**Louis D Brown Peace Institute Incident Response Plan**

**Document Control**

**Document Title:** Louis D Brown Peace Institute

Incident Response Plan  
 **Document Version:** 1.0  
 **Effective Date:** TBD  
 **Review Date:** TBD  
 **Document Owner:** Anthony Johnson  
 **Approval:**

**Table of Contents**

* **Introduction**
  + 1.1 Purpose
  + 1.2 Scope
  + 1.3 Objectives
* **Incident Response Team**
  + 2.1 Formation
  + 2.2 Roles and Responsibilities
  + 2.3 Contact Information
* **Incident Identification**
  + 3.1 Detection Methods
  + 3.2 Reporting Procedures
  + 3.3 Incident Categories
* **Incident Handling**
  + 4.1 Triage and Initial Assessment
  + 4.2 Incident Containment
  + 4.3 Eradication and Recovery
  + 4.4 Communication Procedures
* **Post-Incident Activity**
  + 5.1 Lessons Learned
  + 5.2 Documentation and Reporting
  + 5.3 Continuous Improvement
* **Training and Awareness**
  + 6.1 Team Training
  + 6.2 Awareness Programs
* **Tools and Resources**
  + 7.1 Incident Response Tools
  + 7.2 External Resources
* **Review and Update**
  + 8.1 Regular Review
  + 8.2 Plan Update Procedures

**1. Introduction**

**1.1 Purpose**

The purpose of this Incident Response Plan is to provide a structured approach for effectively responding to and mitigating security incidents within Louis D Brown Peace Institute.

**1.2 Scope**

This plan covers all information systems, networks, and data owned, operated, or supported by the Louis D Brown Peace Institute.

**1.3 Objectives**

* Minimize the impact of security incidents on Louis D Brown Peace Institute's operations.
* Ensure a consistent and coordinated response to incidents.
* Enhance the organization's ability to detect, respond to, and recover from security incidents.

**2. Incident Response Team**

**2.1 Formation**

The Incident Response Team (IRT) is composed of Winston Commock and Mario Rodrigues. The team will be activated in the event of a security incident.

**2.2 Roles and Responsibilities**

* **Incident Coordinator:** Mario Rodrigues
* **Investigator/Analyst:** Winston Commock
* **Communications Coordinator:** Mario Rodrigues
* **Technical Support:** Winston Commock

**2.3 Contact Information**

* Incident Coordinator: email: [mario@ldbpeaceinstitute.org](mailto:mario@ldbpeaceinstitute.org) PN: 781-261-1732
* Investigator/Analyst: Email:[winston@ldbpeaceinstitute.org](mailto:winston@ldbpeaceinstitute.org) PN: 857-990-8801
* Communications Coordinator: [mario@ldbpeaceinstitute.org](mailto:mario@ldbpeaceinstitute.org) PN: 781-261-1732
* Technical Support: Email:[winston@ldbpeaceinstitute.org](mailto:winston@ldbpeaceinstitute.org) PN: 857-990-8801

**3. Incident Identification ( detection and analysis phase)**

**3.1 Detection Methods**

* Firewall
* Antivirus Software
* Security Information and Event Management(SIEM)
* Threat Intelligence Feeds
* Vulnerability Scanning
* Email Filtering and Anti-Phishing Solutions
* General user

**3.2 Reporting Procedures**

**Law Enforcement Notification:**

* If the cyber attack involves illegal activities, consider notifying law enforcement agencies.
* Provide them with relevant information and cooperate with their investigation.

**Regulatory Reporting:**

* If your organization is subject to data protection regulations, report the incident to the relevant regulatory authorities as required by law.

**Customer Notification**:

* If customer data is compromised, consider notifying affected individuals in accordance with data breach notification laws.
* Provide guidance on protective measures they can take.

**Post-Incident Analysis:**

* Conduct a thorough post-incident analysis to understand the attack vectors, vulnerabilities exploited, and areas for improvement.
* Update incident response plans based on lessons learned.

**Continuous Monitoring:**

* Implement continuous monitoring for any signs of persistent threats or future attacks.
* Enhance security measures based on the insights gained from the incident

**3.3 Incident Categories**

* Phishing Attacks
* Social engineering
* Malware attacks
* Trojan attacks
* ransomeware attacks
* DDos attacks

**4. Incident Handling**

**4.1 Triage and Initial Assessment**

* Identify the Nature of the Incident:

Determine the type of incident, whether it's a malware infection, a data breach, a denial-of-service attack, or another form of cyber threat.

* Gather Information:

Collect relevant information about the incident, such as the affected systems, the attack vector, and any indicators of compromise. This information will aid in the eradication process.

* Perform Forensic Analysis:

Conduct a forensic analysis to understand the extent of the compromise, identify the entry point, and gather evidence that may be useful for legal or regulatory purposes

**4.2 Incident Containment**

* Isolate and Contain:

Immediately isolate the affected systems from the network to prevent the incident from spreading. Implement containment measures to stop the ongoing impact.

**4.3 Eradication and Recovery**

* Eradicate Malicious Code and Artifacts:

Use antivirus software, malware removal tools, and manual inspection to identify and remove malicious code from affected systems. Ensure that all remnants of the malware are eradicated.

* Patch and Update Systems:

Identify and patch any vulnerabilities that were exploited during the incident. Keep systems and software up-to-date to prevent future vulnerabilities.

* Change Credentials:

Change passwords and credentials for affected accounts to prevent unauthorized access. Implement strong password policies.

**4.4 Communication Procedures**

* Communicate Internally and Externally:

Communicate the resolution of the incident to internal stakeholders, including employees, and if necessary, external stakeholders such as customers or regulatory authorities.

**5. Post-Incident Activity**

**5.1 Lessons Learned**

* Hold a post-incident review to analyze the incident response process and identify areas for improvement. Document lessons learned to enhance future incident response capabilities.

**5.2 Documentation and Reporting**

* **Incident Ticketing:**

Create a centralized incident ticket for each identified incident.

Include incident details such as date, time, description, and the initial impact assessment.

* **Incident Containment and Eradication:**

**Containment Strategies:**

Document the strategies employed to contain the incident and prevent further damage.

Include details on isolating affected systems and network segments.

**Eradication Steps:**

Outline the steps taken to eradicate malicious elements from the affected systems.

Specify tools and procedures used for malware removal.

* Recovery and System Restoration:

Recovery Plan:

Document the plan for restoring affected systems to normal operation.

Include steps for validating the integrity of restored systems.

Backup and Restore Procedures:

Detail how backup data was used in the recovery process.

Document any challenges or issues encountered during the restoration.

* Communication and Reporting:

Internal Communication:

Document internal communication regarding the incident, including notifications to key stakeholders and updates provided to the incident response team.

External Communication:

Record communication with external parties, such as law enforcement, regulatory bodies, or affected third parties.

Ensure that external communication adheres to legal and regulatory requirements.

Incident Reporting:

Create a comprehensive incident report that includes an executive summary, incident timeline, findings, and recommendations.

Provide technical details for IT and security teams, as well as non-technical summaries for executives.

* Lessons Learned and Post-Incident Review:

Post-Incident Review:

Document the findings and outcomes of the post-incident review.

Include feedback on the effectiveness of the incident response plan and areas for improvement.

Lessons Learned:

Record key lessons learned from the incident, including insights into the organization's strengths and weaknesses in responding to the incident.

* Policy and Procedure Updates:

Policy and Procedure Documentation:

Update incident response policies and procedures based on lessons learned.

Ensure that documentation reflects the most current incident response practices.

* Regulatory Compliance:

Compliance Documentation:

Maintain documentation that demonstrates compliance with applicable laws and regulations.

Include records of any required notifications or reports.

* Training and Awareness:

Training Records:

Document training sessions conducted for incident response team members and other relevant staff.

Keep records of attendees and topics covered.

* Continuous Improvement:

Improvement Plan:

Develop an improvement plan based on the lessons learned and findings from the incident.

Implement changes to enhance incident response capabilities.

**5.3 Continuous Improvement**

* Use the insights gained from the incident to continually improve cybersecurity measures, incident response procedures, and overall security posture.

**6. Training and Awareness**

**6.1 Team Training**

An annual group training where staff is updated on changes to the incident response plan, new methods threat actors use to attempt to breach a company, providing knowledge of different cyber attacks and what to look for, and testing the plan out

**6.2 Awareness Programs**

**Phishing Simulations**

* Simulate phishing attacks to test employees' ability to recognize and avoid phishing emails.
* Provide feedback and additional training for those who fall for simulated phishing attempts

**Security Policies and Procedures:**

* Clearly communicate security policies and procedures to employees, emphasizing the importance of compliance.
* Ensure that everyone understands their role in maintaining a secure work environment.

**Cybersecurity Resources:**

* Provide easily accessible resources such as online articles, videos, and infographics that explain common cyber threats and preventive measures.
* Establish a centralized platform for employees to access relevant information.

**7. Tools and Resources**

**7.1 Incident Response Tools**

* Malware Analysis and Removal Tools

Ex: Malware Analysis Sandbox and Anti-Virus and Anti-Malware Solutions

* Network Traffic Analysis Tools

Ex: Packet Analyzers and Network Security Monitoring (NSM) Tools

* Detection and Analysis Tools:

Ex: SIEM tool , Threat Intelligence Platforms, and IDS (Intrusion Detection System)

Add sources to use

**7.2 External Resources**

Infonet is the third party to be reached out to during All incidents

Law enforcements for ransomware attacks

**8. Review and Update**

**8.1 Regular Review**

* Annual Review:

Conduct a comprehensive review of the entire incident response plan annually. This review should encompass all aspects of the plan, including procedures, contact information, roles and responsibilities, and technology.

* Continuous Monitoring:

Implement continuous monitoring of the threat landscape and organizational changes. If there are significant developments in the threat environment or the organization's structure, consider conducting an out-of-cycle review.

* Post-Incident Reviews:

After each incident, perform a thorough post-incident review. Evaluate how well the incident response plan worked in practice and identify areas for improvement. Use these insights to update the plan promptly.

* Regulatory Compliance Updates:

Stay informed about changes in regulations or compliance requirements that may impact the incident response plan. Update the plan accordingly to ensure ongoing compliance.

**8.2 Plan Update Procedures**

* Significant Changes in the Organization:

Any substantial changes to the organization's structure, IT infrastructure, or business processes may necessitate a review of the incident response plan.

* Technological Changes:

Advances in technology or the adoption of new systems and applications may require updates to the incident response plan to address emerging threats.

* Regulatory Changes

If there are updates to relevant laws, regulations, or compliance requirements, the incident response plan should be reviewed to ensure ongoing compliance.

* Lessons Learned from Incidents

After each incident, conduct a thorough post-incident review. Use the lessons learned to update and improve the incident response plan. This may prompt more frequent reviews if incidents occur frequently.

* Changes in Threat Landscape

The cybersecurity threat landscape is dynamic. Regularly monitor emerging threats and update the incident response plan to address new attack vectors or tactics.

* Personnel Changes:

Changes in key personnel responsible for incident response, or changes in their roles, may require a review and update of the plan to ensure that responsibilities are clearly defined.

* Incident Response Team Training:

As incident response team members gain new skills or if there are changes in team composition, update the plan to reflect the current expertise and roles.