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

Cybersecurity Protocols Documentation for 911EDA Inc.

911EDA, Carlsbad CA 92011

1. **Introduction**
This document outlines the cybersecurity protocols implemented by 911EDA Inc. to safeguard its digital assets, including PCB design files, client information, and internal communications. These protocols are designed to ensure compliance with NIST SP 800-171, DFARS 252.204-7012, and other applicable cybersecurity standards.

2. **Purpose**
The purpose of this document is to provide a comprehensive overview of the cybersecurity measures and practices in place at 911EDA Inc. It aims to establish a clear understanding among employees, contractors, and partners about their roles and responsibilities in maintaining the security posture of the organization.

3. **Scope**
The scope of this document encompasses all systems, networks, and data managed by 911EDA Inc. that are involved in the storage, processing, and transmission of CUI, specifically relating to PCB designs and client data.

4. **Cybersecurity Protocols**

4.1 **Access Control**
- Implementation of Role-Based Access Control (RBAC) to ensure users have access only to resources necessary for their roles.
- Enforcement of Multi-Factor Authentication (MFA) for accessing sensitive systems and data.

4.2 **Data Encryption**
- Use of Advanced Encryption Standard (AES) for encrypting data at rest and in transit, safeguarding against unauthorized disclosure.
- Management of encryption keys using secure key management practices.

4.3 **Network Security**
- Deployment of firewalls and Intrusion Detection Systems (IDS) to monitor and control incoming and outgoing network traffic.
- Regular network segmentation to isolate critical systems and data from the broader network.

4.4 **Malware Protection**
- Installation of up-to-date antivirus and anti-malware solutions on all endpoints and servers.
- Regular scanning of systems and networks to detect and remove malicious software.

4.5 **Incident Response**

- Establishment of an Incident Response Team (IRT) with clear roles and responsibilities as outlined in the IRP.
- Regular training and drills to ensure preparedness for responding to cybersecurity incidents.

4.6 **Awareness and Training**

- Conducting ongoing cybersecurity awareness training for all employees to recognize and mitigate cyber threats.
- Specialized security training for IT staff on the latest cybersecurity practices and technologies.

5. **Continuous Monitoring and Assessment**

- Implementation of continuous monitoring strategies to detect anomalies and potential security threats.
- Regular security assessments and audits to evaluate the effectiveness of cybersecurity measures.

6. **Vendor and Third-Party Security**

- Conducting security assessments of vendors and third-party service providers to ensure they meet 911EDA Inc.'s security standards.
- Incorporating security requirements into contracts with vendors and third parties handling CUI.

7. **Compliance and Reporting**

- Maintaining records of cybersecurity practices and incidents to demonstrate compliance with relevant cybersecurity regulations.
- Reporting cybersecurity incidents as required by DFARS 252.204-7012 and other applicable laws.

8. **Document Maintenance**

- Regular review and update of this document to reflect changes in cybersecurity threats, technologies, and regulatory requirements.

9. **Conclusion**

The Cybersecurity Protocols Documentation is a living document, crucial for the ongoing effort to protect 911EDA Inc. from cyber threats. Adherence to these protocols by all employees and contractors is mandatory to ensure the security and integrity of our operations and client data.