Royal Bank of Canada (RBC)

IR Plan, Playbook and Policy

REVISION HISTORY ---- **5**

TESTING & REVIEW CYCLE ---- **6**

PURPOSE & SCOPE ---- **7**

- Purpose ---- 7
- Scope ---- 7

AUTHORITY ---- **8**

DEFINITIONS ---- **9**

HOW TO RECOGNIZE A CYBER INCIDENT ---- **12**

CYBER SECURITY INCIDENT RESPONSE TEAM (CSIRT) ---- **14**

- CSIRT Structure ---- 14

CSIRT ROLES ---- **14**

CSIRT RESPONSIBILITIES ---- **15**

- Executives ---- 15
- Incident Handler ---- 15
- Communications Expert ---- 16
- CSIRT Team ---- 16

CONTACT INFORMATION ---- **17**

- CSIRT Contacts ---- 17
- External Contacts ---- 18
- Other Stakeholder Contacts ---- 18

INCIDENT TYPES ---- **20**

INCIDENT SEVERITY MATRIX ---- **21**

INCIDENT HANDLING PROCESS ---- **23**

- Incident Handling Process Overview ---- 23
- Preparation ---- 24
- Identification ---- 24
- Containment ---- 25
- Eradication & Recovery ---- 26
- Lessons Learned ---- 26

INCIDENT SPECIFIC HANDLING PROCESSES ---- **27**

- Data Breach ---- 27
- Ransomware ---- 27
- Tampering of Payment Terminals ---- 27
- Widespread Service Interruption ---- 27
- Loss of Equipment ---- 28

APPROVALS ---- 29

Responsible Party ---- 29
Incident Handler ---- 29

POLICY ---- 30

POLICY FOR CAPTURING USER INFORMATION ---- 31

Purpose ---- 31
Responsibilities ---- 31
Policy Statement ---- 31
Procedures ---- 31
1. *Authorization: NIST CSF ID.AM-1* ---- *31*
2. *Minimization: NIST SP 800-53 Rev. 5 CM-8* ---- *31*
3. *Encryption: NIST CSF PR.DS-1* ---- *31*
4. *Access Control: NIST CSF PR.AC-1* ---- *31*
5. *Logging: NIST CSF PR.PT-1* ---- *31*

Compliance ---- 31

POLICY FOR ACCESSING AND DISSEMINATING PII ---- 32

Purpose ---- 32
Responsibilities ---- 32
Policy Statement ---- 32
Procedures ---- 32
1. *Access Control: NIST CSF PR.AC-1* ---- *32*
2. *Data Masking* ---- *32*
3. *Encryption* ---- *32*
4. *Monitoring* ---- *32*
5. *Training* ---- *32*

Compliance ---- 32

POLICY FOR COMMUNICATING TLP RED INFORMATION ---- 33

Purpose ---- 33
Responsibilities ---- 33
Policy Statement ---- 33
Procedures ---- 33
1. *Approval* ---- *33*
2. *Secure Channels* ---- *33*
3. *Need-to-Know Basis* ---- *33*
4. *Confidentiality Agreements* ---- *33*
5. *Documentation* ---- *33*

Compliance ---- 33

POLICY FOR DATA RETENTION AND DESTRUCTION ---- 34

Purpose ---- 34
Responsibilities ---- 34
Policy Statement ---- 34

PROCEDURES ---------- 34
1. *Retention Schedule* ---------- *34*
2. *Secure Storage* ---------- *34*
3. *Regular Audits* ---------- *34*
4. *Destruction Methods* ---------- *34*
5. *Documentation* ---------- *34*

COMPLIANCE ---------- 34

POLICY FOR LOG RETENTION AND INCIDENT LOGS ---------- 35

PURPOSE ---------- 35
RESPONSIBILITIES ---------- 35
POLICY STATEMENT ---------- 35
PROCEDURES ---------- 35
1. *Log Retention Period* ---------- *35*
2. *Storage* ---------- *35*
3. *Incident Logs* ---------- *35*
4. *Regular Reviews* ---------- *35*
5. *Destruction* ---------- *35*

COMPLIANCE ---------- 35

REFERENCES ---------- 36

Revision History

The organization is responsible for ensuring that all changes are recorded, making sure that all fields are accurately recorded. The Incident Response Plan has been modified as follows:

Date	Version	Modification	Modifier

Testing & Review Cycle

There will be quarterly testing of the Incident Response Plan. This 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 the end of every quarter.
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 Royal Bank of Canada (RBC) 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 Royal Bank of Canada (RBC). 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 Royal Bank of Canada (RBC) 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 CEO, David I. McKay. During times when a high or critical cyber security incident is underway, this responsibility is entrusted to the CIFO, Adam Evans.

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 Royal Bank of Canada (RBC). This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by Royal Bank of Canada (RBC).
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:

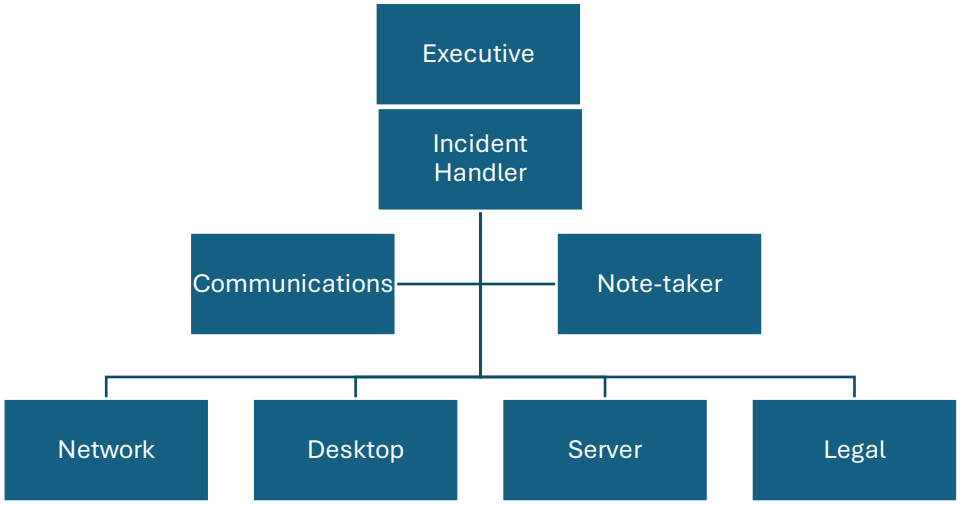
1. Excessive or unusual log-in and system activity, in particular from any inactive user IDs (user accounts)
2. Excessive or unusual remote access activity into your business. This could relate to staff or third-party providers
3. The occurrence of any new wireless (Wi-Fi) networks visible or accessible 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 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 is responsible for documenting all actions, observations, and communications during an incident.

Network Technician	The Network Technician is responsible for managing and securing the organizations network infrastructure during an incident
Desktop Technician	The Desktop Technician is responsible for addressing issues related to end user devices. For example, desktops, laptops, phones, and other endpoints during an incident
Server Technician	The Server Technician is responsible for managing and securing the organizations server infrastructure during an incident.
Legal Technician	The Legal Technician is responsible for providing legal and regulatory support during an incident response.

CSIRT Responsibilities

The responsibilities described below are organized by role within Royal Bank of Canada (RBC).

Executives

The Executives are/is responsible for:

1. Provide a strategic direction and oversight of the CSIRT
2. Making high-level decisions during major incidents
3. Ensuring that there are adequate resources to effectively respond to incidents
4. Ensuring that the organization's incident response practices are legal, regulatory and industry compliant
5. Provide continuous support for improving the incident response process
6. Raising awareness for cybersecurity and ensuring preparedness within the organization

Incident Handler

The Incident Handler is responsible for:

1. Verify and assess the severity and impact of the reported incident
2. Investigate and identify the affected systems, application, and data to determine attack vectors
3. Implement measures to contain the incident
4. Ensure threat has been eliminated and execute plan to restore to normal operations
5. Prepare incident reports and all actions taken

6. Review and identify strengths/weaknesses in the incident response process

Communications Expert

The communications expert is responsible for:

1. Ensure timely and accurate communication among CSIRT members and updates to senior management
2. Serve as the primary point of contact for external communications related to the incident
3. Maintain detailed records of all communications related to the incident
4. Tailor communications strategies to address needs and concerns of different stakeholders
5. Update communication protocols based on past incidents and changing threat landscape
6. Ensure all communications comply with legal and regulatory requirements

CSIRT Team

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

1. Coordinate and oversee incident response activities
2. Communicate effectively with senior management
3. Ensure the incident response is up to date and members are aware of procedures

All staff members are responsible for:

1. Participating in cybersecurity awareness training
2. Providing accurate and detailed information about suspected incidents
3. Ensuring compliance with data protection and privacy regulations
4. Avoiding altering and deleting of any data relevant to incident
5. Ensuring to use strong, unique passwords and following best practices
6. Provide feedback to improve incident response process

Contact Information

CSIRT Contacts

CSIRT Role	Name	Title	Phone	Email
*Incident Handler** (lead)*	*Bruce Ross*	*Group Head, Technology and Operations*	*?*	*?*
Incident Handler (backup)	*Adam Evans*	*Chief Information Security Officer*	*?*	*?*
Note-taker	*?*	*?*	*?*	*?*
Communications	*?*	*?*	*?*	*?*
Network	*?*	*?*	*?*	*?*
Desktop	*Abhishek Baghel*	*Lead System Admin*	*?*	*?*
Server	*?*	*?*	*?*	*?*
Legal	*Maria Douvas*	*Chief Legal And Administration Officer*	*?*	*?*
Executive	*David McKay*	*Chief Executive Officer*	*?*	*?*

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

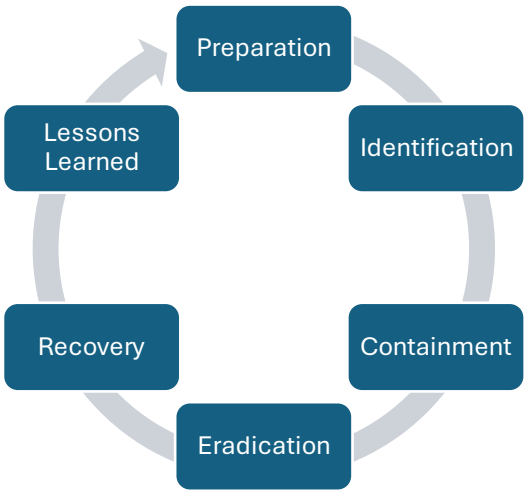
Category	Indicators	Scope	Action
1 – Critical	Data loss, Malware	Widespread and/or with critical servers or data loss, stolen data, or unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
2 – High	Theoretical threat becomes active	Widespread 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

- Policy Development: RBC creates detailed incident response policies tailored to its banking operations, addressing scenarios like data breaches, phishing attacks, and system disruptions.
- Team Formation: RBC establishes a dedicated CSIRT comprising cybersecurity experts, legal advisors, communications specialists, and IT personnel to ensure a comprehensive response to incidents.
- Training and Awareness: RBC conducts regular cybersecurity training for employees, focusing on recognizing phishing attempts, handling sensitive data securely, and following incident response protocols.
- Tools and Resources: RBC invests in advanced security tools such as SIEM (Security Information and Event Management) systems, threat intelligence platforms, and forensic analysis tools to enhance incident detection and response capabilities.
- Incident Response Plan: RBC develops and maintains an updated incident response plan that includes specific procedures for different types of incidents, roles and responsibilities, communication channels, and escalation paths.
- Risk Assessment: RBC regularly conducts risk assessments and vulnerability scans across its network, applications, and infrastructure to identify potential security threats and prioritize mitigation efforts.
- Communication Plan: RBC establishes clear communication channels for internal and external stakeholders, including employees, customers, regulatory bodies, and law enforcement agencies, to ensure timely and accurate reporting and coordination during incidents.
- Drills and Exercises: RBC conducts simulated incident response drills and tabletop exercises to test the effectiveness of its response plan, validate team roles, and identify areas for improvement.

Identification

- Monitoring and Detection: RBC deploys robust monitoring systems, including intrusion detection systems (IDS), endpoint detection and response (EDR) tools, and network traffic analysis tools, to detect and alert on suspicious activities and potential security incidents in real-time.
- Initial Analysis: Upon detection of an incident, RBC's CSIRT quickly performs an initial analysis to assess the nature, scope, and severity of the incident, leveraging threat intelligence feeds and historical data for context.

- Incident Classification: RBC categorizes incidents based on their impact on banking operations, customer data, regulatory compliance, and reputation, using a tiered approach to prioritize response efforts accordingly.
- Notification: RBC follows established notification protocols to promptly notify internal stakeholders, including senior management, legal teams, and IT support, as well as external parties such as regulators and industry partners, about confirmed incidents.
- Documentation: RBC maintains detailed incident logs and documentation, including timestamps, affected systems, forensic evidence, actions taken, and communication records, to support incident investigation, analysis, and reporting.

Containment

- Immediate Actions: RBC's CSIRT implements rapid containment measures, such as isolating compromised systems, blocking malicious traffic, revoking unauthorized access credentials, and implementing firewall rules, to prevent further spread and minimize impact.
- System Backups: RBC ensures the availability and integrity of backup data, regularly testing backup and recovery procedures to facilitate quick restoration of affected systems and services in case of data loss or corruption.
- Long-term Strategy: RBC develops comprehensive containment strategies, including segmented network architecture, access controls, endpoint security measures, and data encryption, to maintain ongoing protection and resilience against evolving threats.
- Communication: RBC maintains transparent and proactive communication with internal stakeholders, customers, and regulators throughout the containment process, providing regular updates on containment progress, impact assessment, and recovery timelines.
- Evidence Preservation: RBC's CSIRT preserves digital evidence following legal and forensic standards, using secure forensic tools and techniques to capture and analyze volatile data, file metadata, network logs, and system artifacts for incident reconstruction and attribution.

Eradication & Recovery

- Root Cause Analysis: RBC conducts thorough root cause analysis (RCA) to identify the underlying factors and vulnerabilities exploited in the incident, collaborating with internal teams, external experts, and industry peers to validate findings and implement corrective actions.
- Clean Up and Patching: RBC removes malicious components, restores system configurations, applies security patches and updates, and strengthens security controls to eliminate vulnerabilities and prevent recurrence of similar incidents.
- Testing and Validation: RBC rigorously tests restored systems and services, conducting functionality tests, vulnerability assessments, penetration testing, and regression testing to ensure that security controls are effective, and operations are restored to normal levels.
- Monitoring and Response Readiness: RBC enhances continuous monitoring capabilities, threat intelligence integration, and incident response readiness, incorporating lessons learned from the incident into ongoing security improvements and resilience strategies.

Lessons Learned

- Post-Incident Review: RBC conducts comprehensive post-incident reviews and debriefings, involving key stakeholders and subject matter experts, to evaluate the effectiveness of the incident response process, identify gaps or shortcomings, and capture lessons learned.
- Improvement Actions: Based on post-incident analysis, RBC implements corrective actions, process enhancements, technology upgrades, and training initiatives to strengthen incident response capabilities, reduce response times, and mitigate future risks.
- Knowledge Sharing: RBC promotes knowledge sharing and collaboration across teams, leveraging incident reports, case studies, best practices, and industry insights to enhance collective understanding of emerging threats, attack trends, and effective response strategies.
- Continuous Improvement: RBC fosters a culture of continuous improvement and adaptive resilience, regularly reviewing and updating incident response plans, procedures, and controls in alignment with evolving regulatory requirements, industry standards, and cybersecurity frameworks.

Incident Specific Handling Processes

Data Breach

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

- Isolate the affected systems to prevent further exfiltration and preservation of evidence
- Notify senior management, legal counsel, and relevant stakeholders such as CEO and CIFO

Ransomware

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

- Isolate and contain attack, followed by identifying the variant, assess capabilities and extent of data exfiltration
- Deploy back systems and restore data to restore critical services, followed by notifying relevant stakeholders

Tampering of Payment Terminals

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

- Isolate affected terminals from network and disable compromised communication channels, document details of tampering
- Determine if sensitive payment data has been exfiltrated, notify relevant stakeholders and senior management

Widespread Service Interruption

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

- Prioritize impacted services based on criticality to the organization's operations and restore as needed
- Notify key stakeholders, and senior management and the impact on the business

Loss of Equipment

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

- Investigate the nature and circumstances of the equipment lost and document details pertaining to the equipment
- Notify the relevant stakeholders and senior management about the incident

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
CEO, David I. McKay	David McKay	1	2024-06-11

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
CIFO, Adam Evans	Adam Evans	1	2021-06-11

POLICY

Policy for Capturing User Information

Purpose

To ensure the secure and compliant capture of user information through packet capture or other network monitoring methods.

Responsibilities

- **Security Officers**: Grant authorization for packet captures.
- **Network Administrators**: Conduct packet captures and ensure compliance with policy.
- **IT Personnel**: Monitor and maintain encryption and access controls.

Policy Statement

Packet captures must be conducted securely, with strict access controls and encryption, to protect user information and comply with regulatory requirements.

Procedures

1. **Authorization:** NIST CSF ID.AM-1
    - Obtain written approval from a designated security officer before initiating packet capture.
    - Document the purpose and scope of the packet capture.
2. **Minimization**: NIST SP 800-53 Rev. 5 CM-8
    - Define the specific data to be captured and ensure it is limited to the minimum necessary for the task.
    - Avoid capturing unnecessary or unrelated data.
3. **Encryption:** NIST CSF PR.DS-1
    - Encrypt all captured data during transmission and storage using approved encryption methods.
    - Regularly review and update encryption protocols.
4. **Access Control:** NIST CSF PR.AC-1
    - Implement role-based access controls (RBAC) to restrict access to captured data.
    - Maintain a list of authorized personnel and update it regularly.
5. **Logging:** NIST CSF PR.PT-1
    - Maintain detailed logs of all packet capture activities, including the purpose, data scope, duration, and personnel involved.
    - Store logs securely and review them regularly for compliance.

Compliance

- Regular audits will be conducted to ensure adherence to this policy.
- Non-compliance will result in disciplinary actions, which may include termination of employment.

Policy for Accessing and Disseminating PII

Purpose

To protect the confidentiality, integrity, and availability of Personally Identifiable Information (PII) accessed or disseminated within RBC.

Responsibilities

- **Data Protection Officers**: Oversee PII protection measures.
- **Employees**: Access PII only as required for their role and in compliance with this policy.
- **IT Security Team**: Implement and monitor encryption and access controls.

Policy Statement

Access to PII must be strictly controlled and disseminated only through secure channels to authorized personnel.

Procedures

1. **Access Control:** NIST CSF PR.AC-1
    - Use role-based access controls to restrict access to PII.
    - Regularly review and update access control lists.
2. **Data Masking**: NIST SP 800-53 PM-18
    - Apply data masking techniques when PII is used in reports or non-production environments.
    - Ensure only masked data is visible to unauthorized personnel.
3. **Encryption**: NIST CSF PR.DS-1 NIST CSF DE.CM-1
    - Encrypt PII at rest and in transit using industry-standard encryption methods.
    - Regularly review and update encryption protocols.
4. **Monitoring**: NIST CSF DE.CM-1
    - Continuously monitor access to PII using automated tools.
    - Generate alerts for unauthorized access attempts and investigate promptly.
5. **Training**: NIST CSF PR.AT-1
    - Conduct regular training sessions for employees on PII protection.
    - Include guidelines on recognizing and handling PII securely.

Compliance

- Regular audits will be conducted to ensure adherence to this policy.
- Non-compliance will result in disciplinary actions, which may include termination of employment.

Policy for Communicating TLP RED Information

Purpose

To ensure the secure communication of highly sensitive information classified as RED under the Traffic Light Protocol (TLP).

Responsibilities

- **Senior Management**: Approve the communication of TLP RED information.
- **Employees**: Handle TLP RED information in compliance with this policy.
- **IT Security Team**: Ensure secure communication channels are available and used.

Policy Statement

TLP RED information must be communicated securely, with strict controls and documentation, to protect its confidentiality.

Procedures

1. **Approval**: NIST CSF PR.IP-11
    - Obtain written approval from senior management before communicating TLP RED information.
    - Document the approval process and purpose of the communication.
2. **Secure Channels**: NIST CSF PR.DS-5
    - Use encrypted emails or secure messaging platforms to transmit TLP RED information.
    - Verify the security of the communication channels before use.
3. **Need-to-Know Basis**: NIST CSF PR.AC-4
    - Share TLP RED information only with individuals who have a legitimate need to know.
    - Maintain a list of authorized recipients and update it regularly.
4. **Confidentiality Agreements**: NIST SP 800-53 SA-5
    - Require recipients to sign confidentiality agreements before receiving TLP RED information.
    - Document and store confidentiality agreements securely.
5. **Documentation**: NIST CSF PR.PT-1
    - Document all instances of TLP RED information sharing, including the purpose, recipients, and communication method.
    - Store documentation securely and review it regularly for compliance.

Compliance

- Regular audits will be conducted to ensure adherence to this policy.
- Non-compliance will result in disciplinary actions, which may include termination of employment.

Policy for Data Retention and Destruction

Purpose

To define the retention periods and destruction methods for different types of data, ensuring compliance with legal and regulatory requirements.

Responsibilities

- **Data Managers**: Maintain the data retention schedule.
- **IT Personnel**: Implement secure storage and destruction methods.
- **Compliance Officers**: Conduct regular audits and ensure compliance.

Policy Statement

Data must be retained and destroyed in accordance with the defined retention schedule and secure methods to ensure compliance with legal and regulatory requirements.

Procedures

1. **Retention Schedule**: NIST CSF PR.IP-4
    - Establish and maintain a data retention schedule defining the retention periods for various types of data.
    - Review and update the schedule regularly.
2. **Secure Storage**: NIST CSF PR.DS-1
    - Store data securely during the retention period to protect against unauthorized access.
    - Implement appropriate security measures such as encryption and access controls.
3. **Regular Audits**: NIST CSF PR.IP-5
    - Conduct regular audits to ensure compliance with the data retention schedule.
    - Document audit results and address any identified issues promptly.
4. **Destruction Methods**: NIST CSF PR.IP-6
    - Implement secure data destruction methods (e.g., shredding, degaussing, digital wiping) when the retention period expires.
    - Document the destruction process, including the type of data, destruction method, date, and personnel involved.
5. **Documentation**: NIST CSF PR.PT-1
    - Maintain records of data destruction activities.
    - Store documentation securely and review it regularly for compliance.

Compliance

- Regular audits will be conducted to ensure adherence to this policy.
- Non-compliance will result in disciplinary actions, which may include termination of employment.

Policy for Log Retention and Incident Logs

Purpose

To manage the retention and handling of log files, including those related to security incidents.

Responsibilities

- **Log Managers**: Define and manage log retention periods.
- **IT Personnel**: Ensure secure storage and destruction of logs.
- **Security Officers**: Review logs for security threats and compliance.

Policy Statement

Log files must be retained and handled securely, with appropriate retention periods and destruction methods to ensure compliance and support forensic analysis.

Procedures

1. **Log Retention Period**: NIST CSF PR.IP-4
    - Define retention periods for different types of logs, ensuring compliance with regulatory and business requirements.
    - Review and update retention periods regularly.
2. **Storage**: NIST CSF PR.DS-1
    - Store logs securely, ensuring integrity and protection against unauthorized access.
    - Implement appropriate security measures such as encryption and access controls.
3. **Incident Logs**: NIST CSF DE.DP-4
    - Retain logs related to security incidents for a longer period as required for forensic analysis and regulatory compliance.
    - Ensure incident logs are easily accessible for review.
4. **Regular Reviews**: NIST CSF DE.CM-1
    - Regularly review logs to detect and respond to potential security threats.
    - Document review processes and findings.
5. **Destruction**: NIST CSF PR.IP-6
    - Securely destroy logs after the retention period expires, ensuring no residual data remains accessible.
    - Document the destruction process, including the type of logs, destruction method, date, and personnel involved.

Compliance

- Regular audits will be conducted to ensure adherence to this policy.
- Non-compliance will result in disciplinary actions, which may include termination of employment.

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/?
- Welcome to Compass. (n.d.-c). https://web.compass.lighthouselabs.ca/p/13/projects/ir-playbook
- NVD - Home. (n.d.). https://nvd.nist.gov/