**Systems Acquisition, Development and Maintenance**

**Doc A14**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 Systems Acquisition, Development and Maintenance 3

1.1 Scope 3

1.2 Responsibilities 3

2 Procedure 3

2.1 Information security requirements analysis and specification 3

2.2 Securing application services on public networks 3

2.3 Secure development policy, Secure system engineering principles and Secure development environment 3

2.4 System change control procedures 4

2.5 Technical review of applications before platform changes 4

2.6 Restrictions on changes to software packages 4

2.7 System security testing, System acceptance criteria and Protection of test data 4

3 Document Control and Approval 6

3.1 Distribution 6

3.2 Version Information 6

# Systems Acquisition, Development and Maintenance

## Scope

This procedure is applicable for ensuring information security is an integral part of information systems across the entire lifecycle of systems within the scope of the Information Security Management System as defined in the ISMS Manual.

## Responsibilities

The Risk and Compliance Team is responsible for defining the controls.

The CTO is responsible for the success of the controls by holding all staff accountable to implementing and following controls defined.

The application development management team is responsible for implementing the defined controls.

All employees, contractors and third parties have responsibilities to comply with the requirements of this procedure as defined below.

# Procedure

## Information security requirements analysis and specification

Any new application is evaluated, and appropriate security requirements defined.

The application product and development teams, in consultation with the Information Security Team, (and clients and external suppliers where necessary) define and produce the specification.

The specification forms part of the quotation if appropriate.

The new or revised system must not introduce any new security risks and be compatible with the current company security requirements.

Risk assessments are conducted as appropriate or reviewed to ensure that such systems are specified correctly.

## Securing application services on public networks

Cryptographic controls are applied to all applications which pass information over public networks.

## Secure development policy, Secure system engineering principles and Secure development environment

All development sprints have identified security requirements in accordance with the secure development policy. These requirements are reviewed at appropriate stages during the development lifecycle.

The development environment itself is accessible only by authorized users.

Software under development is stored in secure locations with limited authorized access.

Where development is outsourced, the source code will be held by Wacky Widget and where required, controlled access will be provided and managed.

Good security principles as defined in industry best practice are used at all times when not contrary to Company specific guidelines.

A contract must exist between the company and outsourced partner. The contract must include security and IP ownership requirements in accordance with the supplier relationships procedure.

## System change control procedures

Systems are changed as per the procedures set out in the quality management process Change Management Procedure.

## Technical review of applications before platform changes

Teams directly responsible for software development, review any changes to OS, code-based frameworks, and supporting software to determine if there is any adverse effect on applications prior to implementing on production systems. Testing is arranged as appropriate.

## Restrictions on changes to software packages

No changes to software packages should occur unless authorized by the Product Specialist.

## System security testing, System acceptance criteria and Protection of test data

Security testing is performed during the development stage and QA stage of the application. Testing is proportionate to and focused on the likely threats and vulnerabilities i.e. web applications may be tested more rigorously and for different risks than those for internal use only.

Product owners are directly responsible for ensuring that security tests are scheduled with the Risk & Compliance team. All releases which move into the production environment must be security tested in advance.

A summary of each finding should be uploaded onto a central tracking platform and assigned to the appropriate teams. All findings should be documented within a report and stored in accordance with its classification rating.

External penetration testing will be carried out by a qualified external 3rd party and will be tested against the production environment. The required cycle will be decided per application and based on a risk assessment and contractual obligations.

Live data is not used for testing purposes unless explicitly approved by the Chief Technology Officer. In this instance the access control procedures which apply to live production systems must also apply to test application systems.

Test data used is created solely for test purposes or is an anonymized version of the live data and must contain no actual personal information.

# Document Control 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 and is the published version.

This document was approved by Chief Technology Officer and is issued on a version controlled basis.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 