**PROJECT 7**

**Title: Incident Response (IR) Plan, Playbook and Policy**

***By Titobiloluwa (Tito) Ilori***

**Table of Content**

|  | **Sections** | | **Page No.** | |
| --- | --- | --- | --- | --- |
| **1** | **Data Breach Incident Response Playbook For RBC – Using NIST 7-step** | | | **2** |
| **2** | **Procedures That Activate the Data Breach Playbook** | | | **4** |
| **3** | **Policy Set for the Playbook** | | | **7** |
| **3.1** | | **User's Information Capture Policy** | | **7** |
| **3.2** | | **PII Access Policy** | | **10** |
| **3.3** | | **Key Management and Cryptography Policy** | | **12** |
| **3.4** | | **Information Classification Policy** | | **14** |
| **3.5** | | **TLP Communication Policy** | | **16** |
| **3.6** | | **Data Retention and Disposal Policy** | | **18** |
| **3.7** | | **Incident Response Policy** | | **21** |
| **3.8** | | **Emergency Change Policy** | | **23** |
|  | **Appendix A: Citations** | | | **25** |

**1. DATA BREACH IR PLAYBOOK FOR RBC –** *Using NIST 7-step*

A screenshot of a computer screen

Description automatically generated

[\*] Global Privacy Notice: Accountability and Privacy By Design – RBC - <https://www.rbc.com/privacysecurity/ca/global-privacy-notice.html>

= Preparation

= Detection

= Analysis

= Containment

= Eradication

= Recovery

= Post-Incident Activity

**Five Items Where this Playbook May Be Triggered**

1. Unauthorized Authentication Attempts on the Domain Controller
2. Disruption of Critical Operational Business Processes (e.g., DoS)
3. Active Phishing Campaign
4. Insider Threat - Admin Tampering or Disabling Login
5. Reports of removable and/or mobile devices being used to copy data.

**Items where stakeholders would need to be informed of the incident. [labelled in the playbook]**

**A.** Compromise of Domain Controller.

1. Data breach on the server
2. Compliance Regulations have been violated (on Laptop/Desktop)
3. Determination of completed or ongoing financial fraud.
4. Risk of the stolen data being released to the public.
5. Disruptions damaging to business operations or the brand of the organization.
6. Insider and 3rd party threat to the intellectual property of the organization

**More Details about The Stakeholder Numbered in the Playbook above.**

1. Internal Stakeholders: The Information/Computer Security Team (CSIRT), Global Chief Privacy Officer and/or Data Protection Officers, Employee/Branch Involved, Legal Department, PR team.
2. External Stakeholders: Law Enforcement, Affected Customers/Investors/Shareholders, Data Protection Authorities Or regulatory bodies.
3. The legal team will ensure the management of regulatory compliance while;
4. the Public Relations (PR) team will handle public communication (affected customers/investors...)

**The following set of policies is attached to this playbook (Chapter 3) for effectively, namely;**

1. User's Information Capture Policy
2. PII Access Policy
3. Key Management and Cryptography Policy
4. Information Classification Policy
5. TLP Communication Policy
6. Data Retention and Disposal Policy
7. Incident Response Policy
8. Emergency Change Policy

**2. Procedures That Activate the Data Breach Playbook**

**2.1 Procedure for Unauthorized Authentication Attempts on the Domain Controller**

Objective: Identify and respond to several unauthorized authentication attempts on the domain controller to prevent potential data breaches.

Steps:

**Step 1:** Real-time Monitoring - Continuously monitor authentication logs and establish alert thresholds for detecting multiple failed login attempts.

**Step 2:** Incident Detection - When the threshold is exceeded, trigger an alert to the Security Operations Center (SOC) or designated Incident Response Team (IRT).

**Step 3:** Incident Response - The IRT investigates the source of the unauthorized attempts, identifies affected accounts, and determines the potential impact.

**Step 4:** Account Lockout & Remediation - Temporarily lockout affected accounts to prevent further unauthorized access. Reset passwords for compromised accounts and notify users.

**Step 5:** Analysis & Mitigation - Analyze attack patterns, update security measures, and implement additional security controls to mitigate similar incidents in the future.

**Step 6:** Communication - Notify relevant stakeholders, including management and regulatory authorities, about the incident and actions taken to mitigate risks.

**2.2 Procedure for Disruption of Critical Operational Business Processes (e.g., DoS)**

Objective: Detect and respond to disruptions in critical business processes caused by a Denial of Service (DoS) attack.

Steps:

**Step 1:** DoS Detection - Monitor network traffic and server performance to identify signs of a potential DoS attack (e.g., sudden spikes in traffic, and resource exhaustion).

**Step 2**: Incident Confirmation - Verify if the unusual activity is a legitimate DoS attack by cross-referencing with threat intelligence sources or specialized DoS protection solutions.

**Step 3**: Incident Response - Activate the Incident Response Team to initiate the predefined DoS mitigation strategy.

**Step 4**: Mitigation - Divert traffic through DoS protection services, filter malicious traffic, and apply rate-limiting measures to reduce the impact of the attack.

**Step 5**: Business Continuity - Implement backup systems or alternative processes to maintain critical operations during the attack.

**Step 6**: Investigation - Analyze the DoS attack to understand its nature, origin, and potential implications for future improvements to the security infrastructure.

**Step 7**: Reporting & Communication - Report the incident, actions taken, and impact to the relevant authorities, internal stakeholders, and customers if necessary.

**2.3 Procedure for Active Phishing Campaign**

Objective: Detect and respond to an ongoing phishing campaign to minimize the risk of sensitive data compromise.

Steps:

**Step 1**: Email and Web Filtering - Implement strong email and web filtering mechanisms to block known phishing domains and malicious links.

**Step 2**: User Awareness - Conduct regular phishing awareness training for employees to recognize and report suspicious emails.

**Step 3**: Phishing Detection - Utilize phishing detection tools to identify and quarantine suspicious emails sent to users.

**Step 4**: Incident Response - When a phishing attempt is reported or detected, activate the Incident Response Team to analyze and respond promptly.

**Step 5:** Remediation - If any users have clicked on malicious links or provided credentials, take appropriate actions like resetting passwords and performing system scans for malware.

**Step 6**: Threat Intelligence - Share relevant phishing indicators with threat intelligence sources to improve industry-wide defences against similar attacks.

**Step 7**: Communication - Communicate with impacted users about the incident, reiterate best practices, and encourage reporting of any suspicious activities.

**2.4 Procedure for Insider Threat - Admin Tampering or Disabling Login**

Objective: Detect and respond to insider threats involving administrative tampering or attempts to disable login mechanisms.

Steps:

**Step 1**: Privileged Access Monitoring - Implement monitoring and audit controls to track privileged user activities, especially those related to sensor tampering or login mechanisms.

**Step 2**: Access Control - Limit access rights based on the principle of least privilege to reduce the potential damage of insider threats.

**Step 3**: Anomaly Detection - Utilize anomaly detection and behaviour analytics to identify unusual activities performed by privileged users.

**Step 4**: Incident Response - Activate the Incident Response Team when suspicious activities are flagged.

**Step 5**: Investigation - Conduct a thorough investigation to determine the intent and extent of the insider threat.

**Step 6**: Containment - Temporarily revoke access to critical systems if necessary to prevent further tampering or unauthorized actions.

**Step 7:** Reporting & Communication - Report the incident to management, HR, or legal departments, and involve law enforcement if required by regulations or the severity of the incident.

**3. POLICY SET FOR THE PLAYBOOK**

This set of policies should be regularly reviewed, updated and communicated to all relevant personnel within the financial institution to ensure effective implementation and adherence. Additionally, the policies must be compliant with relevant data protection laws and regulations in Canada, such as the Personal Information Protection and Electronic Documents Act (PIPEDA).

[Here](https://docs.google.com/presentation/d/16K6iqqKVMkQq07ZoJfMZ7ZZyg9o-5Hem/edit?usp=sharing&ouid=115416687649530778723&rtpof=true&sd=true) is the link to the slideshow that explains “Why” the policy is being created, and the consequences of non-compliance to both the company and the individual.

**3.1 User's Information Capture Policy 1,3**

**1. Purpose**

The purpose of this User's Information Capture Policy is to establish guidelines and procedures for capturing and handling personal information from users, including customers, employees, and any other individuals, in the financial institution. This policy aims to protect the privacy and confidentiality of user information and ensure compliance with PIPEDA and other applicable data protection laws.

**2. Scope**

This policy applies to all employees, contractors, and third-party entities who capture or have access to personal information from users within the financial institution.

**3. Definition of Personal Information**

a. Personal Information (PI): For the purposes of this policy, personal information refers to any information about an identifiable individual, including but not limited to name, address, contact details, social insurance number, financial information, and any other data that can be used to identify an individual.

**4. Consent for Information Capture**

a. Consent Collection: Before capturing any personal information from users, explicit consent shall be obtained in a clear and transparent manner. Users shall be informed of the specific purposes for which their information is being collected, used, or disclosed.

b. Withdrawal of Consent: Users shall have the right to withdraw their consent for information capture at any time. Processes shall be in place to allow users to withdraw their consent and have their information securely deleted unless legal or regulatory requirements dictate otherwise.

**5. Data Minimization**

a. Minimal Data Collection: Only the minimum amount of personal information required to achieve the specified purpose shall be collected from users. Data capture shall adhere to the principle of data minimization.

**6. Security Measures**

a. Data Security: Personal information captured from users shall be stored securely using appropriate technical and organizational measures to prevent unauthorized access, loss, or disclosure.

b. Access Controls: Access to user data shall be restricted to authorized personnel with a legitimate business need, following the principle of least privilege.

**7. Data Retention**

a. Retention Period: Personal information shall be retained for only as long as necessary to fulfill the purposes for which it was collected, as per the Data Retention and Disposal Policy.

b. Data Disposal: Once the retention period expires or when personal information is no longer needed, it shall be securely disposed of following the Data Retention and Disposal Policy.

**8. Data Sharing and Disclosure**

a. Third-Party Sharing: Personal information shall not be shared with third parties without obtaining explicit consent from the user, except where required or permitted by law.

b. Data Disclosure: Personal information shall be disclosed only to authorized personnel who need the data to perform their duties or comply with legal obligations.

**9. Training and Awareness**

a. Data Privacy Training: All employees, contractors, and third-party entities involved in capturing and handling user information shall undergo regular data privacy and security training to understand their responsibilities and the potential risks associated with handling personal information.

**10. Incident Reporting**

a. Data Breach Reporting: Any suspected or confirmed data breach involving user's personal information must be promptly reported to the Data Protection Officer (DPO) or the designated incident response team.

**11. Consequences of Non-Compliance**

a. Policy Enforcement: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

b. Legal Consequences: Failure to comply with PIPEDA and other applicable data protection laws may lead to legal consequences for the financial institution.

**12. Policy Review and Updates**

a. Policy Review: This policy shall be reviewed regularly to ensure its continued relevance and alignment with changes in regulations and the financial institution's operations.

b. Policy Approval: Any updates to this policy shall be reviewed and approved by the Data Protection Officer (DPO) or designated data governance authority.

**13. Policy Dissemination and Training**

a. Policy Distribution: This policy shall be distributed to all relevant employees, contractors, and third-party entities who capture personal information within the financial institution.

b. Training and Education: Regular training and education programs shall be conducted to ensure that employees understand and adhere to the information capture requirements.

**3.2 PII Access Policy 2,3**

**1. Purpose**

The purpose of this PII Access Policy is to establish guidelines and procedures for accessing and handling Personally Identifiable Information (PII) within the financial institution. This policy aims to ensure that access to PII is granted only to authorized individuals with a legitimate business need and that appropriate security measures are in place to protect the privacy and confidentiality of PII.

**2. Scope**

This policy applies to all employees, contractors, and third-party entities who have access to PII within the financial institution.

**3. Access Control Measures**

a. Need-to-Know Principle: Access to PII shall be granted based on the principle of least privilege, following the "need-to-know" principle. Employees shall only have access to the PII required to perform their job responsibilities.

b. Role-Based Access: Access permissions to systems, databases, and applications containing PII shall be assigned based on job roles and responsibilities. The HR department shall communicate role changes to the IT department promptly.

c. Two-Factor Authentication (2FA): For systems containing sensitive PII, two-factor authentication (2FA) shall be implemented to enhance access security and prevent unauthorized access.

**4. PII Access Request and Approval**

a. Access Request Process: Employees or contractors requiring access to PII must submit a formal access request through the designated process, specifying the reason for the access and the data required.

b. Access Approval: Access requests shall be approved by the data owner (CPO) or an authorized approver, based on the principle of least privilege. The approval process shall include verification of the individual's need for access and their adherence to data protection policies.

**5. PII Access Monitoring and Review**

a. Access Logs: Logs recording access to systems and databases containing PII shall be maintained and regularly monitored for unusual or unauthorized activity.

b. Access Reviews: Regular access reviews shall be conducted to ensure that access privileges are up-to-date and align with the principle of least privilege.

**6. Data Segregation and Encryption**

a. Data Segregation: PII shall be segregated and restricted from being stored or accessed in non-designated systems or unsecured locations.

b. Data Encryption: PII transmitted over networks or stored in databases shall be encrypted using industry-standard encryption algorithms to protect against unauthorized interception.

**7. Third-Party Access to PII**

a. Third-Party Agreements: Third-party entities that require access to PII must sign data protection agreements or contracts that include confidentiality and data security provisions.

b. Third-Party Access Reviews: Regular reviews shall be conducted to assess third-party entities' compliance with data protection agreements and their access to PII.

**8. Employee Training and Awareness**

a. Data Privacy Training: All employees, contractors, and third-party entities with access to PII shall undergo regular data privacy and security training to understand their responsibilities and the potential risks associated with handling PII.

b. Data Breach Response Training: Employees shall receive training on data breach response procedures and their role in reporting and mitigating data breaches.

**9. Incident Reporting**

a. Data Breach Reporting: Any suspected or confirmed data breach involving PII must be promptly reported to the Data Protection Officer (DPO) or the designated incident response team.

**10. Consequences of Non-Compliance**

a. Policy Enforcement: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

b. Legal Consequences: Employees found to have accessed or disclosed PII without proper authorization may face legal consequences under PIPEDA and other applicable laws.

**11. Policy Review and Updates**

a. Policy Review: This policy shall be reviewed regularly to ensure its continued relevance and alignment with changes in regulations and the financial institution's operations.

b. Policy Approval: Any updates to this policy shall be reviewed and approved by the Data Protection Officer (DPO) or designated data governance authority.

**12. Policy Dissemination and Training**

a. Policy Distribution: This policy shall be distributed to all relevant employees, contractors, and third-party entities who handle PII within the financial institution.

b. Training and Education: Regular training and education programs shall be conducted to ensure that employees understand and adhere to the PII access requirements.

**3.3 Key Management and Cryptography Policy 4**

**1. Purpose**

The purpose of this Key Management and Cryptography Policy is to establish guidelines and procedures for the secure generation, storage, distribution, and use of encryption keys and cryptographic materials within the financial institution. This policy aims to ensure the protection of sensitive data, including Personal Information, in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA).

**2. Scope**

This policy applies to all employees, contractors, and third-party entities that have access to the financial institution's information systems and handle sensitive data.

**3. Key Management**

a. Key Generation: Cryptographic keys must be generated using approved, industry-standard algorithms and methods. Keys should have sufficient entropy to resist brute-force attacks and should be created in a secure, controlled environment.

b. Key Storage: Encryption keys must be stored securely and separately from the data they protect. Keys should be stored in encrypted key vaults or hardware security modules (HSMs) with strict access controls.

c. Key Distribution: The distribution of cryptographic keys shall follow a secure process, involving multiple factors of authentication and authorized individuals. Keys should be securely transmitted and protected during transit.

d. Key Rotation: Encryption keys must be rotated regularly, as per the key management schedule, to reduce the potential impact of key compromise. The rotation process should ensure seamless data decryption and re-encryption with new keys.

**4. Cryptography Implementation**

a. Approved Algorithms: Only cryptographic algorithms approved by the financial institution's security team and in compliance with industry standards shall be used.

b. Strong Cipher Suites: SSL/TLS cipher suites, encryption protocols, and hashing algorithms must be configured to use strong cryptographic primitives and resist known vulnerabilities.

c. Data at Rest Encryption: Sensitive data, including Personal Information, must be encrypted when stored on devices, databases, or in the cloud. Encryption keys for data at rest must be managed in accordance with this policy.

d. Data in Transit Encryption: All sensitive data transmitted over public networks, such as the Internet, must be encrypted using approved encryption protocols.

**5. Cryptographic Security Controls**

a. Cryptographic Module Security: Any cryptographic modules or hardware used must comply with relevant standards, such as FIPS 140-2, and undergo regular security assessments.

b. Cryptographic Operations Logging: Cryptographic operations, including key generation, distribution, and usage, must be logged, and monitored for security purposes.

c. Cryptographic Incident Response: Procedures for handling cryptographic incidents, such as suspected key compromise or misuse, must be documented and communicated to all relevant personnel.

**6. Compliance and Auditing**

a. Regular Audits: Cryptographic processes, procedures, and configurations shall be regularly audited to ensure compliance with this policy and relevant regulations.

b. Compliance with PIPEDA: The financial institution shall ensure that the cryptographic measures in place meet the requirements of PIPEDA for protecting Personal Information.

**7. Training and Awareness**

All employees, contractors, and third-party entities handling cryptographic materials or sensitive data shall receive appropriate training on cryptographic best practices and the key management process.

**8. Review and Updates**

This policy shall be reviewed and updated at least annually or as necessary to accommodate changes in technology, regulatory requirements, or the financial institution's operations.

**3.4 Information Classification Policy 3, 6**

**1. Purpose**

The purpose of this Information Classification Policy is to establish a standardized framework for classifying and handling all information, including personal and sensitive data, within the financial institution. This policy aims to protect the privacy of individuals' personal information and comply with the requirements of the Personal Information Protection and Electronic Documents Act (PIPEDA).

**2. Scope**

This policy applies to all employees, contractors, and third-party entities that have access to the financial institution's information assets.

**3. Information Classification Levels**

The financial institution shall use the following classification levels to categorize its information:

a. Public Information (PI): Information that is freely available to the public and has no confidentiality or privacy implications. Examples include general marketing materials and public announcements.

b. Internal Use Only (IUO): Information intended for internal use only and should not be disclosed to external parties. This includes non-sensitive internal documents and general company information.

c. Personal Information (PII): Information that contains personally identifiable information of individuals, such as customers, employees, or business partners. This category includes data protected under PIPEDA.

d. Confidential Information (CI): Highly sensitive information that requires strict access controls and safeguards. This may include financial data, strategic plans, or trade secrets.

**4. Information Confidentiality Classification 6**

a. Classified Confidential: Applies when unauthorized disclosure could reasonably be expected to cause limited or moderate injury to the national interest.

**4.1 Protected**: Information is categorized as “Protected A,” “Protected B” or “Protected C” when unauthorized disclosure could reasonably be expected to cause injury outside of the national interest:

b. Protected C: Applies to the very limited amount of information when unauthorized disclosure could reasonably be expected to cause extremely grave injury outside the national interest, for example, loss of life.

c. Protected B: Applies to information when unauthorized disclosure could reasonably be expected to cause serious injury outside the national interest, for example, loss of reputation or competitive advantage; and

d. Protected A: Applies to information when unauthorized disclosure could reasonably be expected to cause limited or moderate injury outside the national interest, for example, disclosure of an exact salary figure.

**5. Information Handling Guidelines**

a. Classification Responsibility: It is the responsibility of data owners and custodians to classify information accurately based on its sensitivity and importance.

b. Handling Requirements: Each classification level has specific handling requirements, including access controls, encryption, and secure transmission, as outlined in the Data Handling Guidelines document.

c. Access Controls: Access to sensitive information, especially Personal Information (PII) and Confidential Information (CI), shall be granted on a need-to-know basis, and user access will be regularly reviewed and audited.

d. Transmission and Storage: Confidential and Personal Information must be transmitted and stored in an encrypted format, both internally and externally, to prevent unauthorized access.

e. Retention and Destruction: Personal Information will be retained as required by PIPEDA and the organization's data retention policy. Once data is no longer needed, it will be securely destroyed following approved data destruction methods.

**6. Training and Awareness**

All employees, contractors, and third-party entities with access to the financial institution's information shall receive regular training on this Information Classification Policy, data handling procedures, and PIPEDA compliance.

**7. Compliance and Enforcement**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. The Data Protection Officer (DPO) shall monitor and enforce compliance with this policy and report any violations to the appropriate authorities as required by law.

**8. Review and Updates**

This policy shall be reviewed and updated regularly to ensure its continued relevance and alignment with changes in PIPEDA regulations and the financial institution's operations.

**3.5 TLP Communication Policy 7**

**1. Purpose**

The purpose of this TLP Communication Policy is to establish guidelines for sharing sensitive information, including potential cybersecurity threats and incidents, with other financial institutions and trusted partners within the cybersecurity community. This policy aims to ensure that the sensitivity of the shared information is appropriately indicated using the Traffic Light Protocol (TLP) framework.

**2. Scope**

This policy applies to all employees, contractors, and third-party entities involved in incident response and information sharing within the financial institution.

**3. TLP Designations**

a. TLP RED: Information marked as TLP RED is highly sensitive and should be shared only with individuals who have a direct need to know and have signed appropriate non-disclosure agreements. TLP RED information is strictly for incident response and handling purposes and should not be disseminated beyond the authorized recipients.

b. TLP AMBER: Information marked as TLP AMBER is sensitive and should be shared with a limited group of trusted partners and stakeholders who are actively involved in incident response and have a legitimate need to know. Recipients of TLP AMBER information should be aware of their responsibilities regarding handling and dissemination.

c. TLP GREEN: Information marked as TLP GREEN is for general dissemination within the financial institution or the wider cybersecurity community. TLP GREEN information can be shared openly with appropriate context and without restrictions.

**4. TLP Handling Procedures**

a. TLP Marking: All sensitive information shared within or outside the financial institution must be appropriately marked with the relevant TLP designation.

b. Access Controls: Access to TLP RED information must be restricted to designated members of the incident response team and individuals who are directly involved in mitigating the incident. TLP AMBER information should be shared with authorized partners who have previously agreed to adhere to TLP guidelines.

c. Dissemination Guidelines: Recipients of TLP RED and TLP AMBER information must be informed of the restrictions on sharing and must seek approval before further disseminating the information.

d. Retention and Destruction: TLP RED and TLP AMBER information must be retained only for the duration required for incident response and investigation. Once the information is no longer needed, it should be securely destroyed according to the organization's data retention and destruction policy.

**5. Training and Awareness**

All employees and individuals involved in information sharing and incident response must receive training on TLP guidelines and best practices for handling and disseminating sensitive information.

**6. Compliance and Enforcement**

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. The Incident Response Team (IRT) and designated authorities shall monitor and enforce compliance with this policy.

**7. Review and Updates**

This policy shall be reviewed regularly to ensure its continued relevance and alignment with changes in industry best practices and the financial institution's operations.

**3.6 Data Retention and Disposal Policy 8,9**

**1. Purpose**

The purpose of this Data Retention and Disposal Policy is to establish guidelines and procedures for the retention and secure disposal of data within the financial institution. This policy aims to ensure that data is retained for the necessary period, in compliance with legal and regulatory requirements, and disposed of securely when no longer needed.

**2. Scope**

This policy applies to all employees, contractors, and third-party entities that handle and manage data within the financial institution.

**3. Data Classification**

a. Sensitive Data: Data containing personally identifiable information (PII), financial records, and other sensitive information must be identified and appropriately classified based on its sensitivity and legal requirements.

b. Non-Sensitive Data: Non-sensitive data, which does not contain PII or sensitive information, may also be classified for organizational purposes.

**4. Data Retention**

a. Retention Periods: Data retention periods will be defined for each data category based on legal, regulatory, and business requirements. The Data Classification and Retention Schedule will specify the retention periods for different types of data.

b. Review and Updates: The Data Classification and Retention Schedule will be reviewed and updated at least annually or as needed to reflect changes in regulations and business needs.

**5. Data Disposal**

a. Secure Data Disposal: Data disposal will be carried out using secure methods, such as data wiping, physical destruction, or encryption-based disposal, to prevent unauthorized access.

b. Disposal Process: The Data Disposal Process will be documented and followed to ensure consistent and secure data disposal practices.

c. Authorized Disposal Personnel: Only authorized personnel, following the Data Disposal Process, are allowed to perform data disposal activities.

**6. Data Backup and Archiving**

a. Backup Policy: Data backup policies and procedures will be established to ensure the availability and integrity of data for business continuity purposes.

b. Archiving Policy: Data archiving guidelines will be defined to manage the long-term retention and accessibility of historical data.

**7. Compliance and Auditing**

a. Compliance Monitoring: The Chief Privacy Officer (CPO) or assigned personnel will monitor compliance with this policy and related data management practices.

b. Data Inventory and Audit: Regular data inventories and audits will be conducted to identify and validate data retention and disposal practices.

**8. Incident Response and Data Disposal**

a. Data Breach Incident Response: In the event of a data breach or security incident, the Data Breach Incident Response Team will follow predefined procedures to determine if any affected data requires secure disposal. Disposal activities will be documented as part of the incident response process.

b. Secure Disposal During Decommissioning: When decommissioning hardware, equipment, or software that contains data, the responsible team shall ensure that all data is securely disposed of in accordance with the Data Disposal Process.

**9. Monitoring and Reporting**

a. Data Disposal Auditing: The Data Disposal Process shall be subject to periodic audits to ensure compliance with this policy. Audit results will be reported to the DPO or relevant authority.

b. Data Retention Compliance: Compliance with the Data Retention Schedule will be regularly monitored, and any deviations will be investigated and remediated promptly.

**10. Third-Party Data Processors**

a. Third-Party Contracts: Third-party entities processing data on behalf of the financial institution shall be contractually bound to comply with this policy's data retention and disposal requirements.

b. Due Diligence: The financial institution shall conduct due diligence on third-party data processors to ensure that they have adequate data management and disposal practices in place.

**11. Employee Separation**

a. Data Removal: When an employee's tenure with the financial institution ends, their access to data and systems shall be promptly terminated, and any data in their possession shall be securely returned or disposed of according to the Data Disposal Process.

**12. Training and Awareness**

All employees, contractors, and third-party entities involved in data management must receive training on this policy, data retention schedules, and secure data disposal procedures.

**13. Review and Updates**

This policy shall be reviewed and updated periodically to ensure its continued relevance and alignment with changes in regulations and the financial institution's operations.

**14. Exceptions**

Exceptions to this policy may be granted in specific circumstances, subject to approval by the Chief Privacy Officer or relevant authority and must be documented and justified.

**3.7 Incident Response Policy 10,11**

**1. Purpose**

The purpose of this Incident Response Policy is to establish a structured approach for identifying, assessing, and responding to security incidents that involve personal information within the financial institution. This policy aims to protect the confidentiality, integrity, and availability of personal information and to comply with PIPEDA and other applicable data protection laws.

**2. Scope**

This policy applies to all employees, contractors, and third-party entities who handle personal information within the financial institution and are involved in incident response activities.

**3. Incident Classification**

a. Security Incident: A security incident refers to any event that compromises or threatens to compromise the confidentiality, integrity, or availability of personal information.

b. Data Breach: A data breach is an incident where there is unauthorized access to, or disclosure of, personal information that may result in significant harm or the risk of significant harm to individuals.

**4. Incident Response Team (IRT)**

a. IRT Formation: An Incident Response Team shall be established, comprising representatives from IT, Information Security, Legal, Privacy, Communications, and relevant business units.

b. IRT Responsibilities: The IRT shall be responsible for coordinating incident response efforts, conducting investigations, and communicating with relevant stakeholders.

**5. Incident Reporting**

a. Reporting Procedure: All employees and contractors must promptly report any suspected or confirmed security incidents or data breaches to the designated incident reporting channel.

b. Data Breach Notification: In the event of a data breach involving personal information, the IRT shall assess the risk of significant harm to affected individuals and, if required by law, notify affected individuals and relevant authorities.

**6. Incident Response Process**

a. Incident Identification: The IRT shall promptly identify and confirm security incidents, including data breaches, based on incident reports and monitoring activities.

b. Incident Triage: Incidents shall be triaged based on their severity, impact on personal information, and potential risks to the financial institution and affected individuals.

c. Containment and Mitigation: The IRT shall take immediate actions to contain the incident, minimize its impact, and prevent further unauthorized access or disclosure of personal information.

d. Investigation: The IRT shall conduct a thorough investigation to determine the cause, scope, and extent of the incident, and to identify affected individuals and data.

e. Remediation and Recovery: The IRT shall develop and execute a plan for remediating the incident, recovering affected systems, and restoring the security of personal information.

**7. Data Breach Notification and Communication**

a. Notification Obligations: If the data breach poses a real risk of significant harm to affected individuals, the IRT shall notify those individuals in accordance with PIPEDA requirements.

b. Regulatory Reporting: The IRT shall report data breaches to the appropriate regulatory authorities, as required by PIPEDA or other applicable laws.

c. Stakeholder Communication: The IRT shall communicate with relevant stakeholders, including customers, employees, business partners, and regulators, as necessary, to provide updates on the incident and its resolution.

**8. Post-Incident Review**

a. Post-Incident Analysis: The IRT shall conduct a post-incident review to assess the effectiveness of the incident response process and identify opportunities for improvement.

**9. Training and Awareness**

a. Incident Response Training: All employees, contractors, and third-party entities involved in handling personal information shall receive training on the incident response procedures outlined in this policy.

**10. Policy Review and Updates**

a. Policy Review: This policy shall be reviewed regularly to ensure its continued relevance and alignment with changes in regulations and the financial institution's operations.

b. Policy Approval: Any updates to this policy shall be reviewed and approved by the designated authority or data governance committee.

**11. Policy Dissemination**

a. Policy Distribution: This policy shall be distributed to all relevant employees, contractors, and third-party entities who handle personal information within the financial institution.

**3.8 Emergency Change Policy 1,2,3**

**1. Purpose**

The purpose of this Emergency Change Policy is to establish guidelines and procedures for handling emergency changes to systems, applications, and processes within the financial institution. This policy aims to mitigate the risk of security incidents, including those involving personal information, that may arise during emergency change situations.

**2. Scope**

This policy applies to all employees, contractors, and third-party entities involved in managing and executing changes to the financial institution's systems and processes which shall be assessed and formally approved by senior management.

**3. Definition of Emergency Change**

a. Emergency Change: An emergency change refers to any change that is necessary to address an immediate threat or to prevent a significant disruption to the financial institution's operations, including those that could impact the security of personal information.

**4. Emergency Change Procedures**

a. Identification and Justification: Emergency changes must be identified and justified promptly by the appropriate authority, such as the Incident Response Team (IRT) or the IT Security Team. The reason for the emergency change and its potential impact on personal information security shall be documented.

b. Approval and Authorization: The emergency change must be approved by the designated authority, such as the Change Advisory Board (CAB) or the IT Steering Committee, before implementation. The approval process shall consider the urgency of the situation and the potential risks to personal information.

c. Testing and Validation: Wherever possible, the emergency change shall be tested and validated in a controlled environment to minimize adverse effects on personal information and other critical systems.

**5. Data Protection and Privacy Considerations**

a. Personal Information Security: Emergency changes must prioritize the security of personal information. Any changes that could potentially compromise the confidentiality, integrity, or availability of personal information shall be carefully assessed and appropriately mitigated.

b. Data Handling Compliance: Emergency changes must adhere to data handling and data protection requirements as outlined in relevant policies and privacy regulations, including PIPEDA.

**6. Communication and Reporting**

a. Incident Notification: In case the emergency change is triggered by a security incident involving personal information, the Incident Response Team shall be informed immediately for appropriate response and investigation.

b. Stakeholder Communication: Stakeholders affected by the emergency change, including data subjects whose personal information may be impacted, shall be informed about the change and its implications as soon as feasible by the PR team.

**7. Rollback Plan**

a. Rollback Strategy: An emergency change must have a well-defined rollback plan to return the systems and processes to their previous state if the change does not produce the desired outcome or introduces unintended consequences.

**8. Documentation and Post-Change Review**

a. Change Documentation: The emergency change process and its outcomes shall be documented in detail, including reasons, actions taken, and results.

b. Post-Change Review: After the emergency change has been implemented, a post-change review shall be conducted to evaluate its effectiveness and any impact on personal information security.

**9. Training and Awareness**

a. Training on Emergency Change Procedures: Employees, contractors, and third-party entities involved in emergency change management shall receive training on the procedures outlined in this policy.

**10. Policy Review and Updates**

a. Policy Review: This policy shall be reviewed periodically to ensure its continued relevance and alignment with changes in regulations and the financial institution's operations.

b. Policy Approval: Any updates to this policy shall be reviewed and approved by the designated authority or data governance committee.

**11. Policy Dissemination**

a. Policy Distribution: This policy shall be distributed to all relevant employees, contractors, and third-party entities involved in emergency change management within the financial institution.

**Appendix A: Citations**

1. PIPEDA in brief - Office of the Privacy Commissioner of Canada (May 31, 2019) - <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/>

2. The Digital Privacy Act and PIPEDA - Office of the Privacy Commissioner of Canada (Nov 20, 2015) - <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_63_s4/>

3. PIPEDA fair information principles - Office of the Privacy Commissioner of Canada (May 31, 2019) - <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/>

4. Government of Canada Key Management Infrastructure (GC KMI), Communications Security Establishment (Mar 19, 2021) - <https://www.cse-cst.gc.ca/en/accountability/transparency/reports/government-canada-key-management-infrastructure-gc-kmi>

5. Cryptographic & Key Management Policy (V5.0 Jan 12, 2023 LT) - <https://qrs-research.co.uk/wp-content/uploads/2021/10/Cryptographic-and-Key-Management-Policy.pdf>

6. Directive on Security Management - Appendix J: Standard on Security Categorization - Government of Canada (July 1, 2019) - <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32614>

7. Traffic Light Protocol (TLP) Definitions and Usage - CISA (Aug 22, 2022) - <https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage>

8. Personal Information Retention and Disposal: Principles and Best Practices - Office of the Privacy Commissioner of Canada (Aug 13, 2021) - <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/gd_rd_201406/>

9. PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention - Office of the Privacy Commissioner of Canada (Aug 13, 2020) - <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/>

10. What you need to know about mandatory reporting of breaches of security safeguards - Office of the Privacy Commissioner of Canada (Aug 13, 2021) - <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>

11. A full year of mandatory data breach reporting: What we’ve learned and what businesses need to know - Office of the Privacy Commissioner of Canada (Oct 31, 2019) - <https://www.priv.gc.ca/en/blog/20191031/>