# Development Team Security Policy

**Purpose:**
This policy governs secure development practices for the development team, ensuring the security of code and systems from design to deployment.
**Key Areas:**

**1. Secure Coding Standards:**
- All development must follow secure coding practices to prevent vulnerabilities such as SQL injection and cross-site scripting (XSS).
- Developers must ensure input validation, output encoding, and encryption in code handling sensitive data.

**2. Access Control:**
- Only authorized developers should have access to development environments, with role-based access control (RBAC) in place.
- Use version control to track changes and maintain accountability in the codebase.

**3. Encryption and Authentication:**
- Developers must use strong encryption methods for sensitive data, both in storage and transit.
- Implement multi-factor authentication (MFA) for access to critical systems and databases.

**4. Vulnerability Management:**
- Developers must be familiar with the OWASP Top 10 vulnerabilities and apply mitigation techniques during development.
- Regularly perform security testing on the codebase to identify and address vulnerabilities early in the development lifecycle.

**5. Code Review:**
- Conduct peer reviews of code to ensure adherence to secure development practices.
- Review and address security issues before code is merged or deployed to production environments.

**6. Reporting:**
- All discovered vulnerabilities, whether during development or testing, must be reported to the QA and IT security teams for further analysis and resolution.