Medical Society of Prince Edward Island (MSPEI) Playbook

Table of Contents

Medical Society of Prince Edward Island (MSPEI) Data Breach Response Policy Report

Table of Contents

Introduction:

This incident playbook report presents a comprehensive framework tailored for the Medical Society of Prince Edward Island (MSPEI) to effectively address security breaches and ensure the protection of sensitive data. In today's digital landscape, the risk of unauthorized access to confidential information poses a significant threat to organizations. Therefore, MSPEI recognizes the critical importance of having robust incident response procedures in place.

Purpose:

The purpose of this incident playbook is to establish a structured and effective framework for responding to security breaches within the Medical Society of Prince Edward Island (MSPEI). By implementing this playbook, MSPEI aims to enhance its ability to detect, contain, and mitigate the impact of security incidents, safeguarding the confidentiality, integrity, and availability of sensitive data.

Additionally, the playbook seeks to clearly define the roles and responsibilities of key stakeholders involved in the incident response process, ensuring a coordinated and efficient response. Moreover, it aims to maintain trust and confidence among MSPEI members, stakeholders, and the broader community, while also ensuring compliance with regulatory requirements and best practices in incident response.

Assuming the scenario:

In the context of a data breach incident at MSPEI, a unique scenario could involve a sophisticated cyberattack targeting the organization's internal systems and sensitive data. For instance, malicious actors could exploit vulnerabilities in MSPEI's network infrastructure to gain unauthorized access to confidential medical records and sensitive information. This could potentially compromise the privacy and security of MSPEI's members, including physicians, retired physicians, and medical learners in Prince Edward Island.

In such a scenario, the incident response team at MSPEI would need to promptly detect and respond to the security breach to minimize the impact on affected systems and stakeholders. Technical remediation efforts would involve isolating affected systems, removing malicious software, and implementing enhanced security measures to prevent further unauthorized access. Additionally, a comprehensive review of security awareness training programs would be necessary to educate employees about the evolving threats and best practices for safeguarding sensitive data.

Furthermore, MSPEI would need to enhance its email security measures and implement stricter access controls to prevent similar incidents in the future. This could include deploying advanced email filtering solutions to detect and block phishing attempts, as well as enforcing multi-factor authentication and encryption protocols to secure sensitive communications and data transmission.

Overall, the incident response playbook for MSPEI would prioritize proactive measures to prevent, detect, and respond to data breaches effectively, ensuring the confidentiality, integrity, and availability of sensitive information and maintaining trust among stakeholders.

Scope:

The scope of this incident playbook encompasses the response framework for security breaches within the Medical Society of Prince Edward Island (MSPEI). It addresses incidents involving unauthorized access to sensitive data across MSPEI's infrastructure. The playbook delineates procedures for incident detection, assessment, and response while defining the roles and responsibilities of both internal and external stakeholders.

Additionally, it outlines communication protocols, measurable metrics for assessing response effectiveness, and supportive policies. The playbook also emphasizes the importance of periodic testing and re-evaluation to ensure continued relevance and efficacy. By establishing this scope, MSPEI aims to bolster its cybersecurity defenses and protect the confidentiality, integrity, and availability of sensitive data.

Users:

The users of the Incident Response Playbook at MSPEI are the individuals or groups responsible for implementing and overseeing incident response activities within the organization. This includes the Incident Response Team (IRT), consisting of the Incident Response Lead, IT Security Specialist, Legal Counsel, Communications Manager, and other relevant stakeholders involved in incident management. By identifying the users, MSPEI ensures that the playbook is aligned with the roles and responsibilities of its intended audience.

The primary users of this playbook include the Incident Response Team (IRT), comprising !Dr. John Smith (CIO), !Sarah Jones, (Legal Counsel), !Emily White (Communications Manager), and !Dr. Michael Brown (Chief Executive Officer), who are responsible for coordinating incident response efforts and ensuring effective communication and collaboration across the organization.

Organization Information:

- **Organization Name:** Medical Society of Prince Edward Island (MSPEI)
- **Representation**: Represents approximately 400 physicians, retired physicians, and medical learners in PEI.

- **Established**: 1855
- **Affiliation**: Division of the Canadian Medical Association.

Internal Stakeholders:

- **Chief Executive Officer (CEO):** Dr. John Smith!
- **Legal Counsel:** Sarah Jones!
- **Communications Manager:** Emily White!

External Stakeholders:

- **Health PEI:** Responsible for physician recruitment and patient registry management.!
- **College of Physicians and Surgeons of Prince Edward Island**: Regulates and licenses physicians, handles complaints.!

Roles and Responsibilities:

Senior Management:

Role: Senior management, including CEO Dr. Michael Brown and CIO Dr. John Smith, provides overall leadership and direction for the incident response process.

Responsibilities:

- Approve the Incident Response Playbook and associated policies.
- Allocate resources and support for incident response activities.
- Review and endorse incident response strategies and decisions.
- Monitor the effectiveness of incident response efforts and ensure compliance with organizational objectives.

Incident Response Team (IRT):

Role: The Incident Response Team, led by the Incident Response Lead, is responsible for executing the incident response process and implementing response strategies.

Responsibilities:

- Identify, assess, and respond to security incidents affecting MSPEI's information systems and assets.
- Develop incident response plans and recommend appropriate actions and countermeasures.
- Implement and monitor incident response efforts, including containment and recovery actions.
- Report regularly to senior management on incident status, trends, and effectiveness of response measures.

Department Heads:

Role: Department heads, such as heads of IT, operations, and communications, are responsible for managing incidents within their respective departments.

Responsibilities:

- Identify department-specific incidents and vulnerabilities.
- Implement controls and measures to contain and mitigate identified incidents.
- Ensure compliance with incident response policies and procedures.
- Report significant incidents and breaches to the Incident Response Team and senior management.

Employees:

Role: All employees, including technical staff, support staff, and management, play a crucial role in identifying and reporting security incidents within their areas of responsibility.

Responsibilities:

- Identify and report potential security incidents, breaches, and vulnerabilities.
- Adhere to organizational policies and procedures related to incident response and information security.
- Participate in training and awareness programs to enhance understanding of security incidents and response procedures.
- Collaborate with the Incident Response Team to implement and maintain effective incident response measures.

Incident Overview:

- **Incident Name:** Security Breach Incident
- **Incident Type:** Unauthorized Access

- **Impact Assessment:**
  - Confidentiality Effect: High
  - Integrity Effect: High
  - Availability Effect: High

Incident Severity Matrix:

The severity levels could be categorized as Low, Medium, High, and Critical. The criteria for each severity level would be based on factors such as the impact on confidentiality, integrity, and availability of data, the extent of disruption to business operations, potential financial losses, regulatory compliance implications, and the level of reputational damage.

For example, a Low Severity incident might involve a minor security breach with limited impact on data integrity or availability, resulting in minimal disruption to operations. A Medium Severity incident could encompass a more significant breach affecting multiple systems or compromising sensitive data, resulting in moderate disruption to operations and potential financial losses.

A High Severity incident might involve a major data breach or cyberattack with widespread impact on data confidentiality, integrity, and availability, leading to significant disruption to operations, financial losses, and regulatory compliance implications. A Critical Severity incident would represent a severe cyber incident or data breach posing an imminent threat to the organization's operations, reputation, or financial stability, requiring an emergency response to contain and mitigate the threat effectively.

Escalation criteria would define when incidents should be escalated to higher severity levels based on changes in the incident's impact, scope, or criticality. This ensures that the response effort is proportional to the severity of the incident and allows for timely escalation and allocation of resources to address emerging threats effectively.

Severity Level	Criteria
Low	Limited impact on data confidentiality, integrity, and availability. Minimal disruption to operations. Negligible financial losses. Low regulatory compliance implications
Medium	Moderate impact on data confidentiality, integrity, and availability. Significant disruption to operations. Moderate financial losses. Moderate regulatory compliance implications
High	Significant impact on data confidentiality, integrity, and availability. Major disruption to operations. Significant financial losses. High regulatory compliance implications
Critical	Severe impact on data confidentiality, integrity, and availability. Critical disruption to operations. Severe financial losses. Imminent regulatory compliance implications

This table outlines the criteria for each severity level, helping to categorize incidents based on their impact, scope, and criticality, and guiding the escalation process during incident response.

Incident Details:

- **Nature of Incident:** Security breach resulting in unauthorized access to sensitive data.
- **Affected Systems:** Member database, financial records, communications systems.
- **Detection Method:** Intrusion detection system alerts.

Incident Response Playbook:

In the incident response playbook tailored for MSPEI, the incident response overview outlines a structured approach for detecting, assessing, and responding to security incidents effectively. It encompasses key phases including preparation, identification, containment, eradication, recovery, and

lessons learned. The playbook is designed to ensure a coordinated and efficient response, aiming to minimize disruption to operations and mitigate the impact of security breaches on MSPEI's stakeholders.

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

Fig: Incident Response Phases

Preparation:

- In this phase, MSPEI ensures that all incident response team members, including the Incident Response Lead, IT Security Specialist, and Communications Manager, are trained and aware of their roles and responsibilities.
- Contact information for key stakeholders and external resources, such as the SOC and legal counsel, is validated and updated.
- The availability and functionality of incident response tools and resources, such as monitoring systems and communication channels, are reviewed and verified.
- Communication channels and protocols for reporting and escalating security incidents are established to ensure timely and effective communication during the incident response process.

Identification:

- During this phase, MSPEI monitors security alerts and logs for indicators of compromise (IoCs) or suspicious activities on its network and systems.
- The Incident Response Team, led by the Incident Response Lead and supported by the IT Security Specialist, conducts initial triage to determine the nature and scope of the security incident.
- Relevant information, such as timestamps, affected systems, and potential impact, is gathered to classify the incident based on severity and criticality.
- The incident is thoroughly assessed to understand the extent of the breach and its potential impact on MSPEI's operations and stakeholders.

Containment:

- In this phase, MSPEI takes immediate action to isolate affected systems or networks to prevent further spread of the data breach.
- Predefined escalation procedures based on severity and impact assessment are followed to ensure a swift and effective response.
- Access controls or temporary measures are implemented to limit the impact of the incident on MSPEI's operations.
- Evidence and logs are preserved for forensic analysis and investigation to identify the source of compromise and contain the breach effectively

Eradication:

- During the eradication phase, MSPEI investigates the root cause of the data breach to identify the source of compromise.
- Efforts are made to remove or neutralize malicious presence within the environment, working closely with the Incident Response Team and external resources such as the SOC.
- Remediation measures, including patching vulnerabilities and applying updates recommended by security experts, are implemented to enhance the organization's security posture and resilience against similar incidents in the future.

Recovery:

- The recovery phase focuses on restoring affected systems and services to normal operations following successful eradication of the data breach.
- Coordination with IT teams, external consultants, and stakeholders is crucial to ensure a smooth recovery process.
- Data integrity is verified, and backups are restored if necessary to recover lost or corrupted data.

- Progress and expected timelines for restoration efforts are communicated transparently to stakeholders, including MSPEI's management team and regulatory bodies, to minimize disruption and maintain trust among stakeholders.

Lessons Learned:

- After the incident has been resolved and operations have returned to normal, MSPEI conducts a comprehensive post-incident review to extract valuable insights and lessons learned from the data breach incident.
- The Incident Response Team, along with key stakeholders and external consultants, participates in the review process to assess the effectiveness of the response efforts.

Trigger Items Affecting Incident Response Flow:

- **Anomalous Network Activity:** Detection of unusual or suspicious network activity, such as unauthorized access attempts, unusual data transfers, or unusual login patterns, may trigger an investigation into a potential data breach.
- **Intrusion Detection System Alerts:** Alerts generated by intrusion detection systems (IDS) or intrusion prevention systems (IPS) indicating potential security breaches or suspicious activities on the network could signal the need for immediate investigation and response.
- **Unusual Login Attempts:** A sudden increase in failed login attempts or unauthorized access to sensitive systems or databases may indicate a potential security breach and trigger the initiation of incident response procedures.
- **Data Exfiltration Indicators:** Detection of data exfiltration indicators, such as large volumes of data being transferred to external locations or unauthorized access to confidential files, may indicate a data breach and prompt immediate action to contain the incident.
- **Reports from External Sources:** Reports or notifications from external sources, such as security researchers, law enforcement agencies, or regulatory bodies, regarding suspicious activities or potential security incidents involving MSPEI's systems or data may trigger an investigation and response by the incident response team.

Escalations:

- **Escalation Trigger 1:** Significant increase in compromised systems beyond initial assessment.
  - **Who might the escalation go to:** Incident Response Lead, CIO
  - **Reasoning:** Top-level management needs to be informed to allocate additional resources if needed.
- **Escalation Trigger 2:** Evidence of data exfiltration.
  - **Who might the escalation go to:** Legal Counsel, Communications Manager
  - **Reasoning:** Legal implications and communication strategy need to be addressed promptly.
- **Escalation Trigger 3:** Failure of initial containment measures.
  - **Who might the escalation go to:** Incident Response Lead, IT Security Specialist
  - **Reasoning:** Immediate action is necessary to prevent further damage.
- **Escalation Trigger 4:** Persistent attempts of unauthorized access despite initial mitigation efforts.
  - **Who might the escalation go to:** Executive Director, Regulatory Bodies
  - **Reasoning:** Decision-makers and regulatory bodies should be informed of ongoing risks and potential compliance issues.
- **Escalation Trigger 5:** Discovery of insider involvement in the breach.
  - **Who might the escalation go to:** Legal Counsel, Human Resources
  - **Reasoning:** Legal and HR departments need to address legal implications and initiate internal investigations.

Stakeholder Communication:

- **MSPEI Members:**
  - Information to be communicated: Notification of the breach, steps taken to mitigate impact, guidance on protective measures.
  - Reasoning: Members need to be informed to take necessary precautions to protect themselves and their data.
- **Health PEI:**
  - Information to be communicated: Notification of breach, assistance required in containing incident.
  - Reasoning: Health PEI needs to be informed to collaborate in containing the breach and ensuring patient data security.
- **College of Physicians and Surgeons of PEI:**
  - Information to be communicated: Reporting of incident details, cooperation in investigation.
  - Reasoning: Regulatory body responsible for overseeing medical practitioners needs to be informed for compliance purposes and potential disciplinary actions.
- **Media/Press:**

- Information to be communicated: Managed by Communications Manager, providing accurate information to maintain public trust.
- Reasoning: Transparency with the media is crucial to maintain public trust and credibility.

- **Regulatory Bodies:**
  - Information to be communicated: Compliance reports as required.
  - Reasoning: Regulatory bodies need to be informed to ensure compliance with regulations and guidelines, and to report any breaches as required by law.

Frequency of Testing and Re-evaluation:

- The playbook will be tested annually and updated as needed or after significant changes in infrastructure or regulations.

Flow chart:

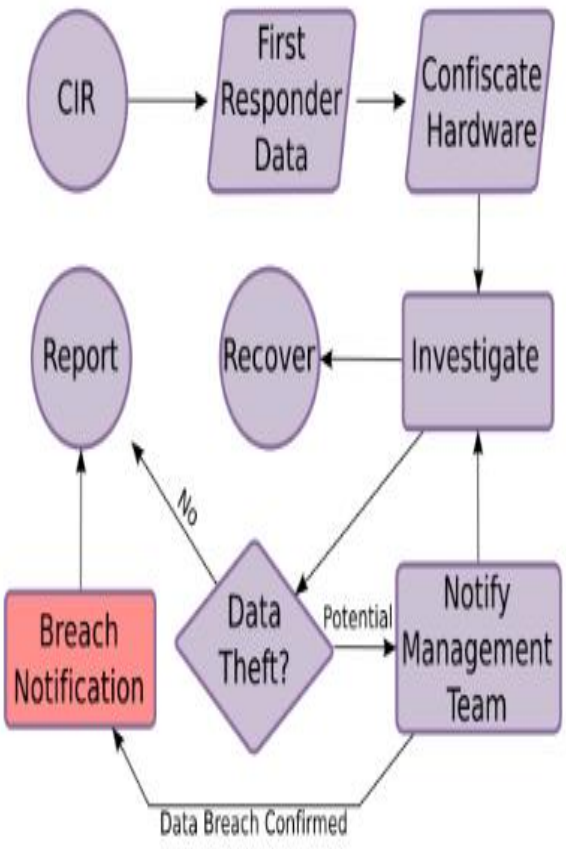

Fig: Flowchart representation

Conclusion:

By implementing this incident playbook, MSPEI aims to effectively respond to security breaches, protect sensitive data, and maintain trust among stakeholders. It is imperative for the organization to continuously review and update its incident response procedures to adapt to evolving threats and regulatory requirements. Regular training and simulation exercises should also be conducted to ensure readiness and effectiveness in responding to incidents. With a comprehensive and proactive approach to incident management, MSPEI strives to uphold its commitment to the security and integrity of its operations and the trust of its members and stakeholders.

Medical Society of Prince Edward Island (MSPEI) Data Breach Response Policy Report

Purpose:

The purpose of this policy is to establish the goals and vision for the breach response process within the Medical Society of Prince Edward Island (MSPEI). It defines the circumstances under which the policy applies, staff roles and responsibilities, standards, and metrics for incident response. The policy aims to focus significant attention on data security breaches and outlines how MSPEI's established culture of openness, trust, and integrity should respond to such incidents. It is intended to protect MSPEI's employees, partners, and data from illegal or damaging actions by individuals, knowingly or unknowingly.

Background:

This policy mandates that any individual suspecting a theft, breach, or exposure of MSPEI Protected data must immediately report it via email to Helpdesk@MSPEI.org(**giving random email**), by calling [!999 999 9999(**giving some random number**)], or through the help desk reporting web page at http://MSPEI.org. The Information Security Administrator will investigate all reported incidents to confirm if a breach has occurred and initiate appropriate procedures if necessary.

Scope:

This policy applies to all individuals who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or handle personally identifiable information or Protected Health Information (PHI) of MSPEI members. Any agreements with vendors will also contain language protecting MSPEI's data.

1. Policy Confirmed Theft, Data Breach, or Exposure of MSPEI Data:

As soon as a theft, data breach, or exposure containing MSPEI protected data is identified, the process of removing all access to that resource will begin. The Executive Director will chair an incident response team to handle the breach or exposure. The team will include members from IT Infrastructure, IT Applications, Legal, Communications, Member Services (if Member data is affected), Human Resources, and the affected unit or department. Additionally, other departments and individuals may be involved based on the data type.

The Executive Director will be notified of the theft, breach, or exposure. IT, along with the designated forensic team, will analyze the breach to determine the root cause. Forensic investigators provided by MSPEI's cyber insurance will also analyze the breach to determine its cause and impact.

Roles and responsibilities include Sponsors, Information Security Administrator, Users, and the Incident Response Team. The Incident Response Team will be chaired by Executive Management and will include representatives from various departments to manage the incident effectively.

Enforcement Personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Third-party partner companies found in violation may have their network connection terminated.

Data retention periods will be defined based on legal, regulatory, and business requirements. Upon expiration of retention periods, data will be securely destroyed using approved methods. Procedures for data retention and destruction will be documented and communicated to relevant personnel.

Logs, both normal and those involved in security incidents, will be retained for a specified period based on regulatory requirements and organizational needs. Logs will be securely stored and accessible only to authorized personnel for monitoring, analysis, and investigation purposes.

1.a. Policy 1: User Information Capture Policy:

Policy Statement : MSPEI shall implement policies and procedures to govern the capture of user information through Packet Capture or other network monitoring methods. Any collection of user information shall be conducted in compliance with relevant laws and regulations, and with due consideration for user privacy and data security.

Policy Details : This policy applies to all MSPEI personnel involved in the capture of user information through Packet Capture or other network monitoring activities.

Responsibilities : The IT Security Specialist shall oversee the implementation of this policy and ensure compliance with applicable laws and regulations. All personnel involved in network monitoring activities shall adhere to the procedures outlined in this policy.

Procedures :

Prior Authorization : Before capturing any user information, personnel must obtain proper authorization from the IT Security Specialist or designated authority.

Data Minimization : Only collect user information necessary for legitimate business purposes. Avoid capturing sensitive or unnecessary data.

Encryption : Ensure that any captured user information is encrypted during transmission and storage to protect against unauthorized access.

Access Control : Limit access to captured user information to authorized personnel only. Implement appropriate access controls and authentication mechanisms.

Retention Period : Define a clear retention period for captured user information. Dispose of data promptly once it is no longer needed for its intended purpose.

Consequences of Non-Compliance : Failure to comply with this policy may result in disciplinary action, including but not limited to reprimand, suspension, or termination of employment. Additionally, non-compliance may expose MSPEI to legal and regulatory risks, including fines, penalties, and damage to reputation.

Policy Review : This policy shall be reviewed annually by the IT Security Specialist to ensure its effectiveness and relevance. Any updates or revisions to the policy shall be communicated to all relevant personnel in a timely manner.

Policy Approval : This policy is approved by [!Dr. Michael Brown] and is effective as of [04-11-2024].

1.b. Policy 2: Personally Identifiable Information (PII) Access and Dissemination policy:

Policy Statement : MSPEI shall establish policies and procedures to govern the access, handling, and dissemination of Personally Identifiable Information (PII) to ensure compliance with applicable laws and regulations, safeguard user privacy, and mitigate the risk of unauthorized disclosure or misuse of sensitive information.

Policy Details : This policy applies to all MSPEI personnel who access, handle, or disseminate PII in the course of their duties.

Responsibilities : The Chief Information Officer (CIO) shall oversee the implementation of this policy and ensure its alignment with relevant laws and regulations. All personnel with access to PII shall receive training on data handling procedures and their responsibilities under this policy.

Procedures :

Access Control: Limit access to PII to authorized personnel only, based on the principle of least privilege. Implement role-based access controls and authentication mechanisms to ensure that only authorized individuals can access sensitive information.

Data Handling : Personnel shall handle PII with care and discretion, ensuring that it is not disclosed or disseminated inappropriately. PII should only be accessed or used for legitimate business purposes and in accordance with applicable laws and regulations.

Dissemination Controls : When disseminating PII, personnel must ensure that it is securely transmitted and shared only with authorized recipients. Implement encryption and secure communication channels to protect PII from unauthorized access or interception.

Reporting Requirements : Personnel shall promptly report any unauthorized access, disclosure, or misuse of PII to the designated authority, such as the IT Security Specialist or Data Protection Officer.

Consequences of Non-Compliance : Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Additionally, non-compliance may expose MSPEI to legal and regulatory risks, including fines, penalties, and damage to reputation.

Policy Review : This policy shall be reviewed annually by the CIO to ensure its effectiveness and alignment with changing legal and regulatory requirements. Any updates or revisions to the policy shall be communicated to all relevant personnel in a timely manner.

Policy Approval : This policy is approved by [!Dr. Michael Brown] and is effective as of [04-11-2024].

1.c. Policy 3: Handling of Information Classified as Red in the TLP:

Policy Statement : MSPEI shall establish policies and procedures for the handling and communication of information classified as RED in the Traffic Light Protocol (TLP) to ensure appropriate safeguarding of sensitive information and protection against unauthorized disclosure.

Policy Details : This policy applies to all MSPEI personnel who handle, transmit, or communicate information classified as RED in the TLP.

Responsibilities : The Incident Response Lead shall oversee the implementation of this policy and ensure compliance with TLP guidelines. All personnel involved in incident response, communication, and information sharing shall be trained on TLP classification and handling procedures

Procedures :

TLP Classification : Information shall be classified according to the TLP guidelines, with RED indicating information that should be handled with the highest level of sensitivity and restricted to authorized recipients only.

Access Control : Limit access to RED information to individuals with a legitimate need-to-know, based on their role and responsibilities. Implement strict access controls and authentication mechanisms to prevent unauthorized access.

Communication Protocols : When communicating RED information, personnel must adhere to TLP guidelines and ensure that it is shared only with authorized recipients who have been briefed on the sensitivity of the information.

Encryption : RED information shall be encrypted during transmission and storage to protect against unauthorized interception or disclosure.

Consequences of Non-Compliance : Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Additionally, non-compliance may jeopardize the confidentiality of sensitive information and expose MSPEI to legal and regulatory risks.

Policy Review : This policy shall be reviewed annually by the Incident Response Lead to ensure its effectiveness and alignment with TLP guidelines. Any updates or revisions to the policy shall be communicated to all relevant personnel in a timely manner.

Policy Approval : This policy is approved by [!Dr. Michael Brown] and is effective as of [04-11-2024].

1.d. Policy 4: Data Retention and Destruction Policy:

Policy Statement : MSPEI shall establish policies and procedures for the retention and destruction of data to ensure compliance with legal and regulatory requirements, protect sensitive information, and minimize the risk of data breaches.

Policy Details : This policy applies to all data held or processed by MSPEI, including electronic and physical records, regardless of format or location.

Responsibilities : The Data Protection Officer (DPO) shall oversee the implementation of this policy and ensure compliance with applicable laws and regulations. All personnel responsible for data management and storage shall be trained on data retention and destruction procedures.

Procedures :

Data Classification : Classify data based on its sensitivity and regulatory requirements to determine appropriate retention periods and disposal methods.

Retention Periods : Establish retention periods for different types of data based on legal, regulatory, and business requirements. Periodically review and update retention schedules to ensure compliance with changing regulations and business needs.

Secure Storage : Store data securely during the retention period, using encryption and access controls to prevent unauthorized access or disclosure.

Destruction Methods : Implement secure methods for data destruction, including shredding, degaussing, or secure deletion of electronic records. Ensure that destruction processes are documented and auditable.

Consequences of Non-Compliance : Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Additionally, non-compliance may lead to legal and regulatory sanctions, including fines and penalties for data breaches or non-compliance with retention requirements.

Policy Review : This policy shall be reviewed annually by the Data Protection Officer to ensure its effectiveness and alignment with legal and regulatory requirements. Any updates or revisions to the policy shall be communicated to all relevant personnel in a timely manner.

Policy Approval : This policy is approved by [!Dr. Michael Brown] and is effective as of [04-11-2024].

1.e. Policy 5: Log Retention Policy:

Policy Statement : MSPEI shall establish and maintain policies and procedures for the retention of logs, including both normal operational logs and those logs involved in security incidents. These policies aim to ensure the availability of log data for operational, investigative, and regulatory purposes while minimizing the risk of unauthorized access or disclosure.

Policy Details : This policy applies to all log data generated by our organization's systems, networks, and applications, including but not limited to access logs, security logs, event logs, and audit trails.

Responsibilities : The IT Security team shall be responsible for overseeing the implementation of this policy and ensuring compliance with its provisions. All personnel involved in log management, including system administrators and security analysts, shall be trained on the procedures outlined in this policy.

Procedures :

Log Classification : Logs shall be classified based on their sensitivity and relevance to operational and security requirements.

Retention Periods : Our organization shall establish retention periods for different categories of logs, taking into account legal, regulatory, and operational considerations. Normal operational logs may have shorter retention periods, while logs involved in security incidents may be retained for longer periods for investigative and forensic purposes.

Secure Storage : Log data shall be stored securely to prevent unauthorized access, tampering, or deletion. Access controls and encryption mechanisms shall be implemented to protect log data from unauthorized disclosure.

Review Logs : Logs shall be regularly reviewed and analyzed for security incidents, anomalies, or compliance violations. Retained logs shall be periodically audited to ensure their integrity and completeness.

Consequences of Non-Compliance : Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Additionally, non-compliance may lead to legal and regulatory consequences, including fines and penalties for data breaches or non-compliance with log retention requirements.

Policy Review : This policy shall be subject to annual review by the IT Security team to ensure its effectiveness and alignment with legal and regulatory requirements. Any updates or revisions to the policy shall be communicated to all relevant personnel in a timely manner.

Policy Approval : This policy is approved by [!Dr. Michael Brown] and is effective as of [04-11-2024].

Link for PPT:

https://docs.google.com/presentation/d/1Fnr-Du79J4nSUE7nEEyCs6DpVPffviFk/edit?usp=sharing&ouid=111996183170088279081&rtpof=true&sd=true

Conclusion:

In conclusion, the implementation of these five policies is essential for ensuring the security and integrity of MSPEI's data and information systems. By establishing clear guidelines and procedures for capturing user information, accessing personally identifiable information (PII), handling sensitive information, communicating highly sensitive data, retaining data, and managing log retention, MSPEI can enhance its overall security posture and mitigate the risk of data breaches or unauthorized access.

These policies provide a framework for safeguarding MSPEI's data assets, protecting the privacy of its members, and maintaining compliance with regulatory requirements. They outline the responsibilities of personnel involved in data handling and management and establish consequences for non-compliance, thereby promoting accountability and adherence to best practices in information security.

By regularly reviewing and updating these policies to reflect changes in technology, regulations, and organizational requirements, MSPEI can adapt to evolving threats and challenges in the cybersecurity landscape. Additionally, ongoing training and awareness initiatives will ensure that all employees are equipped with the knowledge and skills necessary to uphold these policies effectively.

Overall, the adoption of these policies demonstrates MSPEI's commitment to data protection, privacy, and regulatory compliance, fostering trust and confidence among its members, partners, and stakeholders.

References:

OpenAI. (n.d.). ChatGPT . Retrieved from- https://openai.com/chatgpt

NIST Incident Response Plan: Process, Templates, and Examples - https://www.cynet.com/incident-response/nist-incident-response/

How to Respond to a Data Breach + Policy Template - https://reciprocity.com/how-to-respond-to-a-data-breach-policy-template/

Information Security Incident & Breach Handling Procedure - https://www.alaska.edu/oit/policies-standards/information-security/

Incident Response Playbook Template - https://github.com/aws-samples/aws-incident-response-playbooks/blob/master/playbooks/IRP-PersonalDataBreach.md

IACS Cyber Security Incident Response Playbook - https://s3.ca-central-1.amazonaws.com/medias.bba.ca/documents/pdf/BBA_Cybersecurity_final7.pdf

Develop an Incident Response Plan: Fillable template and example - https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example

Federal Government Cybersecurity Incident & Vulnerability Response Playbooks - https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Data Protection Policy - https://easylegaldocs.com/templates/policies/data-protection-policy/

How to Write a Policy for Your Business and Employees - https://www.sweetprocess.com/how-to-write-a-policy/#:%7E:text=A%20policy%20is%20simply%20a,is%20your%20organization's%20action%20plan

Traffic Light Protocol - https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

MSPEI- https://www.mspei.org/

Mastering Log Retention Policy: A guide to Securing Your data - https://cribl.io/blog/mastering-log-retention-policy-a-guide-to-securing-your-data/

Data Retention Policy 101: Best Practices, Examples & More [with Template] - https://www.intradyn.com/data-retention-policy/

Responding to a Company-Wide PII Data Breach - https://www.cbiz.com/insights/articles/article-details/responding-to-a-company-wide-pii-data-breach-article