Technical Incident Response Report

Date	
Prepared By	
Contributor(s)	
Department	
Incident Name	
Incident Number	

Alberta Government

Table of Contents

Purpose 3
Incident Summary 3
Information Exposure 3
Investigative Findings 3
Containment 4
Preservation of evidence 4
Eradication 4
Recovery 4
Lessons learned 5
Appendix 5

Purpose

This report outlines key sections of deliverables associated with technical documentation and tracking of an incident during all phases of incident response, including detection, containment, eradication, recovery and lessons learned.

Incident Summary

- How the incident was detected, including timeline.
- What is the source of the attack, critical attack path and potential motivation?
- What is the method/tactic of the attack (malware, malicious document, and other adversary tactics or agents)?
- Determining the potential business impact of the cyber security incident

Information Exposure

- What information was breached/accessed/stolen and impact with respect to operations, teaching or research?

Investigative Findings

Incident Timeline

Key events in timeline leading to the detection of the compromise

Date & Time (MDT)	Detection Source & Description
	MDE:
	MDE:

Incident Analysis

Malware and miscellaneous files connected to the compromise

Name	Location/File Path	Hash	Size	User	Malicious IP	Vulnerability Exploited

Extent of the compromise

List of assets (compromised, suspected to be compromised, clean). This includes devices such as servers, workstations and laptops, user accounts, services, applications, etc.

Server	IP address	Purpose	User Account	Process	Comments

Containment

Describe the steps take to contain the incident. The objective of containment is not always to return (directly) to business as usual, but to make best efforts to return to functionality as normal, while continuing to analyse the incident and plan longer term remediation

The goal of containment is to limit damage from the security incident and prevent any further damage

Preservation of evidence

- Engagement of Threat Intel
- Forensic image of disk
- A detailed written log of every action during the investigation
- Documentation of the environment (network topology, system architecture, etc. …)

Eradication

Eradication is intended to remove malware or other artifacts introduced by the attacks, and fully restore the affected system.

- Do you know the point of entry?
- How do fix the problem and verify the threat has been eradicated?
- What additional hardening, patching, and/or configuration steps need to be taken?
- Is there any patching that needs to be done to ensure other systems on the network aren't affected or do configuration changes need to be made to applications/software to prevent infection/spread
- Are you able to monitor the system for evidence of a future compromise?

-

Recovery

- The goal of recovery is to bring all systems back to full operation, after verifying they are clean and the threat is removed.

Lessons learned

-

Appendix

Version History

Date	Name	Version Number	Comments