CHOICE EQUITY BROKING PVT. LTD

SOFTWARE DEVELOPMENT POLICY

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	11-Jan-20	1.5	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	15-July-21	1.6	Sunil Utekar	Yogesh Jadhav
Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav
Reviewed On	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj
Reviewed On	20-Feb-25	2.2	Abhishek Vinayak	Ashutosh Bhardwaj

TABLE OF CONTENTS

1.0 Purpose

Appropriate security controls shall be incorporated in development and implementation of business applications in Choice Equity Broking Pvt. Ltd. (Choice) information processing environment.

2.0 Scope

This policy applies to:-

- API Development
- Web Development
- Mobile Application Development
- Outsourced Development
- open-source software integration

3.0 Policy

3.1 Key Principles of Secure Development

1. Secure Development Lifecycle (SDLC)

The SDLC for all development types must incorporate security at each phase:

- **Requirements Gathering**: Include security requirements from the start and ensure alignment with application security needs.
- **Design**: Apply security by design principles to avoid vulnerabilities, such as secure coding practice and architecture reviews..
- **Development**: Implement secure coding techniques and conduct security code reviews.
- **Testing**: Perform thorough security testing, including static and dynamic analysis including vulnerability scanning and security code review.
- **Deployment**: Ensure the security of production environments by conducting final validation.
- **Maintenance**: Continuously monitor and patch systems post-deployment to address new vulnerabilities or performance issues.

2. Application Security Requirements

Application security requirements must be identified and enforced across all platforms and environments. These include:

- **Authentication & Access Control**: Use multi-factor authentication (MFA)/ Dual-factor authentication and role-based access control (RBAC) for all users wherever possible. Enforce least privilege access.
- **Data Protection**:
    - Implement encryption for data in transit and at rest.
    - Use secure communication protocols.
    - Implement strict data retention and deletion policies.
- **Vulnerability Prevention**:

    - Protect against common threats such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and buffer overflow attacks.
    - Implement input validation and output encoding techniques to avoid injection flaws.

3. Secure System Architecture and Engineering Principles

- **Security by Design**: Integrate security controls and practices during the design phase, not as an afterthought.
- **Defense in Depth**: Employ multiple layers of security controls (e.g., firewalls, intrusion detection systems, encryption, etc.).
- **Zero Trust Architecture**: Ensure all components authenticate and authorize every request, regardless of source, and encrypt communications at every layer.

4. Secure Coding Practices

Developers should adhere to secure coding guidelines to prevent vulnerabilities. These include:

- **Secure Coding Standards**: Adopt and enforce secure coding guidelines, such as OWASP top ten or other industry best practices (as feasible) to prevent common vulnerabilities.
- **Code Reviews**: Conduct regular peer reviews and pair programming.
- **Secure Development Tools**: Use integrated development environments (IDEs) and tools that support secure coding practices (e.g., IDE-based vulnerability scanners, linters, Sonar Lint).
- **Training**: Provide continuous secure coding education for all developers.
- **Prohibited Practices**:
    - Hard-coding sensitive data like passwords or keys.
    - Using deprecated or vulnerable libraries or frameworks.
    - Failing to sanitize input before processing.

5. Security Testing in Development and Acceptance

- **Static Application Security Testing (SAST)**: Analyze source code for vulnerabilities before runtime.
- **Vulnerability Testing**: Simulate attacks to identify potential security risks.

6. Outsourced Development

For any outsourced development, the following must be ensured:

- Security practices must be in line with organizational standards.
- The vendor must provide evidence of secure development practices, including secure coding, testing, and compliance certifications (if any) such as ISO 27001, ISO 12207.
- Explicit security clauses must be included in contracts and agreements with third-party developers.
- The Information Security team should evaluate that all necessary security requirements of the Choice Equity are met and any exceptions are documented and signoff by CISO.

7. Separation of Development, Test, and Production Environments

- **Environment Segregation**: Maintain clear separation between development and production environments to prevent unauthorized access and data leakage.
- **Access Control**: Strictly control access to each environment, with minimal overlap between personnel involved in development, testing, and production.
- **Data Handling**: Production data should never be used in testing environments without anonymization or pseudonymization.

8. Change Management

- **Version Control**: All changes to code and configurations must be tracked using secure version control systems, such as Gitlab.
- **Change Approval**: Introduce a formal change approval process to ensure all changes are reviewed from a security perspective before deployment.
- **Auditing**: Maintain logs of all changes, who approved them, and when they were made, to enable post-incident analysis if needed.

9. Test Information

- **Data Integrity**: Ensure that test data cannot be used to access or modify production systems.
- **Environment Security**: Ensure that test environments are secured and monitored to prevent unauthorized access to sensitive data during testing.
- **Testing Constraints**: No real production data should be used in testing unless necessary, and if used, it must be anonymized to protect sensitive information.

10. Protection of Information Systems During Audit Testing

- **Test Environment Isolation**: During audit testing or assessments, systems being tested should be isolated from the live production environment to prevent accidental disruption.
- **Data Privacy and Protection**: Ensure that any sensitive data exposed during audit tests is properly protected using encryption and access control measures.
- **Compliance**: All audit tests must adhere to regulatory and compliance requirements concerning data privacy.

3.2 Controls in Software Development

Planning and Initiation Phase

- Project Lead shall document the business requirement specifications.
- Project lead along with the project team shall be responsible to build the essential security mechanisms within the application.
- Documentation of security mechanisms within the application shall be part of the Business Requirements Specification (BRS) document of the application. Such specification shall be added to the BRS based on the requirement.
- The Business Requirements Specification (BRS) document shall be revised after every modification and shall be protected as seriously as the application itself.
- A preliminary risk analysis shall be performed to determine the security controls required for the system or application under development.

- Security vulnerabilities shall be considered when designing connectivity or interface with other systems and applications.
- A balance shall be maintained between user requirements and appropriate security controls.

Requirement Analysis

Security requirements for the software shall be prepared based on:

- Security requirements from the information owners
- Technology controls
- Applicable regulatory guidelines

Software Design

- Security specifications for the software shall be documented to provide the development group with standard requirements. This enables Choice Equity Broking Pvt. Ltd. (Choice) in identifying, reviewing and testing the security functionalities of the software. Project lead shall review the security specifications which shall be in accordance with the standard security checklist of Choice wherever applicable.

Software Development

- This phase integrates all the components of the system or application based on the design. During development, the following steps occur:
    - The executable code is created. In some cases script code is created.
    - The required files and databases are built and populated.
    - The hardware, software and communication services necessary to support the development effort are assembled
    - The documents to support testing, implementation and maintenance of the system are compiled.
    - Sensitivity of data to be processed, stored and transmitted by the system;
    - Applicable external and internal requirements, e.g. from regulations or policies;
    - Security controls already implemented by the organization that support system development;
    - The need for segregation between development and production environments;
    - Control of access to the development environment;
    - Monitoring of change to the environment and code stored therein;
    - Control over movement of data from and to the environment.
    - Code review from information security perspective shall be conducted
- Where software development is outsourced, the following points shall be considered:
    - Licensing arrangements, code ownership and intellectual property rights
    - Certification of the quality and accuracy of the work carried out
    - Right of access (to source code wherever permitted by contract, infrastructure, procedures followed) for audit of the quality and accuracy of work done by outsourced supplier/contractors
    - Contractual requirements for quality of code, secure design coding and testing practice
    - Testing before installation to detect Back-doors or Trojan code
    - Provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;
    - Provision of evidence that sufficient testing has been applied to guard against the

absence of both intentional and unintentional malicious content upon delivery;
- Provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;
- Escrow arrangements, e.g. if source code is no longer available;
- SBOM for the software
- Contractual right to audit development processes and controls;
- Effective documentation of the build environment used to create deliverables;
- The organization remains responsible for compliance with applicable laws and control efficiency verification.

All modifications, enhancements and installation or implementation of new systems shall subject to Test" by the appropriate users prior to installation into production.

- **Implementation Phase**
  - For software packages, system default settings shall be reviewed prior to installation to determine potential security holes. All third party supplied default passwords shall be changed prior to the system being placed in a production environment.
  - There shall be an inspection and acceptance of security features of the software before moving the final build into the production environment.
  - Recompile all source code before moving the code into production and remove developer access from all software in the production environment.
  - Training shall be imparted to all users of the software.
  - Recovery /rollback shall be considered and kept handy during the implementation.
  - Proper control mechanisms shall be in place to prevent unauthorized modifications to software once it goes into production.

Operations / Maintenance Phase

- The system shall be continuously checked for any malfunctions/ possible compromise of the system.
- All changes to the software shall be carried out in line with Change Management Policy.

Disposition Phase

- Care shall be taken to dispose of the equipment and software in the most secure manner.
- The disposal shall happen in accordance with the classification of the information asset being disposed of.
- All such actions of disposal shall be recorded, the asset register shall be updated and classification labels attached to the asset shall be disposed.

3.3 Controls in Software Procurement

The following controls shall be implemented:

- Buying programs only from authorized distributors and resellers
- Using only evaluated (tried and tested) products
- Controlling access to and modification of code once installed
- Signing escrow agreements wherever possible, in case of non availability of source code to Choice Equity Broking Pvt. Ltd. (CHOICE)
- Testing before installation to detect viruses, Back-doors or Trojan code

3.4 Control of Production Software

- All application source code and production executables shall be maintained in libraries and shall be secured from unauthorized access. Version control of the software shall be maintained by Project / Team Leader.
- The development and production environment shall be kept separate. Preferably these environments shall be hosted on separate networks / subnets not reachable from each other to avoid the accidental corruption/destruction of data.
- Software available for users in the production environment shall include only the executables of the application. The source code shall not be copied to the production environment, unless it is a script.

3.5 Protection of System Test Data

- Production data shall not be used as the test data, unless explicitly authorized by LOB Head of the team using the application and CISO.
- Access controls that are applicable for the production database shall also be applicable for the test systems, if production data is loaded on the test server.
- The use of production information containing sensitive customer information or confidential information shall be restricted only to a team of testers working on that particular project.
- PII data being held in the test server databases shall be encrypted.
- Production data, wherever feasible, shall be masked.
- For the test environment where production data is not loaded on the test servers, access controls can be reduced for the ease of use by testers from various departments.

3.6 Access Control to Program Source Code

- The access to program source code of the production system shall be controlled to prevent any corruption of the application programs.
- Program source code shall not be maintained in the production operational environment.
- The change management policy shall be followed for any modifications to the program source code. Use of version control software is recommended. Access to version control software shall be restricted to software owners.
- All programs shall have a standard naming convention to identify the version numbers
- Old versions of source programs shall be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.

3.7 Encryption

- Choice Equity Broking Pvt. Ltd. (CHOICE) shall consider use of encryption for protection of its sensitive information managed by the software. Appropriate levels of encryption of passwords shall be used for applications, database, operating system, and network devices.
- Encryption type and other implementation details shall be decided based on the relevant legislations and the level of protection required for the information.
- A regular review shall be carried out to determine the level of protection, which shall be given to particular information. This assessment can then be used to determine whether an existing control is appropriate, what type of control shall be applied and for what purpose and business processes.

3.8 Use of Cryptographic Controls

For proper use of cryptographic controls the following controls shall be considered:

- Management approach towards cryptographic controls
- Standards to be adopted for effective implementation
- General principles under which information shall be protected

3.9 Security in Support Processes

3.9.1 Correct Processing in Applications

All application systems across Choice Equity Broking Pvt. Ltd. (CHOICE) shall have appropriate access control mechanisms in place to ensure that the data integrity and security is maintained and any unauthorized access to applications or a part thereof is prevented / restricted.

Application management procedure shall consist of the following:

- Input Data Validation –The input data for the application systems shall be validated for out-of- range values, invalid characters, entering data in compulsory fields, duplicate values in key fields before saving (or committing a transaction).
- Control of Internal Processing – Applications shall be designed to ensure accurate internal processing. Suitable control measures like run-to-run controls shall be built into applications during batch processing.
- Output Data Validation – Reports / output generated from applications shall ensure that integrity of data is checked and all relevant data is processed before generating output.

3.9.2 Security of system files and documentation

- System files and documentation contain a range of sensitive information, e.g. descriptions of application processes, procedures, data structures, authorization process, test data etc. System files and documentation shall be protected from damage, theft and unauthorized access.

3.10 Post Implementation Review

- Implement additional monitoring to detect any anomalies or security incidents resulting from post-implementation changes.
- Verify that post-implementation changes comply with the actual requirements.

4.0 Roles and Responsibilities

- Implementation – Project and Team Leads along with outsourced partners are responsible for implementing the security controls for their respective applications
- Monitoring and Supervision – Application owners are responsible for monitoring and ensuring that all security procedures and controls for various applications are implemented.

5.0 Reference Documents

- ISO 27001:2022

ISO 27001 CONTROL NUMBERS	CONTROL TITLE
5.8	Information security in project management
8.4	Access to source code
8.25	Secure development policy
8.26	Application security requirements
8.27	Secure system architecture and engineering principles
8.29	Security testing in development and acceptance
8.30	Outsourced development
8.31	Separation of development, testing and production environments
8.32	Change management
8.33	Protection of test data