1. **Scope**

All of Retirement Capital’s software developments are covered in the scope of these procedures, including external development.

1. **Responsibilities**

The Chief Information Security Officer (CISO (DIRECTOR)) is responsible for securing the development environment against threats.

The Project Manager is responsible for the security of any given development project.

The Information Security Manager is responsible for overseeing the general security of the development process.

The Relationship manager is responsible for the security requirements in developments by external suppliers.

The software developers are responsible for ensuring that secure coding practices are followed and for reporting identified vulnerabilities.

The IT Department is responsible for ensuring the security of the development environment architecture.

1. **Procedure** (ISO27002 Clause 14.2)
   1. **Secure system engineering** (ISO27002 Clause 14.2.5)
      1. Retirement Capital adheres to the SEI CERT Oracle Coding Standard for Java, as all of our application programmes are Java based.

The detail of this can be found at:

<https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java>

* + 1. All new technology is tested on the test versions of the application to test for vulnerabilities and functional errors.
    2. All development procedures are reviewed on a quarterly basis.
    3. All sub-contractors used for application development will adhere to the SEI CERT Oracle Coding Standard for Java
       1. Sub-contractor compliance is reviewed quarterly by interview and possible on-site inspection.
  1. **Secure development environment** (ISO27002 Clause 14.2.6)
     1. Retirement Capital operates a test environment with strictly limited access that employs the same security controls and the production system. Access is controlled under ISMS-C-DOC 13.1.1, 13.1.3 and 13.1.3a.
        1. All data and code on the test system is treated as Restricted, transmission of data is via encrypted channel and access is controlled under ISMS-C-DOC 13.1.1, 13.1.3 and 13.1.3a.
        2. Patient identifiable test data will not be used and all test data adheres to the requirements of the Data Protection Act 2018.
        3. Development workstation are username/password protected and all interactions with the live and test environments are logged. Logs are reviewed monthly.
        4. Specific personal only are given access to the test and live environments.
        5. Where external organisations are given access to the test environment for software development purposes (including parent and sister companies), this is granted under strict conditions. Access can be suspended at any time and all activity is logged.
        6. Network Segregation: See ISMS-C-DOC 13.1.1, 13.1.3 and 13.1.3a
        7. Access control: See [ISMS-C DOC 9.1.1](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A9\ISMS-C_DOC_9.1.1.docm)
        8. XXX are used to monitor all activity and are review monthly or by exception.
        9. Backups: See ISMS-C DOC 12.3.1
        10. Movement of data and code to and from the environments; See ISMS-C-DOC 13.1.1, 13.1.3 and 13.1.3a
  2. **Outsourced development** (ISO27002 Clause 14.2.7)
     1. All outsourced software development is managed under strict quality control. Subcontractor management is defined in [ISMS-C DOC 15.1.2](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A15\ISMS-C_DOC_15.1.2.docm).
        1. All code developed by third parties specifically for Retirement Capital remains the property of the Retirement Capital group of companies along with all associated IPR.
        2. Adherence to [SEI CERT Oracle Coding Standard for Java](https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java) is mandatory for all sub-contractors and is audited at the start of the relationship and annually thereafter.
        3. Code received from third parties is quarantined before implementation into the test environment, third party test results are reviewed, and acceptance tests conducted.
        4. Security and quality control internal audits made by the supplier will be produced as evidence of compliance.
        5. Supplier test results will be provided by the supplier upon code delivery.
        6. All externally developed code commission by Retirement Capital group will be subject to escrow by the Retirement Capital group.
        7. Retirement Capital reserves the right to audit the development environment at any time and such is included in contractual agreements.
        8. Documentation will be delivered with the externally developed code.
        9. Retirement Capital remains responsible for compliance to procedures, if the quality of any supplier is unacceptable, the supplier will be replaced.
  3. **System security testing** (ISO27002 Clause 14.2.8)
     1. Security is tested by monthly review of the Syslog information that details all access and activity to the test and live environments, as required by [ISMS-C DOCs 14.2.1](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A14\ISMS-C_DOC_14.2.1.docm) and [5.2](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section5\ISMS_DOC_5.2.docm). Annual penetration testing is performed to validate externally facing security. See ISMS-DP DOC 19.7.

***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Chief Information Security Officer (CISO (DIRECTOR)) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |