Cyber Incident Response Plan and Implementation Checklist

Preparation

❑ 1.1 Determine who are the stakeholders in the municipality that need to be involved with development of the Incident Response Plan
  - Organizational leadership
  - IT & Information Security leadership
  - Audit
  - Finance
  - Human Resources
  - Communications
  - Legal Counsel

❑ 1.2 Determine what decisions need to be made
  - Obtain or clarify cyber liability insurance information and requirements
    - How much coverage, what are the limits, what is the retention
    - What is covered?
      - Social engineering
      - Ransomware
      - Malware
      - System restoration
      - Legal and forensic costs
      - Credit monitoring & call center costs
  - Determine vendors needed and obtain contact information as well as a plan for engagement/procurement:
    - Forensics
    - Outside legal counsel
    - Mitigation services such as credit monitoring and call center services
    - Communications services

❑ 1.3 Establish the Incident Response Team (the “Team”)
  - Define Team Members
  - Define Roles
  - Establish contact list with alternative contact information
  - Determine communications protocols – internal and external

❑ 1.4 Establish Goals for the Incident Response Plan (the “Plan”)
  - Establish definitions – data breach, security incident
  - Establish protocols for level of response – e.g. low-level v. high-level security incidents
  - Establish criteria to assess the incident and threat level

- Define the actions to be taken when an incident occurs, including notification to regulatory authorities
- Coordinate with third party service providers – determine procurement requirements
- Determine documentation efforts – who is responsible for documenting the incident, actions taken, the process for documenting the incident
- Communication with law enforcement
- Mitigation – implement processes to mitigate the effects of the incident
- Prevention -- establish the Incident Response Team (the "Team")
- Establish definitions – data breach, security incident
- Assess the incident and threat level
- Define the actions to be taken when an incident occurs
- Restore --present an orderly course of action for restoring functionality
- Document – collect and document the incident
- Mitigation – implement processes to mitigate the effects of the incident
- Define restoration efforts --present an orderly course of action for restoring functionality
- Prevention – improve processes and procedures to help prevent the security incident from happening again
- Education – train and educate employees to prevent future security incidents
- Review – Determine process for review – including lessons learned, review of policies and procedures, assess technology and determine any proposed changes
- Communicate – specify how information should be communicated, who should communicate and how to communicate with municipal leadership

❑ 1.5 Compile key contact information:
- Forensic vendors
- Credit monitoring/call center/identity theft mitigation services vendors
- Outside legal counsel – engage in three-way agreement with forensic vendor
- Cyber insurance broker and insurance company contact information to report a breach/security incident
- Law enforcement officials, including state and federal officials
- Applicable regulatory body--such as the Office of the Attorney General
- Information sharing entities

Detection & Analysis

❑ 2.1 Review information received from the individual(s) reporting the security incident

❑ 2.2 Work with other departments and information technology staff, as appropriate, to determine the risk of continuing operations (e.g. deciding whether to shut down system, disconnect from network, continue operation, etc.); however, any decision to delay the containment should be discussed with legal counsel based on the liability

❑ 2.3 Coordinate with incident response services of a third-party security firm and outside legal counsel as appropriate

❑ 2.4 Implement processes to prevent alteration to the system(s) until a backup has been completed

- ❑ 2.5 Implement processes to change passwords or other security safeguards on any compromised systems
- ❑ 2.6 Maintain detailed documentation on all actions taken
- ❑ 2.7 Determine risk level – low level v. high level risk
- ❑ 2.8 Coordinate outside counsel
- ❑ 2.9 Coordinate third party vendors
- ❑ 2.10 Provide notification to insurance broker/company
- ❑ 2.11 Coordinate responses to incident
- ❑ 2.12 Communicate with affected employees & individuals
- ❑ 2.13 Determine if it is a reportable data breach – If yes:
    - o Determine notification requirements to regulatory authorities
    - o Determine states impacted
    - o Determine notification to law enforcement
    - o Determine notification requirements to affected individuals
- ❑ 2.14 Coordinate incident response services of third-party vendors

Containment, Eradication & Discovery

- ❑ 4.1 Implement processes to prevent alteration to the system(s) until a backup has been completed
- ❑ 4.2 Implement processes to perform a full backup of the system(s) to forensically sterilize media (i.e. disk imaging) and store the backup in a secure area as an important part of the chain of custody (as applicable)
- ❑ 4.3 Work with other departments and information technology staff, as appropriate, in determining that containment is complete, determining additional measures to eradicate the risk and other measures necessary to confirm the incident has been contained;
- ❑ 4.4 Implement processes to change passwords or implement other security safeguards on any compromised system
- ❑ 4.5 Maintain documentation on all actions taken

Post-Incident Activity

- ❑ 5.1 Assess damage and cost; assess the damage and estimate both the damage cost and the cost of the containment efforts.
- ❑ 5.2 Review response and update policies, procedures, plans and guidelines; plan and take preventative steps so the intrusion will not recur.
- ❑ 5.3 Consider whether a procedure or policy was not followed which may have led to the intrusion.
- ❑ 5.4 Determine whether additional user education is warranted.
- ❑ 5.5 Was the incident response appropriate? How could it be improved?
- ❑ 5.6 Was every appropriate party informed in a timely manner?

- ❑ 5.7 Were the incident response procedures followed appropriately? How can they be improved?
- ❑ 5.8 Are all systems patched, systems locked down, passwords changed, anti-virus updated, and appropriate procedures, guidelines and policies in place, etc.?
- ❑ 5.9 Have changes been made to prevent a new and similar incident?
- ❑ 6.0 Should any security measures be updated?
- ❑ 6.1 What lessons have been learned from this experience?

Maintenance & Going Forward

- ❑ 7.1 Determine who has responsibility for maintaining the Plan
- ❑ 7.2 Make sure the Plan is distributed as appropriate, within the municipality
- ❑ 7.3 Review Plan at least annually
- ❑ 7.4 Conduct tabletop exercises at least annually
- ❑ 7.5 Conduct regular staff, user and employee education and training in privacy and security