THE MEDICAL SOCIETY OF PRINCE EDWARD ISLAND (MSPEI)

INCIDENT RESPONSE PLAN

Prepared by and for

CYBERSECURE CANADA Certification

TABLE OF CONTENTS

REVISION HISTORY

The Incident Response Plan has been modified as follows:

Date	Version	Modification	Modifier

TESTING & REVIEW CYCLE

Annual esting of the Incident Response Plan is necessary to ensure the CSIRT (Cyber Security Incident Response Team) is aware of its obligations. Unless real incidents occur, which test the full functionality of the process, this can be achieved using walkthroughs and practical simulations of potential incidents.

1. The Incident Response Plan will be tested at least once annually.
2. The Incident Response Plan Testing will test your business response to potential incidents, identifying process gaps and improvement areas.
3. The CSIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and aspects that need improvement.
4. The Incident Handler will ensure the Security Incident Response Plan is updated and distributed to CSIRT members.

PURPOSE & SCOPE

PURPOSE

This Incident Response Plan exists to ensure The Medical Society of Prince Edward Island (MSPEI) is prepared to manage cyber incidents in an effective and efficient manner. Cyber security incidents are more frequent and sophisticated than ever. No organization globally is immune to attack. Organizations must ensure they are prepared to detect, prevent, and respond to incidents. By having a plan, a team, and conducting exercises, we will be better prepared to respond inevitable incidents. In addition, we will be able to contain the damage and mitigate further risk to the organization. Resources must be deployed in an organized fashion with exercised skills and communication strategies.

This document describes the overall plan for responding to Cyber Security Incidents at The Medical Society of Prince Edward Island (MSPEI). It identifies the structure, roles and responsibilities, types of common incidents, and the approach to preparing, identifying, containing, eradicating, recovering, and conducting lessons learned in order to minimize the impact of cyber security incidents.

The goal of the Incident Response Plan is to ensure The Medical Society of Prince Edward Island (MSPEI) is organized to respond to cyber security incidents effectively and efficiently.

SCOPE

This Incident Response Plan applies to our networks, systems, and data, and stakeholders (for example, employees, contractors, 3rd party vendors) that access them. Members of the organization who are part of the Cyber Security Incident Response Team (CSIRT) are expected to lead or participate in a cyber incidence response. CSIRT members must familiarize themselves with this plan and be prepared to collaborate, with the goal of minimizing adverse effects on the organization.

This document establishes incident handling and incident response capabilities and determines the appropriate response for common cyber security incidents. This document is not intended to provide a detailed list of all activities that should be performed in combatting cyber security incidents.

AUTHORITY

Responsibility for the security of company and customer information resides with the Kris Saunders . During times when a high or critical cyber security incident is underway, this responsibility is entrusted to the General manager.

DEFINITIONS

Acceptable interruption window	in business continuity planning, is the amount of time in which basic functionality must be restored for critical systems. It is a major factor when planning a disaster recovery solution.
Confidentiality	is a classification of data that typically refers to personally identifiable information. It may include such things as social insurance numbers, drivers licence numbers, etc.
Cyber Security Event	is an observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, or a user sending email.
Cyber Security Incident	is any incident that occurs by accident or deliberately that impacts communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services within The Medical Society of Prince Edward Island (MSPEI). This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by The Medical Society of Prince Edward Island (MSPEI).
Denial of Service (attack)	also known as a DoS attack, seeks to make a remote service unavailable to its intended users by flooding its host with superfluous requests, thereby overloading the system.
Exploit	in cyber security terms is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.
Indicators	also known as “Indicators of Compromise” or IOCs, are forensic clues or symptoms left behind by cybersecurity attacks or breaches in the company’s network or systems. These clues are sometimes found in log entries, files, or databases.
Integrity	refers to the maintenance or assurance of data accuracy, consistency, and its accessibility to authorized users for its entire life-cycle.
Maximum tolerable downtime	in business continuity planning, this specifies the maximum period of time that a given business process can be inoperative before the organization’s survival is at risk.
Response playbook	introduces prescriptive cyber security measures and best practices that can be implemented to improve the organization’s security profile. This playbook provides a set

	of standards to reference the organization, improves current systems and implement new ones.
Service availability	describes the state of a system being available and responsive to prospective users. The term is sometimes used to reference a measure of reliability of a system or network resource based on how often it is available as a % of time. For example, 99.97% service availability means that a system is available 99.97% of the time.
SLA	stands for service level agreement and is used to describe a guaranteed measure of service availability. If service availability drops below the prescribed SLA, there are usually financial repercussions, like a money-back guarantee.
Stakeholder relationship map	is a diagram that describes the relationship between individuals in an organization. With respect to cyber security, these diagrams are used to perform IT risk assessments to better inform preventative and reactive measures.
Vulnerability	is a piece of code or bug within a system that causes unintended or unanticipated behavior. A vulnerability implies that this behaviour can be taken advantage of for malicious reasons.
War room	is a dedicated meeting room where major incidents are handled together. It must have a door for privacy, must be available at all times, and must have good communications infrastructure (network, phone, etc.)
Zero-day	is a type of vulnerability that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has at least the potential to be exploited, if it has not already been exploited by cybercriminals.

How To Recognize A Cyber Incident

HOW TO RECOGNIZE A CYBER INCIDENT

A cyber security incident may not be recognized straightaway; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within your environment, or that of your third-party service providers.
Look out for any indication that a security incident has occurred or may be in progress. Some of these are outlined below:

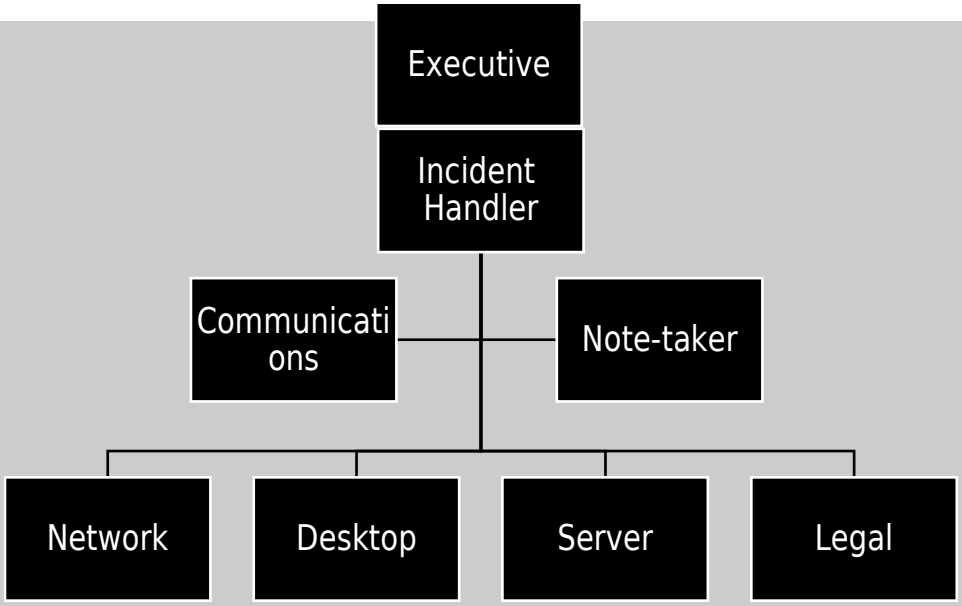
1. Excessive or unusual log-in and system activity, in particular from any inactive user IDs (user accounts)
2. Excessive or unusual remote access activity into your business. This could relate to staff or third-party providers
3. The occurrence of any new wireless (Wi-Fi) networks visible or accessible from your environment
4. The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executable files and programs. This could be on your networks or systems, including web-facing systems
5. Hardware or software key-loggers found connected to or installed on systems
6. Suspicious or unusual activity on, or behaviour of web-facing systems, such on as e-commerce websites
7. Point-of-Sale (POS) payment devices, payment terminals, chip & PIN/signature devices, or dip/swipe card readers showing signs of tampering
8. Any card-skimming devices found in your business
9. Lost, stolen, or misplaced merchant copy receipts or any other records that display a full payment card number or card security code (the three- or four-digit number printed on the card)
10. Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain payment card data or other sensitive data

Cyber Security Incident Response Team (CSIRT)

CYBER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

CSIRT STRUCTURE

Common structure of a Cyber Security Incident Response Team (CSIRT).



CSIRT ROLES

CSIRT ROLES

CSIRT Role	Role Definition
Executive	Accountable Executive for protecting cyber security within the organization. Responsible for reporting to board directors and other executives. Within the CSIRT, this role is responsible for all issues requiring executive decision.
Incident Handler	The Incident Handler is the main triage role of the CSIRT. This role organizes the team and initiates the Incident Response Plan to investigate and respond to cyber security incidents.
Communications	The Communications Expert is responsible for both public relations and internal communications. They are the messenger to ensure that internal/external stakeholders, customers, and the public are informed in a timely and compliant fashion.

Note-taker	The note-taker records the progress of the CSIRT, including anything from meeting minutes, to post-mortem reports.
Network	The Network Engineer provides technical expertise to the response.
Desktop Technician	The Desktop Support Specialist provides technical expertise to the response.
Server Technical	The Server Support Specialist provides technical expertise to the response.
Legal Technician	Legal Counsel providing legal expertise to the CSIRT.

CSIRT RESPONSIBILITIES

The responsibilities described below are organized by role within The Medical Society of Prince Edward Island (MSPEI).

EXECUTIVES

The Executives are/is responsible for:

1. Meeting with the board of directors to best understand what is needed from a security point of view based of the organization's business needs.

2. Regularly reporting any incidents and necessary cyber security actions to the board of directors and other executives.

3. Making decisions on the best way forward based on information provided by the CSIRT team.

4. Making sure that the roles within the CSIRT team are filled and the necessary tools/training are provided for employees to do their jobs.

5. Meeting with key roles within the CSIRT team to better understand what improvements can be made.

INCIDENT HANDLER

The Incident Handler is responsible for:

1. Making sure that the Incident Response Plan and associated response and escalation procedures are defined and documented. Ensure the handling of security incidents is timely and effective.

2. Making sure that the Incident Response Plan is up-to-date, reviewed and tested, at least

once each year.

3. Making sure that staff with Incident Response Plan responsibilities are properly trained, at least once each year.

4. Leading the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan, as and when needed.

5. Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc. as required.

6. Authorising on-site investigations by appropriate law enforcement or payment card industry security/forensic personnel, as required. This includes authorising access to/removal of evidence from the site.

COMMUNICATIONS EXPERT

The communications expert is responsible for:

1. Writing and sending internal and external communications about any incident that occurred.

2. Reporting any cyber incidents to the authorities if needed.

3. Interfacing with executives and other board members to provide information.

4. Interfacing with customers to provide regular updates about any incidents that may affect their experience.

5. Collecting customer responses for impact of incidents, how they were handled and any t ips/suggestions.

6. Collecting lessons learned from members of the CSIRT team and updating management.

CSIRT TEAM

Cyber Security Incident Response Team (CSIRT) members are responsible for:

1. Making sure that all staff understand how to identify and report a suspected or actual security incident.

2. Advising the Incident Handler of an incident when they receive a security incident report from staff.

3. Investigating each reported incident.

4. Taking action to limit the exposure of sensitive information or payment card data and to reduce the risks that may be associated with any incident.

5. Gathering, reviewing and analysing logs and related information from various central and local safeguards, security measures and controls.

6. Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.

7. Reporting each security incident and findings to the appropriate parties. This may include the acquirer, card brands, third party service providers, business partners, customers, etc., as required.

8. Helping law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.

9. Resolving each incident to the satisfaction of all parties involved, including external parties.

10. Initiating follow-up actions to reduce the likelihood of recurrence, as appropriate.

11. Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

1. Making sure they understand how to identify and report a suspected or actual security incident.

2. Reporting a suspected or actual security incident to the Incident Handler (preferable) or to another member of the Cyber Security Incident Response Team (CSIRT).

3. Reporting any security related issues or concerns to line management, or to a member of the CSIRT.

4. Complying with the security policies and procedures of The Medical Society of Prince Edward Island (MSPEI). This includes any updated or temporary measures introduced in response to a security incident (For example, for business continuity, incident recovery or to prevent recurrence of an incident).

CONTACT INFORMATION

CSIRT CONTACTS

CSIRT Role	Name	Title	Phone	Email
*Incident Handler** (lead)*	*Dr Priti Patel !*	*President/Owner !*	*647-555-0001 !*	*jfinlay@jfloral.eg !*
Incident Handler (backup)	*Dylan Smith !*	*General Manager !*	*647-555-0002 !*	*dsmith@floral.e !*
Note-taker	*Lindsay Lau !*	*Assistant Manager !*	*647-555-0003 !*	*dsmith@floral.e !*
Communications	*Dr Priti Patel !*	*President/Owner !*	*647-555-0004 !*	*dsmith@floral.e !*
Network	*Dante Williams !*	*Cybersecurity Vendor Ltd. !*	*647-555-0005 !*	*dsmith@floral.e !*
Desktop	*Dylan Smith !*	*General Manager !*	*647-555-0006 !*	*dsmith@floral.e !*
Server	*Dylan Smith !*	*General Manager !*	*647-555-0007 !*	*dsmith@floral.e !*
Legal	*Yvonne Laurie !*	*Legality Corp. !*	*647-555-0008 !*	*dsmith@floral.e !*
Executive	*Dr Vinod Patel !*	*President/Owner !*	*647-555-0009 !*	*dsmith@floral.e !*
Additional as required				

EXTERNAL CONTACTS

Role	Organization	Name	Title	Phone	Email

OTHER STAKEHOLDER CONTACTS

Role	Organization	Name	Title	Phone	Email

Incident Types

INCIDENT TYPES

Type	Description
Unauthorized Access or Usage	Individual gains physical or logical access to network, system, or data without permission.
Service Interruption or Denial of Service	Attack that prevents access to the service or otherwise impairs normal operation.
Malicious Code	Installation of malicious software (for example, virus, worm, Trojan, or other code).
Ransomware	A specific type of malicious code that infects a computer and displays messages demanding a fee be paid in order for the system to work again.
Distributed Denial of Service (DDoS)	Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable. Symptoms are widespread connectivity failures or system unavailable errors.
Network System Failures (widespread)	An incident affecting the confidentiality, integrity, or availability of networks.
Application System Failures	An incident affecting the confidentiality, integrity, or availability of applications or systems.
Unauthorized Disclosure or Loss of Information	An incident affecting the confidentiality, integrity, or availability of data.
Privacy Breach	An incident that involves real or suspected loss of personal information.
Information Security/Data Breach	An incident that involves real or suspected loss of sensitive information.
Account Data Compromise	A data breach incident specific to payment card data. Such events result in unauthorized access to or exposure of payment card data (cardholder data or sensitive authentication data).
Other	Any other incident that affects networks, systems, or data.

INCIDENT SEVERITY MATRIX

The CSIRT will determine the severity of the incident. They will consider:

1. whether a single system is affected or multiple
2. the criticality of the system(s) affected
3. whether impacting a single person or multiple
4. whether impacting a single team/department, multiple teams/departments, or the entire organization

The Incident Handler must consider the relevant business context and what else is happening with the business at the time to fully understand the impacts and urgency of remedial action.

The CSIRT will consider the available information to determine the known magnitude of impact compared with the estimated size, along with likelihood of the effect spreading and the potential pace of such spread. The CSIRT will determine the potential impacts to the organization, including financial damage, brand and reputational damage, and other types of harm.

The incident may be the result of a sophisticated or unsophisticated threat, an automated or manual attack, or may be nuisance/vandalism.

The CSIRT will determine:

1. whether there is evidence of the vulnerability being exploited
2. whether there is a known patch
3. whether this is a new threat (for example, zero day) or a known threat
4. the estimated effort to contain the problem

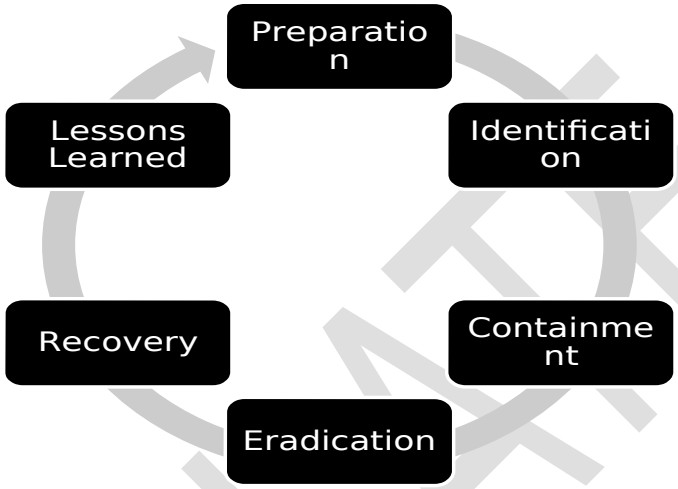
Category	Indicators	Scope	Action
1 – Critical	Data loss, Malware	Widespread and/or with critical servers or data loss, stolen data, or unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
2 – High	Theoretical threat becomes active	Widespread and/or with critical servers or data loss, stolen data, or unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
3 – Medium	Email phishing or active spreading infection	Widespread	Implement CSIRT, Incident Response Plan, create Security Incident, Organization-wide
4 - Low	Malware or phishing	Individual host or person	Notify CSIRT, create Cyber Security Incident

Incident Handling Process

INCIDENT HANDLING PROCESS

INCIDENT HANDLING PROCESS OVERVIEW

In the event of a Cyber Security Incident the Cyber Security Incident Response Team will adhere to the PICERL process as follows.



PREPARATION

In preparation for a data breach incident my organization commits to:

Create and Maintain a Data Breach Plan

- Define who is in charge and how decisions will be made.
- Update the plan every year and note the update date.

Form a Data Breach Response Team

- Put together a team, whether in-house or external, and make sure they are trained for data breaches.
- Clearly define what each team member is responsible for and ensure they are trained.

Understand and Protect Your Systems

- Keep an up-to-date map of where important data is stored and how it moves through your systems.
- Regularly review your security measures to ensure they are strong enough to protect against breaches.

IDENTIFICATION

In the event that a data breach is identified, my organization commits to:

Assemble the Response Team

- Bring together everyone who knows about the breach and involve the Cyber Security Incident Response Team (CSIRT).
- Use a secure meeting space or call to manage the response.

Investigate and Confirm the Breach

- Have the CSIRT confirm if it’s a real data breach or not.
- Find and gather information to prove it’s a breach.

Communicate and Document

- Inform all relevant people while keeping details confidential.
- Document all steps and evidence to maintain a clear record of the breach.

CONTAINMENT

In the event of a data breach my organization commits to:

Implement Response Measures

- Use the incident response plan to guide containment.
- Isolate affected systems and stop malicious activity.

Assess and Repair

- Identify how the breach happened and fix the vulnerabilities.
- Assess the full impact and confirm the breach’s scope.

Document and Preserve Evidence

- Collect and protect evidence, maintaining the chain of custody.
- Keep detailed records of what was found and done during containment.

ERADICATION

In the event of a data breach my organization commits to:

Remove Traces of the Incident

- Identify and fix all exploited weaknesses.
- Remove malware and harmful components from affected systems.

Prevent Recurrence

- Ensure the breach can’t happen again by fixing the identified vulnerabilities.
- Wipe or reformat affected machines before returning them to use, making sure to collect necessary evidence.

Document and Analyze

- Keep detailed logs of the eradication process.
- Analyze how the breach happened and what was exploited to prevent future incidents.

RECOVERY

In the event of a data breach my organization commits to:

Restore Systems

- Restore affected systems one by one.
- Make sure to restore systems from reliable backups to avoid re-infection.

Monitor and Verify

- Keep an eye on systems to ensure the breach doesn't recur and that it's fully resolved.
- Confirm that restored systems are working normally.

Additional Support and Reporting

- Add monitoring to catch any related future activity if needed.
- Contact your cybersecurity insurance provider to file a claim if required. Seek additional help from your Network Security Vendor or Helpdesk if necessary.

LESSONS LEARNED

In the event of a data breach incident my organization commits to:

Review and Report

- Hold a meeting within 2 weeks to discuss lessons learned from the incident.
- Create a follow-up report summarizing findings and recommendations.

Incident Analysis

- Walk through and review the incident report, including how the incident was detected, its scope and severity, and methods used for containment and eradication.
- Identify opportunities for improvement based on the analysis.

Action and Accountability

- Ensure accountability for addressing identified opportunities for improvement.
- Implement changes to enhance incident response and prevention for future incidents.

ESCALATIONS

1. Unauthorized Data Access

- Why: Major security risk.
- Process: Notify CISO and legal team. Start breach response.

2. Critical System Compromise

- Why: Disrupts operations.
- Process: Alert IT and Operations. Engage external experts.

3. Data Exfiltration

- Why: Significant data loss.

- Process: Inform CEO and CCO. Assess impact.

4. Public Disclosure

- Why: Affects reputation.
- Process: Contact PR and legal. Manage public statement.

5. Legal Issues

- Why: Regulatory fines.
- Process: Notify Legal and Compliance. Ensure proper notifications.

STAKEHOLDERS

1. CISO

- Info: Incident details and actions.
- Why: Manages security response.

2. CEO

- Info: Breach summary and impact.
- Why: Oversees company strategy.

3. Legal Counsel

- Info: Legal risks and compliance.
- Why: Handles legal matters.

4. PR Team

- Info: Public messaging.
- Why: Manages company image.

5. Affected Customers

- Info: Breach impact and protection steps.
- Why: Needs to know how to protect themselves.

Sensitive Info to Withhold:

- Vulnerability details: Prevent aiding attackers.
- Personal data: Protect privacy.

INCIDENT SPECIFIC HANDLING PROCESSES

DATA BREACH

If CSIRT investigations confirm that a Data Breach security incident has occurred, please execute the following additional steps:

- Examine the data breach to identify if personal information has been lost due to unauthorized access or unauthorized disclosure.
    - If so, report to Privacy Commissioner of Canada

- Examine the data breach to identify if an Account Data Compromise of credit card information has occurred.
    - If so, contact the Card Acquirer service immediately (see External Contact List section)

RANSOMWARE

If CSIRT investigations confirm that a Ransomware security incident has occurred, please execute to the following additional steps:

- Disconnect devices identified with ransomware from the network immediately
- Examine the ransomware and establish how it infected the device. This will help you to understand how to remove it from the device
- Contact local authorities to report the incident and cooperate with their investigation
- Once the ransomware has been removed, a full system scan must be performed using the most up-to-date anti-virus, anti-malware, and any other security software available, to verify it has been removed from the device
- If the ransomware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by malware
- If data is critical and must be restored, but cannot be retrieved from unaffected backups, search available decryptors from nomoreransom.org
- If there are no backups or decryptors available, contact the Ransomware Decryption Vendor in the External Contact list. Our company policy is to never pay the ransom even if it means permanent data loss
- Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack

---

TAMPERING OF PAYMENT TERMINALS

If CSIRT investigations confirm that tampering of pin pads or payment terminals has occurred, please execute to the following additional steps:

- Stop using the substituted/tampered devices
- Report the substitution/tampering to your device provider and your acquirer
- Follow your device provider or acquirer’s advice to ensure the security of all future card payments. For example, inspect and confirm the integrity of your remaining devices, deploy replacement devices, etc.

Follow your device provider or acquirer’s guidance to investigate the incident. For example, send the substitute/tampered devices to them, allow on-site investigations, etc.
If CSIRT investigations confirm that tampering of pin pads or payment terminals has occurred, please execute the following additional steps:

WIDESPREAD SERVICE INTERRUPTION

If CSIRT investigations confirm that a widespread service interruption security incident has occurred, please execute to the following additional steps:

- Immediately investigate network and access logs to the affected services to identify if there is an active DDoS attack

If confirmed, immediately report to the Network Security Vendor Support Lead or Helpdesk (see External Contact List)

LOSS OF EQUIPMENT

If CSIRT investigations confirm that loss of equipment or theft has occurred, please execute to the following:

- The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to local law enforcement. This includes losses/thefts outside of business hours and at weekends
- If the device that is lost or stolen contained sensitive or payment card data, and the device is not encrypted, CSIRT will complete an analysis of the sensitivity, type and volume of data stolen, including any potentially exposed payment card numbers
- Where possible, CSIRT will use available technology/software to lock down/disable lost or stolen mobile devices (for example., smart phones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed

For additional assistance:

- In the event that CSIRT requires help in identification, contact the Network Security Vendor Support Lead or Helpdesk (see External Contact List). They will provide additional help and expertise

Approvals

APPROVALS

RESPONSIBLE PARTY

Responsibility for the security of company and customer information resides with the following Responsible Party:

Responsible Party Name and Title	Responsible Party Signature	Version	Date
Dr Priti Patel President/Owner		1.0	2021-01-03
Dr Vinod Patel President/Owner		1.0	2021-01-03

The Responsible Party has reviewed the Incident Response Plan and delegates the responsibility for mitigating harm to the organization to the Incident Handler.

During times when a high or critical cyber security incident is underway this responsibility is entrusted to the Incident Handler or their delegate.

INCIDENT HANDLER

The Incident Handler has reviewed the Security Incident Response Plan and acknowledges that, when a high or critical cyber security incident is underway, responsibility for managing the incident is entrusted to the Incident Handler or their delegate.

The Incident Handler or their delegate is expected to handle the incident in a way that mitigates further exposure of the organization. The incident will be handled according to process including identification, containment, eradication, recovery, and lessons learned.

Incident Handler Name and Title	Incident Handler Signature	Version	Date
Priti Patel President/Owner		1.0	2021-01-03

REFERENCES

- National Institute of Standards and Technology (NIST), NIST Special Publication 800-61 Revision 2, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- SysAdmin, Audit, Network & Security (SANS), https://www.sans.org/reading-room/whitepapers/incident
- SysAdmin, Audit, Network & Security (SANS), https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- SANS incident handling forms (SANS), https://www.sans.org/score/incident-forms
- The Office of the Privacy Commissioner of Canada – The Personal Information Protection and Electronic Documents Act (PIPEDA), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronicdocuments-act-pipeda/
- The Office of the Privacy Commissioner of Canada – PIPEDA: What you need to know about mandatory reporting of breaches of security safeguards, https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-yourbusiness/gd_pb_201810/
- Government of Canada – Canada's Anti-Spam Legislation (CASL), https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home
- SANS GIAC Certifications – Incident Handler's Handbook, https://sansorg.egnyte.com/dl/6Btqoa63at/?