1. **Scope**

All of *{OrganisationName}*’s software developments are covered in the scope of these procedures, including external development and e-commerce services.

1. **Responsibilities**
   1. The *{Webmaster}* is responsible for securing the website against external attack.
   2. The *{NetworkManager}* is responsible for the website’s connectivity.
   3. The *{FinanceDirector}* is responsible for the payment facilities, the shareholder information and the online trading facilities.
   4. The *[software developers]* are responsible for ensuring that secure coding practices are followed and for reporting identified vulnerabilities.
   5. The *{InfoSecManager}* is responsible for overseeing the general security of the development process.
   6. The *{ChiefInfoSecOfficer}* is responsible for securing the development environment against threats.
2. **Security requirements analysis and specification** 
   1. Statements of information security requirements are included in the requirements for new information systems, or enhancements to existing information systems.
   2. *{OrganisationName}* carries out a risk assessment (in line with [ISMS DOC 6](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Section_4-10/ISMS_DOC_6.docm)) at the requirements stage of specifying any new information systems, or enhancements to existing systems (irrespective of whether they will be bespoke systems or commercial off the shelf systems). Required controls are identified integrated into the [purchase decision], specification and purchase contract. The {InfoSecManager} is responsible for ensuring that required manual controls are designed and implemented.
   3. Application controls that ensure correct processing are also (where appropriate) considered at the design stage.
   4. Software is subject to testing and formal approval in line with [ISMS-C DOC 12](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_12.docm); non-compliant products are not accepted.
   5. *{OrganisationName}* accepts products tested and evaluated in line with [ ] without requiring further testing.]
3. **Securing application services on public networks**
   1. Information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.
   2. All information published on *{OrganisationName}*’s website must be approved by *[ ]*.
   3. Software, information and downloadable documents must pass the checks for accuracy, completeness, legality, quality, appropriateness *[and ]* that are set out in *ISMS-C DOC [ ]* (which include checks on input from outside *{OrganisationName}*) before they can be approved for release.
   4. All *[some, in which case specify which]* software, information and downloadable documents must be digitally signed *[how?]* before release.
   5. Online data collection is carried out as required in *ISMS-C DOC [ ]*.
   6. E-commerce services [part of ISO27002 Clause 14.1.2].
      1. The web service architecture is described in *ISMS-C DOC [ ]*.
      2. The configuration and operational requirements for the web service connectivity is in *ISMS-C DOC [ ].*
      3. The configuration requirements for the webservers are set out in *ISMS-C DOC [ ].*
      4. E-commerce payment facilities are credit-card based and provided *[online/through a manual service] [by external service provider subject to an external party agreement/internal facility configured how?]*. The client data capture and payment details requirements are set out in *ISMS-C DOC [ ]*.
      5. [*Anti-fraudulent activity controls*.]
      6. [*Procedures for protection of client data, preservation of privacy and privacy statement – refer to any work instructions that deal with configuration requirements necessary to effect these statements.*]
   7. Online trading [part of ISO27002 Clauses 14.1.2 and 14.1.3].
      1. *{OrganisationName}* sells/buys *[details of products/services]* online.
      2. *{OrganisationName}* trades *[only with known parties, who have previously entered into an online trading agreement/with any interested third parties]*.
      3. *{OrganisationName}* requires acceptance of its terms of business before trading commences.
      4. *{OrganisationName}* requires that its customers authenticate themselves by *[details]*.
      5. *{OrganisationName}* deals with non-repudiation of contracts by *[ ]* and digital signatures by *[ ]*.
      6. *{OrganisationName}* deals with tendering, bidding, and awarding contracts and the security issues therein by *[ ]*.
      7. Electronic information *[what?]* is encrypted *[how?]* before it is transmitted between *{OrganisationName}* and its suppliers/customers.
      8. Online transactions are handled as set out in *ISMS-C DOC [ ]*.
4. **Protecting application services transactions**
   1. Information involved in application service transactions is protected in line with Clause 4 above to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.
5. **Secure development policy**

[*You should describe {OrganisationName}’s approach to ensuring the security of developments. This should include policy statements covering the development lifecycle, including:*

* *the security of the development environment*
* *guidance on security in the development lifecycle*
* *security in the software development methodology*
* *secure coding guidelines for each programming language*
* *security requirements in the design phase*
* *security checkpoints in project milestones*
* *secure repositories*
* *version control*
* *required application security knowledge*
* *ensuring developers are capable of avoiding, finding and resolving vulnerabilities.*

*You should link each of these to a procedure describing the specific requirements.*]

[*The policy should also include a statement regarding the use of outsourced development and a requirement for equivalent security to be addressed in agreements with third party developers. (See ISO27002 Clause 14.2.7)*]

1. **System change control procedures**
   1. Changes to systems within the development lifecycle are controlled by the use of the formal change control procedures set out in ISMS-C DOC 12.
2. **Technical review of applications after operating platform changes**
   1. When operating platforms are changed, business critical applications are reviewed and tested in line with ISMS-C DOC 12 to ensure there is no adverse impact on *{OrganisationName}* operations or security.
3. **Restrictions on changes to software packages**
   1. *{OrganisationName}* does not seek bespoke modifications to commercial software packages.
4. **Secure system engineering principles**
   1. *[Describe your methodology for secure system engineering. Security should be designed into all architectural layers, and balance the information security requirements against the need for accessibility.]*
   2. *[Describe how frequently these principles and procedures are reviewed for security, relevance to emerging threats, and applicability to technological advances.]*
   3. *[Where possible, these principles are applied to outsourced information systems through contracts and supplier agreements.]*
5. **Secure development environment**
   1. *[Describe {OrganisationName}’s approach to securing the development environment, bearing in mind that it incorporates people, processes and technologies.]*

1. **Outsourced software development**
   1. *[Describe {OrganisationName}’s procedures for supervising and monitoring outsourced system development (see also* [*ISMS-C DOC 15*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_15.docm)*), including:]*
      1. *[Licensing arrangements, code ownership and the protection of intellectual property rights relating to the outsourced project]*
      2. *[Contractual requirements for secure design, coding and testing]*
      3. *[Providing the supplier with an approved threat model]*
      4. *[Acceptance testing of the deliverable]*
      5. *[Supplier provision of evidence that minimum security thresholds were used to establish acceptable levels of information security]*
      6. *[Supplier provision of evidence that the deliverable has been adequately tested against all known vulnerabilities]*
      7. *[Escrow arrangements]*
      8. *[{OrganisationName}’s audit rights over development processes and controls]*
      9. *[Documentation of the build environment]*
      10. *[Division of responsibility for compliance]*
2. **System security testing**
   1. *[Describe how systems are tested for security during development, including tools used for this purpose.]*
   2. *[Define the extent of testing requirements in accordance with the importance and nature of the system.]*
   3. *[Refer to acceptance criteria for the system or software, as well as project security milestones.]*
   4. *[Testing should also be conducted on received systems or components.]*
   5. *[Describe any requirements for external security testing.]*
3. **System acceptance**
   1. Acceptance criteria for new information systems, upgrades and new versions have been established and suitable tests of the system(s) are carried out during development and prior to acceptance, all as specified in ISMS-C DOC 12.
4. **Protection of test data**
   1. Test data is selected carefully, protected and controlled in line with ISMS-C DOC 12.

***Document Owner and Approval***

The *{FinanceDirector}* 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 *{OrganisationName}* members of staff on the *[corporate intranet]* and is published *[ ]*.

This procedure was approved by the *{ChiefInfoSecOfficer}* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |