2131 PALOMAR AIRPORT RD., STE. 239
CARLSBAD, CA 92011
800.240.3280
WWW.911EDA.COM

Incident Response Plan (IRP)

911EDA, Carlsbad CA 92011

Revision History Table for Incident Response Plan (IRP)

Version	Date	Description of Changes	Author(s)
1.0	02/17/2021	Initial creation of the Incident Response Plan.	Ryan O'Connor, Antonio Pereira, John Bray
1.1	06/15/2021	Updated communication protocols and added templates.	Communications Department
1.2	12/08/2021	Revised incident classification criteria and response actions for clarity.	IT Security Team
1.3	05/23/2022	Enhanced training and awareness program details.	HR Department
1.4	11/14/2022	Introduction of continuous improvement process and KPIs for IRP effectiveness.	Quality Assurance Team
1.5	04/07/2023	Adjustments to the IRT structure and backup contacts.	Ryan O'Connor, Antonio Pereira
2.0	06/05/2023	Major update to align with the latest NIST SP 800-171 revision and DFARS changes.	IT Security Team, Legal Department
2.1	11/22/2023	Minor updates to risk assessment procedures and reporting requirements.	Antonio Pereira

1. **Purpose and Scope**

- **Purpose**: To outline procedures and responsibilities for responding to cybersecurity incidents impacting CUI, ensuring swift containment, eradication, and recovery.
- **Scope**: This applies to all systems, networks, and personnel within 911EDA that store, process, or transmit CUI.

2. **Policy Statement**

911EDA commits to maintaining the confidentiality, integrity, and availability of CUI in compliance with NIST SP 800-171 and DFARS 252.204-7012 through an effective incident response program.

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

3.1 Composition

The Incident Response Team is a dedicated group comprising members from various departments, each bringing specialized expertise to manage and respond to cybersecurity incidents effectively. The team operates under a structured hierarchy to ensure efficient incident handling and communication.

3.2 Roles and Responsibilities

- **IRT Lead**
  - **Primary Contact**: Ryan O'Connor, President
    - Email: roconnor@911eda.com
    - Phone: 800-240-3280 x102
  - **Backup Contact**: Antonio Pereira, IT Security Specialist
    - Email: tpereira@911eda.com
    - Phone: 800-240-3280 x 104
  - **Responsibilities**: Coordinates the incident response efforts, serves as the primary decision-maker, and liaises with external stakeholders, including regulatory bodies and law enforcement agencies.
- **IT Security Members**
  - **Primary Contact**: Antonio Pereira, IT Security Specialist
    - Email: apereira@911eda.com
    - Phone: 800-240-3280 x104
  - **Backup Contact**: Taimur Khan, Design Manager
    - Email: tkhan@911eda.com
    - Phone: 800-320-2480 x110
  - **Responsibilities**: Lead the technical assessment, containment, eradication, and recovery efforts. They are responsible for analyzing the incident's scope and impact and implementing technical controls to mitigate the incident.
- **Communications Department**
  - **Primary Contact**: Taimur Khan, Communications Specialist
    - Email: tkhan@911eda.com
    - Phone: 800-240-3280 x110
  - **Backup Contact**: Ryan O’Connor, President
    - Email: roconnor@911eda.com
    - Phone: 800-320-2480 x102
  - **Responsibilities**: Manages all internal and external communications related to the incident. This includes drafting and disseminating notifications and updates to employees, stakeholders, and the public, ensuring messaging is consistent and accurate.
- **Legal Advisor**
  - **Primary Contact**: John Bray, Legal Advisor
    - Email: jbray@braylaw.com
    - Phone: 760-941-9134
  - **Backup Contact**: Ryan O’Connor, President
    - Email: roconnor@911eda.com
    - Phone: 800-320-2480 x102
  - **Responsibilities**: Provides advice on legal and compliance issues related to the incident, including data breach notification requirements and liaising with external legal counsel as needed. The Legal Advisor ensures that the incident response actions comply with applicable laws and regulations.

3.3 **Activation Protocol**
Upon identification of a potential security incident, the IRT Lead is notified. The Lead then assesses the situation and, if warranted, activates the IRT according to the severity level. All members are expected to be available within the response time outlined in the Incident Classification Criteria.

4. **Incident Response Phases**
The Incident Response Plan is executed through a series of well-defined phases, each critical to effectively managing and mitigating cybersecurity incidents. The following outlines each phase, including specific steps, responsibilities, and tools employed.

4.1 Preparation

- **Objective**: Establish a readiness posture to effectively respond to incidents.
- **Actions**:
    - Conduct regular training and simulation exercises for the Incident Response Team (IRT) and all employees.
    - Ensure incident detection tools (e.g., IDS, SIEM) are properly configured and updated.
    - Maintain an inventory of critical assets and their respective protection measures.
- **Tools/Methodologies**: Incident simulation platforms, employee cybersecurity awareness platforms.

4.2 Detection and Analysis

- **Objective**: Identify and assess the nature and scope of the incident.
- **Actions**:
    - Monitor and analyze alerts from security tools to identify potential incidents.
    - Use log aggregation and analysis tools to gather and interpret relevant data.
    - Classify the incident according to the predefined severity levels in Appendix B.
- **Tools/Methodologies**: Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems, log analysis software.

4.3 Containment

- **Objective**: Limit the spread of the incident and isolate affected systems to prevent further damage.
- **Actions**:
    - Implement short-term containment measures, such as disconnecting infected systems from the network.
    - Apply long-term containment strategies, like re-routing network traffic or establishing secure partitions.
    - Communicate containment actions to relevant stakeholders to minimize operational impact.
- **Tools/Methodologies**: Network segmentation tools, firewall rules adjustments, access control lists (ACLs).

4.4 Eradication

- **Objective**: Remove the cause of the incident and any associated malware or vulnerabilities.
- **Actions**:

- Identify and remove all malicious code and compromised files from affected systems.
- Apply patches to vulnerable systems and update security measures to prevent recurrence.
- Validate the effectiveness of eradication efforts through comprehensive testing.

- **Tools/Methodologies**: Antivirus and anti-malware solutions, patch management systems, vulnerability scanners.

4.5 Recovery

- **Objective**: Restore and return affected systems to normal operations while ensuring they are no longer compromised.
- **Actions**:
  - Gradually restore systems using backups, ensuring no latent threats remain.
  - Monitor the restored systems for any signs of malicious activity.
  - Document lessons learned and integrate findings into future response efforts.
- **Tools/Methodologies**: Backup and recovery solutions, network monitoring tools, incident documentation platforms.

4.6 Post-Incident Activity

- **Objective**: Review and analyze the incident to improve future response efforts and security posture.
- **Actions**:
  - Conduct a post-incident review meeting to discuss the incident's handling, what was done well, and areas for improvement.
  - Update the IRP and security controls based on lessons learned.
  - Provide a detailed report to management and relevant stakeholders outlining the incident, response effectiveness, and recommendations for preventing future incidents.
- **Tools/Methodologies**: Post-incident review templates, IRP update protocols, cybersecurity frameworks for benchmarking improvements.

6. **Communication**

- **Internal Notification**: Alert relevant internal stakeholders and initiate the IRT.
- **External Communication**: Coordinate with external entities, including law enforcement and regulatory bodies, as required by DFARS 252.204-7012 and NIST guidelines.

7. **Documentation and Reporting**

Effective documentation and timely reporting are pivotal components of the incident response process, ensuring accountability, facilitating post-incident reviews, and meeting legal and regulatory requirements.

7.1 **Documentation Best Practices**

- **Objective**: Maintain accurate and comprehensive records of the incident and the response actions taken.
- **Guidelines**:
  - **Initiate Documentation Early**: Begin documentation as soon as an incident is detected, capturing initial alerts, actions taken, and observations.

- **Use a Standardized Format**: Employ a consistent format for documenting incidents to ensure that all necessary information is captured systematically.
- **Detail Incident Timeline**: Construct a detailed timeline of the incident, including detection, response actions, and recovery efforts.
- **Preserve Evidence**: Securely store all digital and physical evidence related to the incident, such as logs, malicious code samples, and compromised files.
- **Confidentiality**: Ensure that the documentation is accessible only to authorized personnel to protect sensitive information.

7.2 **Reporting Requirements**

- **Objective**: Comply with regulatory, contractual, and legal reporting requirements specific to cybersecurity incidents.
- **Procedures**:
  - **DFARS 252.204-7012 Compliance**: For incidents involving defense-related CUI, report to the DoD's designated reporting system within 72 hours of incident detection.
  - **NIST SP 800-171 Compliance**: Document the incident's impact on CUI and the measures taken to safeguard it, for review during compliance audits.
  - **Law Enforcement Notification**: In cases of illegal activity, coordinate with the legal department to notify appropriate law enforcement agencies.
  - **Stakeholder Communication**: Inform affected parties, including customers and partners, in accordance with privacy laws and contractual obligations.

7.3 **Incident Report Content**

- **Incident Description**: Provide a brief overview of the incident, including the type of incident, systems affected, and potential impact.
- **Response Actions**: Outline the response actions taken, including containment, eradication, and recovery efforts.
- **Impact Assessment**: Assess the incident's impact on operations, data, and stakeholders.
- **Lessons Learned**: Highlight key insights gained and any corrective actions implemented to prevent future occurrences.

7.4 **Post-Incident Reporting**

- **Objective**: Conduct thorough post-incident analysis and report findings to relevant stakeholders.
- **Actions**:
  - **Compile a Comprehensive Incident Report**: Utilizing the documentation gathered, compile a report that details the incident timeline, impact, response actions, and lessons learned.
  - **Review and Approval**: The Incident Response Team Lead and relevant department heads should review and approve the report for accuracy and completeness.
  - **Dissemination**: Distribute the report to designated stakeholders, including senior management, affected business units, and compliance officers, ensuring that sensitive information is handled appropriately.

8. **Training and Awareness**
   - Conduct regular training sessions for all employees on recognizing and reporting security incidents.
   - Perform periodic drills and simulations to enhance the IRT's preparedness.

9. **Review and Continuous Improvement**
   - Regularly review and update the IRP to reflect changes in the threat landscape, lessons learned from incident responses, and technological or procedural advancements.

10. **References**
    - NIST SP 800-171: Protecting CUI in Non-Federal Systems and Organizations.
    - DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.

11. **Appendices**
    - Contact Information for IRT Members.
    - Incident Classification Criteria.
    - Incident Response Checklist.
    - Templates for Internal and External Communications.

This IRP is designed to be dynamic, adapting to new threats and incorporating continuous improvement based on incident response experiences and evolving compliance requirements.

Appendix A: Contact Information for Incident Response Team (IRT) Members

1. **IRT Lead**
    - Name: Ryan O'Connor
    - Position: President
    - Email: roconnor@911eda.com
    - Phone: 800-240-3280 x102
2. **IT Security Members**
    - Name: Antonio Pereira
    - Position: IT Security Specialist
    - Email: apereira@911eda.com
    - Phone: 800-240-3280 x104
3. **Communications**
    - Taimur Khan
    - Position: Communications Department
    - Email: tkhan@911eda.com
    - Phone: 800-240-3280 x110
4. **Legal Advisor**
    - Name: John Bray
    - Position: Legal Advisor
    - Email: jbray@braylaw.com
    - Phone: 760-941-9134

Appendix B: Incident Classification Criteria

Severity Level 1 (High)

- **Impact**: Operations critically impacted or significant data breach involving sensitive PCB designs, client data, or Controlled Unclassified Information (CUI).
- **Response Time**: Immediate action required; respond within 1 hour.
- **Examples**:
  - Unauthorized access to PCB design files containing trade secrets or client-specific designs, leading to potential intellectual property theft.
  - A ransomware attack encrypting critical PCB design software or databases, severely disrupting design and production processes.

Severity Level 2 (Medium)

- **Impact**: Operations moderately affected, potential for data exposure, or unauthorized access to non-critical systems.
- **Response Time**: Respond within 4 hours.
- **Examples**:
  - Detection of malware in administrative systems not directly involved in PCB design but potentially capable of lateral movement to critical systems.
  - Phishing attack leading to unauthorized access to an employee's email account, risking exposure of non-sensitive design discussions or client communications.

Severity Level 3 (Low)

- **Impact**: Minimal operational impact, no data breach of sensitive systems, or incidents that affect non-critical aspects of the PCB design process.
- **Response Time**: Respond within 24 hours.
- **Examples**:
  - Discovery of a vulnerability in the company’s public-facing website without evidence of exploitation or risk to internal systems.
  - Minor malware infection on a standalone machine used for generic office tasks without access to critical design software or sensitive information.

Appendix C: Incident Response Checklist

Initial Detection and Reporting

- □ **Identify the Incident**: Record the type of incident (e.g., unauthorized access, malware infection) and the initial detection method.
    - **Notes**: _____
      _____
      _____
- □ **Report to IRT**: Notify the Incident Response Team Lead and relevant members according to the contact list in Appendix A.
    - **Notes**: _____
      _____
      _____

Incident Assessment

- □ **Classify the Severity**: Determine the incident's severity level based on Appendix B criteria and record the rationale.
    - **Notes**: _____
      _____
      _____
- □ **Determine Scope and Impact**: Assess which systems, data, or PCB design processes are affected and estimate the operational impact.
    - **Notes**: _____
      _____
      _____

Containment

- □ **Isolate Affected Systems**: Implement immediate measures to disconnect or limit network access for compromised systems.
    - **Notes**: _____
      _____
      _____
- □ **Apply Longer-term Containment**: Establish more permanent containment measures, such as network segmentation or access restrictions.
    - **Notes**: _____
      _____
      _____

Eradication

- □ **Remove Root Causes**: Identify and eliminate the sources of the incident, such as malware or unauthorized access points.
    - **Notes**: _____
      _____
      _____

- □ **Clean and Restore Systems**: Ensure that affected systems are cleaned of any malicious elements and restored to their original state.
    - **Notes**: _____
      _____
      _____

Recovery

- □ **Restore Operations**: Gradually reinstate normal operations, ensuring that systems are fully functional and secure.
    - **Notes**: _____
      _____
      _____
- □ **Monitor for Anomalies**: Closely observe the restored systems for signs of instability or signs of the incident recurring.
    - **Notes**: _____
      _____
      _____

Post-Incident Review

- □ **Conduct a Lessons-Learned Meeting**: Gather the IRT and relevant stakeholders to review the incident handling process.
    - **Topics Discussed**: _____
      _____
      _____
- □ **Document Findings and Update IRP**: Record the insights gained and implement necessary updates to the IRP and security controls.
    - **Action Items**:_ _____
      _____
      _____

Appendix D: Templates for Internal and External Communications

Internal Notification Template

Subject: [Incident Classification: High/Medium/Low] - Security Incident Notification

Body:

Dear Team,

We want to inform you of a [incident classification] security incident that has been detected within our network/systems. The incident involves [brief description of the incident, e.g., unauthorized access to PCB design files, malware infection].

Action Taken:

- Immediate steps have been taken to contain and address the incident, including [briefly outline actions, e.g., isolating affected systems, implementing additional security measures].

Expected Impact:

- At this time, we anticipate the impact on operations/data to be [state expected impact, e.g., minimal due to our quick response, significant until further notice].

Next Steps:

- The Incident Response Team is actively working to resolve this issue and further updates will be provided as more information becomes available.
- Employees are advised to [any immediate actions for employees, e.g., change passwords, avoid clicking on suspicious emails].

Thank you for your attention to this matter and your cooperation in ensuring our systems' security.

Best,
[Your Name]
[Your Position]

External Communication Template

Subject: Notice of Security Incident

Body:

Dear [Stakeholder/Client/Partner],

We are writing to inform you of a security incident that recently occurred at 911EDA Inc. Upon detection, we promptly initiated our incident response process to address the situation.

Incident Overview:

- A [brief description of the incident, e.g., breach involving unauthorized access to non-sensitive PCB design files] was detected on [date].
- We have taken immediate steps to contain the incident and are conducting a thorough investigation.

Actions Taken:

- Our response efforts have included [outline key response actions, e.g., isolating affected systems, enhancing security protocols].

Commitment to Security and Privacy:

- At 911EDA Inc., we take the security of our systems and the privacy of our clients very seriously. We are committed to resolving this issue swiftly and transparently.

Recommended Actions for You:

- While we have no evidence that client data was affected, we recommend [any recommended actions for recipients, e.g., monitoring accounts for suspicious activity].

We deeply regret any concern this may cause you. We will continue to keep you informed of our progress in resolving this incident and any steps we are taking to strengthen our systems further.

Sincerely,
[Your Name]
[Your Position]

Appendix E: Evidence Preservation Guidelines

Objective

To standardize procedures for collecting, handling, and storing digital evidence during and after cybersecurity incidents, ensuring the integrity and admissibility of evidence for internal investigations, legal proceedings, or regulatory compliance.

Guidelines

- **Immediate Collection**: As soon as an incident is detected, promptly collect and secure all relevant digital evidence, including logs, malware samples, and compromised files.
- **Secure Storage**: Store digital evidence in a secure, access-controlled environment. Physical evidence should be kept in locked containers. Maintain a detailed inventory of stored evidence.
- **Chain of Custody**: Document the chain of custody for all evidence, recording every individual who accessed the evidence and the purpose of access. Use digital chain-of-custody forms where possible.
- **Forensic Copies**: Make forensic copies of digital evidence and conduct analyses on the copies to preserve the original evidence's integrity.
- **Data Integrity**: Use cryptographic hashes to verify the integrity of digital evidence from the time of collection through analysis and storage.
- **Legal Compliance**: Ensure evidence preservation practices comply with applicable laws and regulations. Consult the legal department for guidance on specific legal requirements.

Appendix F: Post-Incident Review Template

Objective
To conduct a structured review of the incident response process, capturing key learnings, identifying improvement opportunities, and documenting corrective actions to enhance future response efforts.

Template Sections

1. Incident Overview

- **Description of Incident:**_____
  _____
  _____
- **Date and Time Detected:** _____
- **Systems/Processes Affected:**_____
  _____
  _____
- **Incident Classification:** _____

2. Response Evaluation

- **Effectiveness of Response:** (Consider speed of detection, containment, and eradication efforts)
  _____
  _____
- **Communication:** (Assess internal and external communication effectiveness)
  _____
  _____
- **Challenges Encountered:** _____
  _____

3. Impact Analysis

- **Operational Impact:**
  _____
- **Data/Intellectual Property Impact:**
  _____
- **Financial Impact:**
  _____
- **Reputational Impact:**
  _____

4. Lessons Learned

- **Successful Strategies:**
  _____
  _____
- **Areas for Improvement:**
  _____
  _____
- **Preventative Measures Identified:**
  _____
  _____

5. Corrective Actions

- **Action Items:** (List specific actions to address identified issues)
  _____
  _____
- **Assigned To:** (Name/department responsible for each action)
  _____
  _____
  _____
- **Deadline:** (Timeline for completion)
  _____
  _____

6. Feedback Loop

- **Process for Integration:** (Describe how lessons learned will be integrated into IRP and security practices)
  _____
  _____
  _____
- **Follow-up Review Date:**
  _____