[Company]

SECURE DEVELOPMENT POLICY

Information security in software development

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Secure Development Policy

3.1 Purpose

The purpose of this policy is to ensure information security is designed and implemented within the development lifecycle.

3.2 Scope

System development of bespoke company software solutions.

All employees and third-party users.

3.3 Principle

Secure software and system engineering principles and standards are implemented and tested.

Information security and privacy are by design and default.

3.4 Segregation of Environments

Development, test, and production environments are separated and do not share common components.

Development, test, and production environments are on separate networks.

There is a segregation of administrative duties between development and test, and production.

3.5 Secure Development Coding Guidelines

Software is designed and developed based on industry secure coding guidelines for the coding technology and the Open Web Application Security Project (OWASP).

The NCSC government guidelines for secure development are considered:

https://www.ncsc.gov.uk/collection/developers-collection

The NIST Whitepaper on MITIGATING THE RISK OF SOFTWARE VULNERABILITIES BY ADOPTING AN SSDF are considered:

https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

3.6 Development Code Repositories

Development code is stored in a secure code repository that enforces and meets the requirements of the access control policy and segregation of duty.

Development code repositories enforce version control and appropriate version archiving.

3.7 Development Code Reviews

Code is reviewed prior to release by skilled personnel other than the code author / developer.

Code is reviewed against the secure development coding guidelines.

Code reviews employ manual and automated techniques.

3.8 Development Code Approval

Code is approved before being promoted into test or production.

3.9 Testing

All pre-production testing occurs in a test environment.

The test environment mirrors as far as possible the production environment.

Application security testing is performed using manual and automated techniques.

Testing is performed that as a minimum test for the OWASP top 10.

External penetration testing is performed prior to initial release and then periodically or after a significant change.

All public facing web applications are tested using manual or automated vulnerability security tools or methods at least annually or after a significant change.

All vulnerabilities identified as part of the testing phase including penetration testing are corrected prior to promotion to production or managed via the risk management process.

Test results including penetration testing are additionally reported to the Management Review Team.

All penetration testing is conducted by an external specialist company.

3.10 Test Data

Production data is never used for testing or development.

Card holder data is never used for testing or development.

Personal data is never used for testing or development.

If sensitive information is required as part of the testing process it is

- sanitised,
- anonymised or

- pseudonymised.

3.11 Promoting Code to Production

Code is promoted to production by approved personnel and is subject to the documented change control process.

The production environment is backed up prior to the promotion of code to production to facilitate roll back for a failed change.

Test data is removed before the application is promoted to production.

No development files or test data are stored in the production environment.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.