Pleaz Software Development Policy

1. Purpose

This policy outlines the principles and practices for software development at Pleaz to ensure compliance with OWASP (Open Web Application Security Project) principles. The goal is to maintain a high level of user data security while supporting the needs of a high-growth software company.

2. Scope

This policy applies to all software development activities at Pleaz, including but not limited to coding, testing, deployment, and maintenance.

3. OWASP Principles

Pleaz commits to following the OWASP Top Ten principles to mitigate the most critical security risks:

1. **Injection**
2. **Broken Authentication**
3. **Sensitive Data Exposure**
4. **XML External Entities (XXE)**
5. **Broken Access Control**
6. **Security Misconfiguration**
7. **Cross-Site Scripting (XSS)**
8. **Insecure Deserialization**
9. **Using Components with Known Vulnerabilities**
10. **Insufficient Logging & Monitoring**

4. Policy Statements

4.1 Security by Design

- All software development projects must integrate security from the initial design phase through to deployment.
- Conduct threat modeling and security risk assessments at the start of each project.

4.2 Secure Coding Practices

- Developers must follow secure coding guidelines as per OWASP Secure Coding Practices.

4.3 Code Review and Static Analysis

- All code must undergo peer review with a focus on security vulnerabilities.

4.4 Authentication and Access Control

- Implement strong authentication mechanisms, following the latest OWASP Authentication Guidelines.
- Ensure proper access control measures are in place to restrict access to sensitive data.

4.5 Data Protection

- Sensitive data must be encrypted both in transit and at rest.

4.6 Vulnerability Management

- Regularly update and patch all components, libraries, and frameworks used in development.

4.7 Incident Response

- Establish and maintain an incident response plan as the IT security Policy.

4.8 Logging and Monitoring

- Implement comprehensive logging and monitoring to detect and respond to security events.

4.9 Continuous Improvement

- Conduct post-incident reviews and root cause analyses to improve security measures continuously.
- Encourage a culture of continuous learning and improvement in security practices.

5. Roles and Responsibilities

5.1 Chief Product Officer (CPO)

- Ensure the implementation and adherence to this policy.

5.2 Development Team

- Follow the secure coding practices and guidelines outlined in this policy.
- Participate in code reviews and security training sessions.

6. Compliance and Enforcement

- Compliance with this policy is mandatory for all software development projects.
- Non-compliance will be addressed through disciplinary actions, which may include termination of employment for severe violations.

7. Review and Update

- This policy will be reviewed annually and updated as necessary to ensure it remains effective and relevant to emerging security threats and business needs.