Town of Bon Accord
building for tomorrow

Policy 23-527

CYBER SECURITY INCIDENT RESPONSE & DISASTER RECOVERY PLAN (DRP)

SECTION: Administration/Council

DEPARTMENT: Administration / Public Works / Finance / Community Services

COUNCIL APPROVAL DATE: December 5, 2023

LAST REVIEWED BY COUNCIL: December 5, 2023

INTRODUCTION

Cyber security is the responsibility of all Town of Bon Accord Council members and Employees regardless of position or title. This policy outlines the responsibility and steps required to report a Cyber Security Incident and limit its potential to denigrate the data integrity, network operability, and reputation of the Town.

PURPOSE

The policy will be used as a guideline to handle Cyber Security Incidents and outline the Disaster Recovery Plan (DRP), ensuring the Town's business processes are maintained, repaired, and/or restored in a timely manner.

SCOPE

The policy governs all End Users, including Town Employees, Council members, as well as all IT assets or network devices owned by the Town.

DEFINITIONS

"BIA" means Business Impact Analysis.

"Council" means the elected officials of the Town of Bon Accord.

"Disaster Recovery Plan (DRP)" means a plan to recover from a specific type of IT disruption or incident. Includes step by step recovery process specific to the applicable network and incident scenario.

“Cyber Security Incident” mean the occurrence or development of an unwanted or unexpected situation which indicates:

- A possible or actual release of information to unauthorized or inappropriate parties,
- A possible or actual breach of Security Controls, and
- A failure of Security Controls which has a significant probability of compromising business operations.

“Employee” means any individual employed by the Town of Bon Accord, including volunteers and third parties.

“End User” means any individual who uses Town hardware, software, or any other technology used to maintain Town operations.

“Security Controls" means safeguards or measures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

“Town” means the Town of Bon Accord.

I. KEY ROLES AND RESPONSIBILITIES

1. **Employees and Council:** All Town Employees and Council members are required to be aware of and take annual training for potential Cyber Security Incidents, and to follow the procedures outlined below if they are suspicious that an incident has taken place.

2. **Senior Leadership Team (SLT):** The Town Manager or designate is responsible for prioritization of actions based on advice from the Incident Manager, as well as public communication, Employee coordination, breach disclosure, and ensuring

that training records are maintained.

3. **Incident Manager:** The Legislative Services and Communications Coordinator is responsible for investigating, reporting on, and leading/coordinating the overall response to the incident.

4. **Third Party Support Provider:** Trinus Technologies Inc. has been designated as the Town's managed services provider. As such, they may work with the Incident Manager to investigate and resolve the incident.

II. GUIDING PRINCIPLES

When managing a Cyber Security Incident, it is crucial to balance the incident from three (3) perspectives, all of which may have different priorities and preferred courses of action.

1. **Forensic Trail:** For compliance and root cause correction it is important to maintain as much raw forensic data pertaining to the nature of the Cyber Security Incident as possible. This includes but is not limited to devices logs and backups of breached configurations.

2. **Mitigation of Threat/Risk**: Understanding and closing the vector of attack and during a Cyber Security Incident is required to ensure that restored services are not compromised in the future. The timing of this mitigation is critical to ensure the least amount of damage or lost data in the event of a breach.

3. **Restoration of Services:** When faced with a disruptive Cyber Security Incident it is likely that the main focus will be on restoring impacted services. Service disruptions will likely result in lost revenue to the Town, however, services should not be restored until the threat has been mitigated enough to ensure that restored services cannot be reinfected.

III. ANNUAL TRAINING STANDARDS

1. Training and practice exercises are mandatory for all Town Employees and Council members.
2. The SLT should implement a practice test of each plan (Schedules "A", “B” and “C”) on an annual basis. During practice, issues that cause the plan to fail can be discovered and corrected.
3. Following the annual practice, plans should be reviewed and updated to assess whether:

    a. The processes/steps are still valid,
    b. Key positions and role delegations are still appropriately assigned, and
    c. Further training is required.

SCHEDULE "A"

DISASTER RECOVERY PLAN (DRP)

1. A Cyber Security Incident may be identified by one (1) of three (3) potential sources:

    a. Disruption to access reported by an End User,
    b. Discovered initially by the Incident Manager, or
    c. Observed by the Third Party Support Provider via a monitoring tool or agent.

2. Once a Cyber Security Incident is discovered, the Incident Manager will perform the following actions to correct or mitigate the disaster. *Note that in some cases the Incident Manager may delegate some or all of these steps and responsibilities to the Third Party Support Provider.*

3. Major incidents should be classified into one (1) of two (2) types:

    a. Disruption of Infrastructure or
    b. Loss of Location.

3.1. **DISRUPTION OF INFRASTRUCTURE**

In the case where system backups are present, only minimal effort (1 hour or less) should be made to restore the network or infrastructure in its current state.

When fast repair of infrastructure is not possible the Third Party Support Provider will immediately restore the most recent required backup to the best available infrastructure and then verify functionality.

a. In the case of damaged or faulty hardware, some infrastructure may require replacement with new, spare, or temporary equipment to fulfill a

recovery.

b. Note that running on contingent, spare, or temporary equipment may result in below average performance for all End Users until the original services can be restored.

3.2. LOSS OF LOCATION

In the event of a loss of location incident (fire, flood, etc.), the Incident Manager will immediately assess the accessibility of BIA-listed resources, as some of them may be cloud based. All services that are not cloud based must be restored in order according to the **BIA Procedure**.

a. Where possible services should be restored using off-site or cloud backups. Local hardware (such as servers) may not be available so an extended period of cloud hosting may be required for these services until new equipment can be purchased and set up.
b. A loss of location may also mean that Employees are not able to work out of that location, nor will they have access to the regular workstation or workspace. Employees may be encouraged to work from an Emergency Command Centre (ECC) or from home using temporary laptops or computers.

SCHEDULE "B"

END USER PROCEDURE

Identifying compromised systems and quickly resolving or restoring functionality is essential to maintain Town business operations. Cyber Security Incidents such as ransomware can propagate rapidly through a network, so acting quickly can help limit the number of affected devices, thus reducing damage and recovery time.

1. A Cyber Security Incident can be stressful, and it is essential to proceed calmly and methodically to ensure that the situation does not escalate.

2. If you suspect that a device has been compromised by a malicious actor or infected with malware (including ransomware), immediately disconnect the device from *both wired and wireless network connections while keeping the power on*. Once disconnected, take a photo or video of any suspicious activity on the device while making detailed notes about the suspicious behavior (**End User Notes**), including

    a. When it started,
    b. How it started, and
    c. What you were doing on the device when it started.

    Share this information with the Incident Manager as soon as possible once the device has been removed from the network.

3. Do not turn off the device unless you must, as this can damage forensic evidence.

4. In the case of ransomware, typically, a message will appear on the screen of the device demanding payment to unencrypt the data on the computer. Be sure to capture a photo of this message to share with the Incident Manager.

5. Promptly communicate to the Incident Manager with a preliminary scope about what is happening, do not try to resolve the situation yourself.

6. Remove all storage devices such as USB drives, external hard drives or memory cards and immediately label these devices “suspect”. These devices should be given to the Incident Manager at the earliest possible convenience.

7. Stop using the device for all work. If you are working on time sensitive tasks, inform the Incident Manager and ask to be given a temporary device. Note that in the event of a large-scale Cyber Security Incident, replacement devices may not be available, and your work (as well as the work of others) may be impacted for a significant amount of time.

SCHEDULE "C"

INCIDENT MANAGER/IT PROCEDURE

The Incident Manager will first assess the situation to determine the nature, breadth, and severity of the incident. If required, the Incident Manager may pass some or all responsibility for the incident management process to the designated Third Party Support Provider. If the severity of the incident is unclear, assume the worst-case scenario until additional information can be gathered. This process will be done quickly to ensure that time sensitive action can be taken as required.

1. Relevant information to complete the **Incident Assessment** includes but is not limited to:

    a. Affected locations,
    b. Employees,
    c. Devices,
    d. Network shares,
    e. Start time of the incident,
    f. Demands and intent of the malicious actor, and
    g. The likely attack vector so that a plan may be created to close any open vulnerabilities.

2. The Incident Manager will create a **Cyber Security Incident Plan** to contain the impact and reach of the incident, such as disconnecting devices that are suspected to be compromised or disconnecting critical devices such as application or backup servers. Where applicable, the Incident Manager will reference previous Cyber Security Incident Plans that may provide guidance on appropriate containment steps for specific types of Cyber Security Incidents.

3. Depending on the severity of the incident, the Incident Manager may determine that engaging third parties such as law enforcement or a cyber security specialist

firm is required. This involvement will be discussed with the SLT prior to engagement.

4. The Incident Manager will engage with the appropriate Employees (including the SLT) and third parties to enact the containment plan as quickly as possible. During this process, effort will be made to isolate devices from the rest of the network and from the internet without deleting evidence of the incident that may be used during a root cause analysis. All containment steps will be carefully documented for future reporting purposes.

5. Severe incidents may require immediate drastic measures such as completely disconnecting all servers from the primary network, completely disabling the Wi-Fi network or completely disconnecting the Town's network from the internet.

6. If the root cause of the incident is clear at this time and is still vulnerable, prompt effort will be made to address this vulnerability as quickly as possible before network functionality is restored.

7. With the incident contained and the active threat to the network mitigated, the Incident Manager will work with the SLT to restore all lost network functionality. Functionality will be restored based on importance to the organization as outlined in the **BIA Procedure**, with high priority items being restored first. This plan will include the restoration of services without the use of any compromised devices. All remediation steps will be carefully documented for future reporting purposes.

8. Restoration of services may involve the use of server or workstation backups to recover the network. In this scenario backups of identified infected machines will be restored in an isolated environment so that they can be confirmed to be clean before they are connected to the production network. If a restoration of backups would destroy the now isolated compromised environment, reasonable efforts will be made to create an isolated backup copy of the compromised environment

before restoration. This backup will be used to determine the root cause of the incident during the reporting phase. If a complete backup is not possible, a backup of relevant system logs may be sufficient.

9. Once network functionality is restored, the Incident Manager will focus on analyzing the incident and determining the root cause. During this phase the Incident Manager will create a **Cyber Security Incident Report** that outlines

    a. the timeline of events,
    b. nature of the incident,
    c. the containment/remediation steps taken,
    d. the likelihood of externally compromised data, and
    e. the lessons learned and recommendations for future improvement.

10. The Incident Manager will determine if the incident has resulted in a beach of sensitive or personal data. If a breach of this data may have occurred, the Incident Manager will contact the Alberta Office of the Information and Privacy Commissioner to report the breach. If personal information was compromised, the Incident Manager will work with the SLT to craft and deliver breach notifications to the impacted parties.

11. Examples of scenarios that require reporting include but are not limited to:

    a. Loss or theft of unencrypted devices containing personal information or remote network access,
    b. Malicious remote access with a user account that has access to personal data,
    c. Suspected exfiltration of personal data via a malicious actor or software, and
    d. Accidental disclosure of personal information (misaddressed email etc.).

12. Once the full analysis of the incident has been completed, any lessons learned or

points for future improvement may be considered in the Town's future budget for planning and implementation.

END USER NOTES

(Completed by the End User)

Be sure to follow the End User Procedure as noted in the above policy. It is the End User's responsibility to share the following information with the Incident Manager as soon as possible once the device has been removed from the network.

Briefly describe the incident:

_____

_____

_____

Date and time you first noticed the incident occurring:

_____

How did the incident begin? (Upon startup, something was clicked or opened, etc.)

_____

_____

What were you doing on the device when the activity began?

_____

_____

_____

Was there an external storage device (USB, hard drive) plugged into the device when the incident occurred? _____

If yes, remove the external storage device immediately label as "suspect". Additionally, please provide the following:

Time and date when the storage device was plugged in:

_____

When and where the device was obtained:

_____

INCIDENT ASSESSMENT

(Completed by the Incident Manager)

Be sure to follow the Incident Manager/IT Procedure as noted in the above policy. It is the Incident Manager's responsibility to first assess the situation to determine the nature, breadth, and severity of the incident as outlined below. This information may be passed to the designated Third Party Support Provider.

Affected location(s):

_____

_____

Employees involved:

_____

_____

Devices affected:

_____

_____

Network(s) affected:

_____

_____

Start date and time of incident:

_____

Demands and intent of malicious actor:

_____

_____

_____

What is the area of vulnerability/likely attack vector?

_____

_____

_____

CYBER SECURITY INCIDENT PLAN

(Completed by the Incident Manager)

Be sure to follow the Incident Manager/IT Procedure as noted in the above policy. It is the Incident Manager's responsibility to create a plan to contain the impact and reach of the incident. Previously used Cyber Security Incident plans may be used for guidance on appropriate steps for specific types of Cyber Security Incidents.

Recommended actions to mitigate further risk (i.e.: disconnecting compromised devices or backup servers from the network, etc.)

_____

_____

_____

_____

What areas of Town business will be affected by these recommended actions?

_____

_____

_____

_____

Recommended timeline to reinstitute resources or processes in accordance with the Business Impact Analysis (BIA) Procedure:

_____

_____

_____

_____

_____

_____

Does the severity of this incident require engagement of third parties (i.e.: law enforcement, cyber security specialist firm, etc.)?

_____

CYBER SECURITY INCIDENT REPORT

(Completed by the Incident Manager)

Once network functionality is restored, the Incident Manager will focus on analyzing the incident and determining the root cause. Examples of scenarios that require reporting include but are not limited to:

- Loss or theft of unencrypted devices containing personal information or remote network access,
- Malicious remote access with a user account that has access to personal data,
- Suspected exfiltration of personal data via a malicious actor or software, and
- Accidental disclosure of personal information (i.e.: misaddressed email etc.).

Outline the timeline of events for the incident:

_____

_____

_____

_____

Describe the nature of the incident (i.e.: malware, ransomware, password leak, etc.):

_____

_____

What steps were taken for containment/remediation?

_____

_____

_____

_____

Is it likely that this incident has compromised externally stored data? Why or why not?

_____

_____

What is thought to be the root cause of the incident?

Was sensitive or personal data compromised during the incident?

If yes, has the SLT been advised? What next steps will be taken to deliver breach notifications to affected parties?

If yes, was the OIPC contacted? Why or why not?

Lessons learned/recommendations for future improvement. List any costs for recommendations for consideration in upcoming annual budget deliberations, pending SLT approval: