*[Author Name]*

*[Entity Name] | [Entity Address] | [Version Number]*

**Run Book**

**Reporting Brain Computing Interface (BCI) Security Incidents**

This free template has been created to assist professionals in the development of Brain Computing Interface (BCI) run books. It is not required to use the existing format. This document is guidance and should not be legal advice. Please refer to legal counsel for explicit requirements related to your industry. Please copy, change, and revise this document as needed for your purposes. This document is a template created explicitly for a starting point and baseline. Please delete this box and any templated labels before using.

Table of Contents

[1. Purpose 2](#_Toc180003812)

[2. Scope 2](#_Toc180003813)

[3. Incident Categories 2](#_Toc180003814)

[4. Incident Reporting Procedure 2](#_Toc180003815)

[4.1 Initial Detection 2](#_Toc180003816)

[4.2 Notification 2](#_Toc180003817)

[4.3 Incident Report Form 3](#_Toc180003818)

[5. Incident Response Procedure 3](#_Toc180003819)

[5.1 Assessment and Classification 3](#_Toc180003820)

[5.2 Response Coordination 3](#_Toc180003821)

[6. Documentation and Reporting 3](#_Toc180003822)

[6.1 Incident Log 3](#_Toc180003823)

[6.2 Final Report 3](#_Toc180003824)

[6.3 Compliance 4](#_Toc180003825)

[7. Training and Awareness 4](#_Toc180003826)

[7.1 Employee Training 4](#_Toc180003827)

[7.2 Drills and Simulations 4](#_Toc180003828)

[8. Review and Updates 4](#_Toc180003829)

[9. Contact Information 4](#_Toc180003830)

[13. Document History 4](#_Toc180003831)

**Run Book for Brain-Computer Interfaces (BCI)**

**Version:** [Insert Version Number]

**Effective Date:** [Insert Date]

**Approved:** [Insert Name]

This run book is designed to ensure a structured and effective approach to handling BCI security incidents. Adherence to these procedures will help safeguard [Entity Name]’s assets and user well-being.

# 1. Purpose

This run book provides a structured approach for reporting and handling security incidents related to Brain Computing Interfaces (BCIs) at [Entity Name]. The goal is to ensure timely and effective response to incidents to protect company assets, user privacy, and maintain operational integrity.

# 2. Scope

This run book applies to all employees, contractors, and third-party users who utilize BCIs at [Entity Name]. It covers procedures for reporting incidents, assessing impact, and coordinating responses.

# 3. Incident Categories

* **Security Breach:** Unauthorized access or use of BCI data or systems.
* **Malfunction:** Functional issues or system errors impacting BCI performance.
* **Data Leak:** Unintended exposure or loss of sensitive information.
* **Health & Safety Concern:** Physical or psychological effects experienced by users.

# 4. Incident Reporting Procedure

## 4.1 Initial Detection

* **User Action:** If a user detects a potential security incident, they should immediately cease using the BCI and secure any related data.
* **Documentation:** Users should document the incident, including time, date, nature of the issue, and any immediate actions taken.

## 4.2 Notification

* **Immediate Supervisor:** Report the incident to the immediate supervisor or manager within 30 minutes of detection.
* **IT Security Team:** Notify the IT Security Team through the designated reporting channel (e.g., internal ticketing system, email, or phone).
* **Health & Safety Officer:** If the incident involves health or safety concerns, contact the Health and Safety Officer.

## 4.3 Incident Report Form

Complete the Incident Report Form with the following details:

* **Incident Type:** (Security Breach, Malfunction, Data Leak, Health & Safety Concern)
* **Description:** Detailed description of the incident.
* **Impact Assessment:** Initial assessment of the potential impact on operations, data, and users.
* **Actions Taken:** Immediate actions taken to mitigate the incident.
* **Contact Information:** Details of the person reporting the incident.

# 5. Incident Response Procedure

## 5.1 Assessment and Classification

* **IT Security Team:** Review the initial report and classify the incident based on severity and impact.
* **Severity Levels:**
  + **Level 1:** Minor issues with minimal impact.
  + **Level 2:** Moderate issues affecting operational efficiency.
  + **Level 3:** Major issues with significant impact on operations or data integrity.
  + **Level 4:** Critical incidents involving severe breaches or health and safety hazards.

## 5.2 Response Coordination

* **Incident Response Team:** Activate the Incident Response Team (IRT) for incidents classified as Level 3 or Level 4.
* **Communication:** Establish clear communication channels for internal stakeholders and affected users. Provide updates as necessary.
* **Containment:** Implement measures to contain the incident and prevent further damage.
* **Eradication:** Identify and eliminate the root cause of the incident.
* **Recovery:** Restore BCI systems and data to normal operation. Verify that the systems are functioning correctly.
* **Post-Incident Review:** Conduct a post-incident review to evaluate the response and identify lessons learned.

# 6. Documentation and Reporting

## 6.1 Incident Log

Maintain a detailed incident log that includes:

* **Incident ID:** Unique identifier for the incident.
* **Timeline:** Chronological log of events and actions taken.
* **Resolution:** Summary of the resolution and any follow-up actions.

## 6.2 Final Report

Prepare a Final Incident Report that includes:

* **Incident Summary:** Overview of the incident.
* **Impact Analysis:** Detailed analysis of the impact on operations and data.
* **Response Evaluation:** Assessment of the effectiveness of the response.
* **Recommendations:** Suggested improvements to policies, procedures, and security measures.

## 6.3 Compliance

Ensure that the incident report and documentation comply with regulatory and legal requirements.

# 7. Training and Awareness

## 7.1 Employee Training

Conduct regular training sessions on incident reporting and response procedures for all users of BCIs.

## 7.2 Drills and Simulations

Organize periodic drills and simulations to test incident response readiness and identify areas for improvement.

# 8. Review and Updates

* **Review:** This run book will be reviewed annually and updated as necessary.
* **Feedback:** Gather feedback from incident response teams and users to improve the procedures.

# 9. Contact Information

For questions or concerns regarding this run book, please contact:

**BCI Security Policy Coordinator**

Email: <policy-coordinator@example.com>

Phone: <Phone Number>

# 13. Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Revision** | **Author** | **Notes** |
| August 2024 | 1.0 | Crawford | Document Creation |
|  |  |  |  |
|  |  |  |  |