IR Plan, Playbook and Policy Project

W06D4 March 14, 2024

By: Heather Fincati

Table Of Contents

Scope of Policies

This document outlines a comprehensive set of policies designed to safeguard critical business assets and mitigate potential security threats, specifically ransomware attacks, within Canadian Tire.

Comprehensive Policy Suite:

1. **Access Control and Privilege Management (ACPM) Policy:** Defines user access controls and privilege levels to minimize the risk of unauthorized access.
2. **Email and Attachment Security (EAAS) Policy:** Establishes protocols for secure email practices and safeguards against phishing attempts.
3. **Endpoint Security and Patch Management (ESPM) Policy:** Outlines procedures for securing devices and ensuring timely software updates to address vulnerabilities.
4. **Data Backups and Recovery (DBAR) Policy:** Defines a comprehensive data backup and recovery strategy to ensure business continuity in case of disruptions.
5. **Incident Response and Reporting (IRAR) Policy:** Provides a structured approach to identifying, containing, and recovering from security incidents.

These policies emphasize clear roles and responsibilities, along with corresponding training programs, to empower employees in maintaining a secure IT environment.

Access Control and Privilege Management (ACPM) Policy

a. Policy Purpose and Scope

Purpose: This policy establishes guidelines for access control and privilege management within the organization. We will safeguard sensitive information and minimize the risk of unauthorized access, data breaches, and system misuse.

Scope: This policy applies to all employees, contractors, and third-party users with access to the organization's IT systems and resources.

b. Responsibilities

Upper Management:

- Publicly endorse and actively promote the importance of information security within the organization.
- Allocate sufficient resources for effective implementation of the ACPM policy (NIST, 2020). This includes funding for user access management tools, security awareness training programs informed by MITRE ATT&CK mitigations (MITRE ATT&CK®, (n.d.)), and personnel with the necessary expertise.
- Provide oversight and ensure the ACPM policy remains current and aligns with evolving security threats.

Business Operational Leads (BOLs):

- **Develop & Enforce:** BOLs collaborate with IT to create, maintain, and enforce policies, tailoring it to their department's needs and industry regulations.
- **Communicate & Educate:** BOLs ensure their teams are aware of the policies through training, onboarding materials, and requiring user acknowledgement.
- **Monitor & Address:** BOLs work with IT to monitor for potential misuse and address any violations through outlined disciplinary actions.

IT Security:

- Develop and implement the ACPM policy in collaboration with relevant stakeholders, including human resources and legal departments.
- Design, implement, and maintain a strong system for controlling who can access our computer systems and what they can do on those systems. This policy will ensure people only have the bare minimum access they need to do their jobs (principle of least privilege).
- Manage user accounts and privileges throughout the employee lifecycle, including creation, modification, suspension, and termination of access rights.
- Continuously monitor and audit system access to identify and address any suspicious activity or potential security breaches.

Individual Users:

- Actively participate in security awareness training programs to stay informed about security best practices and potential threats.
- Comply with all the provisions outlined in the ACPM policy, including following secure access procedures and reporting any suspicious activity promptly.
- Protect sensitive information and avoid unauthorized access to data or systems by adhering to access control protocols. (Note: Avoid modifying or deleting backups unless following established procedures).

c. Policy Statement

This policy emphasizes the importance of robust access controls and least privilege to protect our IT systems and data.

1. **Clearly Defined Roles and Permissions:** We establish well-defined user roles with specific permissions associated with each role. Assigned permissions adhere to the principle of least privilege, granting users only the minimum access level required to perform their designated tasks.

2. **Multi-Factor Authentication (MFA):** An additional layer of security is implemented through mandatory multi-factor authentication (MFA) for all user accounts. This requirement is especially stringent for privileged users and access to critical systems. MFA adds a secondary verification step beyond just a username and password, significantly reducing the risk of unauthorized access.

3. **Regular Reviews and Updates:** To ensure the effectiveness of access controls, we conduct periodic reviews and updates. This process verifies that user permissions remain aligned with their current roles and responsibilities. Additionally, any changes in user roles or system configurations are promptly reflected in access control procedures.

d. Procedures and Guidelines

User Access Request and Approval:

- A formal process will be established for requesting and approving user access to internal systems and resources.
- Requests must clearly define the user's role, required access level, and justification for access.
- Approvals will be granted based on the principle of least privilege.

Account Management:

- User accounts will be disabled upon termination of employment, contract expiration, or any significant changes in job duties.
- Privileged accounts will be subject to more stringent access controls and monitoring.

Password Management:

- Strong password policies will be enforced, including minimum password length, complexity requirements, and regular password changes.
- Sharing of passwords is strictly prohibited.

e. Compliance and Consequences

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Violations may also lead to the suspension or revocation of user access privileges.
- The organization reserves the right to take legal action against any individual or group engaging in unauthorized access attempts or malicious activities.
- Non-compliance with Payment Card Industry Data Security Standard (PCI DSS, 2018) can result in fines, reputational damage, and potential loss of business with card networks.

- Non-compliance with Personal Information Protection and Electronic Documents Act (PIPEDA, 2018), can launch an investigation by the Office of the Privacy Commissioner (OPC) resulting in a possibilities of several things such as; Recommendations and Corrective Action Plans, Publication of Public Reports, and/or Financial Penalties.

f. Exceptions

- Exceptions to this policy include employees requiring admin privileges and/or other contractors or third-parties requiring full system access to perform their functions.

g. Revision History

Policy	Last Revision	Next Revision
ACPM Policy 1.0	13/9/2023	13/9/2024

h. References

Access management. Access Management, Mitigation M0801 - ICS | MITRE ATT&CK®. (n.d.).

https://attack.mitre.org/mitigations/M0801/

Special Publication 800-53 Rev. 5, National Institute of Standards and Technology, NIST, Published: September 2020.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Payment Card Industry Data Security Standard (PCI DSS), Reference Guide, v3.2.1, July 2018

https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Personal Information Protection and Electronic Documents Act (PIPEDA), Legislation and Regulations, Modified: January 2018

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

i. Definitions

Access Control and Privilege Management (ACPM): Controlling who can access our computer systems and what they can do on those systems.

Multi-Factor Authentication (MFA): An extra layer of security that requires something additional besides just a username and password to log in, eg. a code from your phone.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS mandates specific access control requirements for organizations that store, process, or transmit cardholder data. These controls aim to ensure that only authorized personnel have access to cardholder data and that such access is monitored and logged.

Personal Information Protection and Electronic Documents Act (PIPEDA): Is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of their commercial activity. It mandates that organizations implement safeguards to protect personal information, and strong access controls are a key element of such safeguards.

j. Approval and Review Process

Rex Lee is in charge of approval and setting a regular review schedule.

k. Effective Date

13/3/2024

l. Contact Information

Karen Tire - Head of Human Resources

Phone: 999-999-9999

Email: *karen_tire@CTI.com*

Email and Attachment Security (EAAS) Policy

a. Policy Scope and Purpose

Purpose: This policy is designed to create guidelines around acceptable use of email and attachments. We will actively be aware of incoming suspicious email addresses, irregular requests via email, and suspicious attachments to minimize risk of unsafe software (NIST, 2012) entering our systems.

Scope: This policy applies to all employees, contractors, and third-party users with access to the organization's IT systems and resources.

b. Responsibilities

Upper Management:

- Ensures the implementation and enforcement of this policy.
- Publicly endorse and actively promote the importance of information security within the organization.
- Allocates resources for user access management and security awareness training supported by MITRE (MITRE ATT&CK®., (n.d)) mitigations.

Business Operational Leads (BOLs):

- Collaborate with IT to develop user training on email security best practices.
- Integrate email security awareness into departmental onboarding processes.
- Encourage open communication within their teams to report suspicious emails.

IT Security:

- Defines and implements user roles and access controls.
- Manages user accounts and privileges.
- Monitors and audits system access.

Individual Users:

- Comply with the provisions outlined in this policy.
- Any login credential reset requests must go through IT immediately.
- Any login credentials leaked must be reported to IT Security as soon as the user is aware they have been compromised.

c. Policy Statement

To safeguard our organization's data and systems by promoting secure email practices, implementing robust email filtering, and educating employees to identify and avoid phishing attempts.

This statement captures the essence of the policy by highlighting these key points:

1. **Safeguarding data and systems:** This emphasizes the policy's purpose of protecting the organization from potential security threats(NIST, 2018)
2. **Promoting secure email practices:** This indicates the policy encourages responsible email usage by employees
3. **Implementing robust email filtering:** This underlines the importance of technical controls to supplement employee awareness
4. **Educating employees:** This emphasizes the crucial role of employee training in identifying and avoiding phishing attacks

d. Procedures and Guidelines

- **Email Vigilance:**
    - When opening emails, ensure the email is from a trusted source.
    - Do not click on any links that will take you to an external site.
    - Do not download any content nested within the email.
    - In case of breach refer to the corresponding playbook for proper remediation steps.
- **Password Management:**
    - All employees, third-parties, and contractors must keep provided passwords private and secure.
    - All internal employee passwords will be updated on a regular basis.
    - Minimum password length and complexities will be enforced when creating passwords per MITRE (MITRE ATT&CK®. (n.d)) recommendations.
- **Logging In:**
    - All employees must not access their internal email outside of approved devices (i.e., company laptop, office desktop, office designated mobile device).
    - Login attempts done outside of normal devices or hours will be flagged and monitored.

e. Compliance and Consequences

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Violations may also lead to the suspension or revocation of user access privileges.
- The organization reserves the right to take legal action against any individual or group engaging in unauthorized access attempts or malicious activities.
- Non-compliance with Payment Card Industry Data Security Standard (PCI DSS, 2018) can result in fines, reputational damage, and potential loss of business with card networks.
- Non-compliance with Personal Information Protection and Electronic Documents Act (PIPEDA, 2018), can launch an investigation by the Office of the Privacy Commissioner (OPC) resulting in a possibilities of several things such as; Recommendations and Corrective Action Plans, Publication of Public Reports, and/or Financial Penalties.

f. Revision History

Policy	Last Revision	Next Revision
EAS Policy 1.0	13/9/2024	13/4/2025

g. References:

Password policies. Password Policies, Mitigation M1027 - Enterprise | MITRE ATT&CK®. (n.d.).
https://attack.mitre.org/mitigations/

Special Publication 800-61 Rev. 2, National Institute of Standards and Technology, NIST, Published: August 2012
https://csrc.nist.gov/pubs/sp/800/61/r2/final

Payment Card Industry Data Security Standard (PCI DSS), Reference Guide, v3.2.1, Published: July 2018
https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Personal Information Protection and Electronic Documents Act (PIPEDA), Legislation and Regulations, Modified: January 2018
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

h. Definitions

Phishing: is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. Eg; Missed delivery messages, bank deposit messages, credential update messages, Canadian Gov't tax messages, etc.

Strong Password: A strong password is one that is designed to be hard for a person or program to guess. Because the purpose of a password is to ensure that only authorized users can access resources, a password that is easy to guess is a cybersecurity risk. Using a combination of words, numbers and special characters that makes sense to the user will be way more secure. For example, "1Lov3Blu3berri3$inMyP!e" is a strong password.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS mandates specific access control requirements for organizations that store, process, or transmit cardholder data. These controls aim to ensure that only authorized personnel have access to cardholder data and that such access is monitored and logged.

Personal Information Protection and Electronic Documents Act (PIPEDA): Is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of their commercial activity. It mandates that organizations implement safeguards to protect personal information, and strong access controls are a key element of such safeguards.

i. Approval and Review Process

Rex Lee is in charge of approval and setting a regular review schedule.

j. Effective Date

13/3/2024

k. Contact Information

Karen Tire - Head of Human Resources

Phone: 999-999-9999

Email: *karen_tire@CTI.com*

Endpoint Security and Patch Management (ESPM) Policy

a. Police Purpose and Scope

Purpose: This policy is designed to create guidelines around the security of devices like laptops, desktops, and phones (endpoints) and keeping software programs up-to-date with the latest security fixes (patch management). By following these guidelines, we can ensure our systems are protected from security threats (NIST, 2020).

Scope: This policy applies to all devices that connect to the organization's IT systems and resources, including:

- Company-owned laptops, endpoint devices, Point of Sales machines and desktops
- Employee-owned devices (laptops, desktops, phones, tablets) used to access work email, applications, or data
- Contractor and third-party user devices used to access the organization's network

This policy outlines the requirements and procedures for securing these devices and keeping their software up-to-date to minimize security vulnerabilities and cyber threats.

d. Responsibilities

Upper Management:

- Ensures the implementation and enforcement of this policy.
- Publicly endorse and actively promote the importance of information security within the organization.
- Allocates resources for user access management and security awareness training supported by MITRE mitigations.

Business Operational Leads (BOLs):

- Promote awareness and integrate endpoint security and patch management awareness into departmental training programs.
- Facilitate communication while encouraging open communication within their teams to report any suspicious device activity or potential security breaches.
- Ensure compliance by monitoring team members' devices (if applicable) for adherence to the policy, working with IT to address any identified non-compliance issues.

IT Security:

- Defines and implements user roles and access controls.
- Manages user accounts and privileges.
- Monitors and audits system access.

Individual Users:

- Comply with the provisions outlined in this policy.
- Report any suspicious activity or unauthorized access attempts to IT Security immediately.

e. Policy Statements

To safeguard our organization's data and systems by promoting secure email practices, implementing robust email filtering, and educating employees to identify and avoid phishing attempts.

This statement captures the essence of the policy by highlighting these key points:

1. **Proactive Safeguarding:** It emphasizes the preventive nature of the policy, aiming to secure devices before threats arise.
2. **Endpoint Security Measures:** It highlights the different security measures employed, including antivirus, patching, and application control.
3. **Minimize Vulnerabilities:** It underlines the policy’s goal of reducing weaknesses that attackers can exploit.
4. **Mitigate Cyber Threats:** It emphasizes the overall objective of protecting the organization from cyber attacks.

e. Compliance and Consequences

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Violations may also lead to the suspension or revocation of user access privileges.
- The organization reserves the right to take legal action against any individual or group engaging in unauthorized access attempts or malicious activities.
- Non-compliance with Payment Card Industry Data Security Standard (PCI DSS, 2018) can result in fines, reputational damage, and potential loss of business with card networks.
- Non-compliance with Personal Information Protection and Electronic Documents Act (PIPEDA, 2018), can launch an investigation by the Office of the Privacy Commissioner (OPC) resulting in a possibilities of several things such as; Recommendations and Corrective Action Plans, Publication of Public Reports, and/or Financial Penalties.

f. Revision History

Policy	Last Revision	Next Revision
ESAPM Policy 1.0	13/9/2024	13/4/2025

g. References

Special Publication 800-53 Rev. 5, National Institute of Standards and Technology, NIST, Published: September 2020.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Payment Card Industry Data Security Standard (PCI DSS), Reference Guide, v3.2.1, July 2018

https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Personal Information Protection and Electronic Documents Act (PIPEDA), Legislation and Regulations, Modified: January 2018

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

h. Definition

Endpoint Security: Security measures installed on individual devices like laptops, desktops, and phones. Such as; antivirus software, firewalls, etc.

Patch Management: Keeping software programs up-to-date with the latest security fixes that are applied regularly.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS mandates specific access control requirements for organizations that store, process, or transmit cardholder data. These controls aim to ensure that only authorized personnel have access to cardholder data and that such access is monitored and logged.

Personal Information Protection and Electronic Documents Act (PIPEDA): Is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of their commercial activity. It mandates that organizations implement safeguards to protect personal information, and strong access controls are a key element of such safeguards.

i. Approval and Review Process

Rex Lee is in charge of approval and setting a regular review schedule.

j. Effective Date

13/3/2024

k. Contact Information

Karen Tire - Head of Human Resources

Phone: 999-999-9999

Email: *karen_tire@CTI.com*

Data Backups and Recovery (DBAR) Policy

a. Policy Scope and Purpose

Purpose: This policy is designed to ensure the availability and integrity of critical business data by implementing a comprehensive backup and recovery strategy. To minimize downtime and data loss in the event of hardware failures, security incidents, or natural disasters.

Scope: This policy applies to all employees, contractors, and third-party users with access to the organization's IT systems and resources.

b. Responsibilities

Upper Management:

- Ensures the implementation and enforcement of this policy.
- Publicly endorse and actively promote the importance of information security within the organization.
- Allocates resources for user access management and security awareness training supported by MITRE mitigations.

Business Operational Leads (BOLs):

- Identify critical data and collaborate with their teams to identify and categorize critical business data requiring regular backups.
- Awareness & education training integrating data backup and recovery procedures into departmental training programs, emphasizing the importance of data protection.
- Incident reporting should be encouraged so team members promptly report any potential data loss incidents to ensure timely recovery procedures can be initiated.

IT Security:

- Defines and implements user roles and access controls.
- Manages user accounts and privileges.
- Monitors and audits system access.

Individual Users:

- Comply with the provisions outlined in this policy.
- Only authorized personnel will have access to backups.

c. Policy Statement

To ensure business continuity and minimize data loss by implementing a comprehensive backup and recovery strategy. This strategy includes regular backups of critical data to a secure, offsite location following the 3-2-1 backup rule, and regular testing of backups to guarantee successful restoration in the event of disruptions (e.g., hardware failure, power outage).

This statement emphasizes the key aspects of the policy:

1. **Business Continuity:** Highlights the policy's role in ensuring continued operations even during disruptions.
2. **Minimize Data Loss:** Underlines the importance of safeguarding critical information.
3. **Comprehensive Backup Strategy**: Mentions the key components of the backup plan.
4. **3-2-1 Backup Rule:** (NIST, n.d, Page 2), References the specific data redundancy method for added clarity.
5. **Regular Testing:** Emphasizes the importance of verifying backup functionality.

d. Procedures and Guidelines

- **Backups:**
  - Perform weekly backups for all servers.
  - Regularly test backup integrity.
  - Store backups in physically safe locations.
- **Cloud Backups:**
  - Cloud backups done bi-weekly
  - Access must be available 24/7.
  - Integrity must be regularly verified.
- **Recovery:**
  - Only authorized personnel will collect backups and begin the restoration process.
  - Only authorized personnel have the ability to authorize pulling a particular backup state for recovery.
  - Recovery only to be completed once the threat has been confirmed to be 100% eradicated.

e. Compliance and Consequences

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Violations may also lead to the suspension or revocation of user access privileges.
- The organization reserves the right to take legal action against any individual or group engaging in unauthorized access attempts or malicious activities.
- Non-compliance with Payment Card Industry Data Security Standard (PCI DSS, 2018) can result in fines, reputational damage, and potential loss of business with card networks.
- Non-compliance with Personal Information Protection and Electronic Documents Act (PIPEDA, 2018), can launch an investigation by the Office of the Privacy Commissioner (OPC) resulting in a possibilities of several things such as; Recommendations and Corrective Action Plans, Publication of Public Reports, and/or Financial Penalties.

f. Revision History

Policy	Last Revision	Next Revision
DBAR Policy 1.0	13/9/2024	13/4/2025

g. References

Protecting Data From Ransomware and Other Data Loss, The National Cybersecurity Center of Excellence, (n.d)

https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

Payment Card Industry Data Security Standard (PCI DSS), Reference Guide, v3.2.1, July 2018

https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Personal Information Protection and Electronic Documents Act (PIPEDA), Legislation and Regulations, Modified: January 2018

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

h. Definitions

3-2-1 Rule: Create 3 copies of data, store them on 2 different media types and keep 1 physically off-site for redundancy in case of data loss scenarios.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS mandates specific access control requirements for organizations that store, process, or transmit cardholder data. These controls aim to ensure that only authorized personnel have access to cardholder data and that such access is monitored and logged.

Personal Information Protection and Electronic Documents Act (PIPEDA): Is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of their commercial activity. It mandates that organizations implement safeguards to protect personal information, and strong access controls are a key element of such safeguards.

i. Approval and Review Process

Rex Lee is in charge of approval and setting a regular review schedule.

j. Effective Date

13/3/2024

k. Contact Information

Karen Tire - Head of Human Resources

Phone: 999-999-9999

Email: *karen_tire@CTI.com*

Incident Response and Reporting (IRAR) Policy

a. Policy Scope and Purpose

Purpose: This policy is designed to create an understanding of incident response and reporting. The point is to have clear actionable guidelines in case of an incident which will shorten response times and mitigate incident risks.

Scope: This policy applies to all employees, contractors, and third-party users with access to the organization's IT systems and resources.

b. Responsibilities

Upper Management:

- Approve the incident response plan and allocate the necessary resources for its implementation and ongoing maintenance. This includes funding for training, tools, and personnel to effectively execute the plan.
- Provide clear communication regarding the incident response policy to all employees. They are responsible for ensuring the plan is followed during an incident and overseeing the overall response effort.
- Focus on business continuity during an incident. This may involve ensuring critical operations can be maintained even with disruptions and facilitating a swift recovery process.

Business Operational Leads (BOLs):

- Incident awareness training implemented to integrate incident response and reporting procedures into departmental training programs. This training should raise awareness of potential security incidents and emphasize the importance of timely reporting.
- Encouraging open communication to foster a culture of open communication within their teams, where employees feel comfortable reporting suspicious activity without fear of repercussions.
- Incident reporting facilitation with assisting team members in utilizing the established reporting channels (email, helpdesk ticket, phone hotline) to report potential security incidents promptly.

IT Security:

- Develop and maintain the incident response playbook in collaboration with relevant stakeholders, including upper management and legal counsel. The plan should be regularly tested and updated to reflect the latest threats and best practices.
- Implement security measures to detect security incidents promptly. Analyze the nature and scope of the incident to determine the best course of action.
- Enact corresponding playbook to prevent further damage. This may involve isolating compromised systems, stopping the spread of malware, and securing sensitive data.
- Lead the recovery process to restore affected systems and data. Document the incident details and report it to the appropriate authorities, as required by law or regulation.

Individual Users:

- Recognize and report any suspicious activity or potential security incidents promptly to the IT Security team following the established reporting procedures.
- Cooperate with the IT security team during an incident response by following established procedures and instructions. This may involve providing information, isolating affected devices, or changing passwords as directed.
- Actively participate in security awareness training to understand their role in identifying and reporting potential security incidents.

c. Policy Statement

This policy is established to ensure a swift and coordinated response to security incidents, minimizing potential damage and ensuring a swift recovery.

1. **Comprehensive Incident Response Plan**: We prioritize the development and maintenance of a clear incident response plan. This plan outlines a structured approach to identifying, containing, eradicating, and recovering from various security threats, with a specific focus on ransomware attacks. By having a predefined response plan, we can effectively mitigate risks and restore normal operations as quickly as possible (NIST, 2021).
2. **Encouraging Timely Reporting:** We recognize the importance of timely reporting of suspicious activity or potential security incidents. We establish a clear and accessible process for employees to report any concerns they may have. By

encouraging early reporting, we can identify potential threats before they escalate into major incidents.

3. **Continuous Improvement:** The effectiveness of our incident response plan is paramount. We will regularly test and update the plan to ensure its ongoing effectiveness in addressing evolving security threats. This ensures we remain prepared to handle a wide range of security incidents efficiently.

d. Procedures and Guidelines

- **Define multiple reporting channels**:
  - **Email:** A dedicated email address for reporting incidents (e.g., [email address removed]).
  - **Helpdesk Ticket:** A designated ticket category for security incidents within the existing helpdesk system.
  - **Phone Hotline:** A designated phone number for urgent security concerns.

- **Standardized Reporting Form:** Develop a simple form that users can use to report incidents, capturing essential details like:
  - Date and time of the observed activity.
  - A brief description of the suspicious event.
  - Any relevant screenshots or logs (if possible).

- **Confidentiality:** Assure employees that reported incidents will be treated confidentially and that they won't face repercussions for reporting in good faith.

e. Compliance and Consequences

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Violations may also lead to the suspension or revocation of user access privileges.
- The organization reserves the right to take legal action against any individual or group engaging in unauthorized access attempts or malicious activities.
- Non-compliance with Payment Card Industry Data Security Standard (PCI DSS, 2018) can result in fines, reputational damage, and potential loss of business with card networks.

- Non-compliance with Personal Information Protection and Electronic Documents Act (PIPEDA, 2018), can launch an investigation by the Office of the Privacy Commissioner (OPC) resulting in a possibilities of several things such as; Recommendations and Corrective Action Plans, Publication of Public Reports, and/or Financial Penalties.

f. Revision History

Policy	Last Revision	Next Revision
IRAR Policy 1.0	13/9/2024	13/4/2025

g. References

Special Publication 800-61. National Institute of Standards and Technology, NIST, Published: April 2021.
https://www.nist.gov/privacy-framework/nist-sp-800-61

Payment Card Industry Data Security Standard (PCI DSS), Reference Guide, v3.2.1, July 2018
https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Personal Information Protection and Electronic Documents Act (PIPEDA), Legislation and Regulations, Modified: January 2018
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

h. Definitions

Incident response plan (IRP): Is a step-by-step guide for your organization to follow in case of a security incident. It's like a fire drill for IT security!

Potential security incidents: A potential security incident refers to any event or activity that could be a violation of the organization's security policies and might pose a threat to its assets (data, systems, etc.). Even if the exact nature of the threat is unclear, it's crucial to report these situations for further investigation.

Examples might include:

- ○ Receiving unexpected phishing emails.
- ○ Observing unusual system behavior (e.g., slow performance, unexpected pop-ups).
- ○ Witnessing unauthorized access attempts (e.g., failed login attempts).

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS mandates specific access control requirements for organizations that store, process, or transmit cardholder data. These controls aim to ensure that only authorized personnel have access to cardholder data and that such access is monitored and logged.

Personal Information Protection and Electronic Documents Act (PIPEDA): Is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of their commercial activity. It mandates that organizations implement safeguards to protect personal information, and strong access controls are a key element of such safeguards.

i. Approval and Review Process

Rex Lee is in charge of approval and setting a regular review schedule.

j. Effective Date

13/3/2024

k. Contact Information

Karen Tire - Head of Human Resources

Phone: 999-999-9999

Email: *karen_tire@CTI.com*