:
a. Prevention of intentional and unintentional security events

b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents
c. Management of processing capacity to provide for continued operations during security, operational and
d. Detection, mitigation and recovery from envieronmental events and use of backup procedures to support system
e. Identification of confidential information when received or created, determination of retention period for that information, retention and then destruction after period expires

Prevention of intentional and unintentional security events

How are credentials levels determined and how often are they reviewed?
How is data loss prevented?
What intrusion prevention tools are in place (generally)?
How are security events detected, identified, responded to and mitigated against?

How is processing capacity managed to provide continued operations during security, operational and environmental events?

How are environmental events detected, mitigated against, and recovered from, and how are backup procedures used to support system availability?