**ISMS Operations Security**

**Doc A12**

**Version: 1.0**

Publication Date: January 2019

Current Status: Published

Author(s): Michael Woolard

Reviewed By: Michael Woolard

**Table of Contents**

1 ISMS Operations Security 3

1.1 Scope 3

1.2 Responsibilities 3

2 Procedure 3

2.1 Documented operating procedures 3

2.2 Change management 3

2.3 Capacity management 4

2.4 Separation of development, testing and operational environments 4

2.5 Controls against malware 4

2.6 Information backup 6

2.7 Event logging, Protection of log information and Administration 6

2.8 Clock synchronization 6

2.9 Installation of software on operational systems. 6

2.10 Management of technical vulnerabilities 7

2.11 Restrictions on software installation 7

2.12 Information systems audit controls 8

3 Document Control and Approval 9

3.1 Distribution 9

3.2 Version Information 9

# ISMS Operations Security

## Scope

This procedure is applicable to all system operations within the scope of the Information Security Management System as defined in the ISMS Manual. All employees, contractors and third parties have to comply with the requirements of this procedure as defined below.

## Responsibilities

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

Asset owners and Internal IT teams are responsible implementing the controls.

# Procedure

## Documented operating procedures

Procedures or Work Instructions are developed as required to ensure the ISMS is operational

Such procedures follow the requirements of the ISMS manual and are available to all that need them.

## Change Management

The following standard changes are considered routine or insignificant and are therefore not subject to this procedure:

* PC Hardware upgrades
* Standard PC software installs upgrades
* Malware updates
* Operating system vulnerability patching and hot fixes
* Other Third party software vulnerability patching and upgrades

IT changes are identified in a Change Request ticket and logged.

Risk assessments are carried out where required by the change, but do not have to be formally documented within the ticket.

## Capacity Management

Key performance metrics are monitored with automatic alerting when pre-defined thresholds are exceeded.

Availability of production systems is monitored by Operations and relevant nominated contacts are notified should any breach of a threshold occur.

## Separation of development, testing and operational environments

Development, Testing and Production environments are separated logically.

This includes, but not limited to:

* Access by employees
* Deployment of code
* Data usage

## Controls Against Malware

The following controls have been identified and implemented to minimize the threat and damage that could be caused by a virus.

### Prevention

Proactive steps must be taken to prevent viruses from entering Company computers and workstations.

At a minimum Staff should ensure:

* Licensed software should be purchased only from reputable sources
* Software only acquired through the Wacky Widget Procurement process and include a review by the Internal IT Department.
* Access to programs and data should be restricted on a “need to use” basis
* All removable media should be scanned before it is accessed by any computer
* It is preferable not to leave removable storage media (USB data devices, CD/DVD) in the drive bay or attached to interface ports

### Notification

All Information Security weaknesses, events and incidents must be raised in the incident ticketing system as soon as they are seen or experienced in accordance with the Incident Management Procedure. Where this is not possible, the incident must be raised with a senior manager or executive.

### Detection

Antivirus software is installed on all servers, desktops and laptops.

Exceptions must be authorized by the Chief Technology Officer.

### Eradication

It is mandatory that all identified viruses be reported so that proper action is taken, documentation is maintained, and information shared.

If a virus is found:

* Stop using the computer immediately and disconnect from the network. Turn off wireless connection and unplug the network cable
* Isolate all removable media that have been used on the affected computer. These should NOT be used on any other computer
* Raise a ticket in help desk systems to inform the IT Department
* Note the symptoms and record any messages that appear on your screen
* Notify your Supervisor/Manager

### Recovery

Staff should ensure that all company work is saved to a network drive on a server which is backed up every night by the Internal IT Department.

The Internal IT Department will ensure that data backups are taken as per the published schedule and stored off site in a secured environment.

All backups should be scanned, prior to reloading on the system, to ensure that a virus is not present in any file on the backup.

The following procedures will be followed by the Internal IT Department to facilitate the recovery process:

* Software inventory records will be kept
* Original software media will be stored in a secure location
* Ensure that suppliers can be contacted quickly if problems occur

## Information backup

Certain files as defined by Internal IT, in consultation with others, are backed up according to the backup schedule.

A log of the back-ups is retained and checked periodically.

At least annually, production and Internal IT teams perform recovery testing to ensure the back-up process is functional, and a record of this test is retained.

## Event logging, Protection of log information and Administration

Web Application and System logs are enabled and are retained automatically. Records are maintained for a minimum of one month and reviewed periodically or in the event of an incident or breach.

The logs record (where possible) all authorization transactions:

* All account management activities
* Changes to access rights
* Access / modification to access logs
* All privileged operations
* System alerts or failures
* Changes to system security settings

The firewall is configured to alert Internal IT in the event of a significant intrusion event or incident occurring. The firewall logs are reviewed when an incident occurs or is suspected.

The logs are protected by password control and access is restricted to administrative users of the system.

## Clock synchronization

Clocks of all servers and network computers are synchronized to an internet time source.

## Installation of software on operational systems.

Only required software to maintain the production applications may be installed on production servers. Installation of software on servers is carried out by authorized trained staff.

## Management of technical vulnerabilities

A patch management process will be followed that proactively patches operating systems.

A decision on if and when to deploy each patch will be decided based upon:

* Prioritization according to criticality
* Balance of risk of deploying each patch compared to the criticality of the associated vulnerability
* Any patch deployment will follow standard change control processes.
* Operating System patches for workstations are deployed automatically from a central repository. Internal IT reviews the machines to ensure patches have been applied.
* Server patching is planned by Internal IT and rolled out according to this plan.

Anti-Virus is set to be patched automatically.

Internal IT reviews software supplier sites as appropriate to ensure that technical vulnerabilities are understood.

## Restrictions on software installation

The Company’s procedures must be followed when acquiring software from the Internet:

* Software acquired from the Internet must be pre-approved by the Internal IT Department before being installed on to company hardware
* Software should be obtained only from a known source to ensure it is a quality product and is free from tampering
* Software must be screened to ensure viruses are not introduced into the Company
* Payment must be made if required, and licenses verified for public-domain software
* Copyrights must be honored for software and other materials (for example, magazines, books, fonts) available on the Internet.
* Uploading of Company software / correspondence is not allowed unless authorized.

## Information systems audit controls

Where audits are conducted of the information systems, the requirements for access to systems and data is agreed with appropriate management and carefully planned to minimize disruption to business processes.

The scope of technical audit tests is agreed. The audit tests are limited to read-only access to software and data where relevant; access other than read-only is only allowed for isolated copies of system files, which are to be erased when the audit is completed so far as is practicable. Requirements for special or additional processing are identified and agreed where relevant.

# Document Control and Approval

The Chief Information Security Officer 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.

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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 