**ISMS Communications Security**

**Doc A13**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 ISMS Communications Security 3

1.1 Scope 3

1.2 Responsibilities 3

2 Procedure 3

2.1 Network controls and Security of network services 3

2.2 Remote access 3

2.3 Inter-office Network 3

2.4 Internet Connectivity 4

2.5 Segregation in networks 4

2.6 Wireless Networks 4

2.7 Information transfer policies and procedures 4

2.8 File transfers 4

2.9 Electronic messaging 4

2.10 Confidentiality or non-disclosure agreements 5

3 Document Control and Approval 6

3.1 Distribution 6

3.2 Version Information 6

# ISMS Communications Security

## Scope

This procedure is applicable to the protection of information in networks and the supporting information processing facilities within scope as defined in the ISMS Manual.

## Responsibilities

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

The Asset Managers are responsible for implementing the controls.

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

# Procedure

## Network controls and Security of network services

The network is controlled using approved tools.

## Remote access

All communications into the internal network from external public and private networks must take place over the company provided VPN connection.

## Inter-office Network

The Company offices are connected via secure network technologies. Connectivity to any Company network by non-secure means is not permitted.

Adequate network documentation and diagrams are maintained.

## Internet Connectivity

All communications between the Company and the Internet are allowed only through the network supplier chosen by the Company and only through the Company’s secure gateway.

Only those Internet services and functions with documented business purposes for this Company will be enabled at the Internet firewall.

Staff using the Internet are bound by the Acceptable Use Policy.

Staff are not allowed to:

* connect a personal device to the Internet over an access point connected to a company network; or

accounts or services obtained through the Company for official business cannot be used for personal use, either at home or from Company premises.

## Segregation in networks

Systems are hosted on separate network subnets.

Web servers and database servers must be hosted on separate networks.

Defense in depth is implemented via layered networks and restricted access between networks.

## Wireless Networks

Wireless communication to the internal Wacky Widget network is restricted by access controls managed by technologies utilizing Active Directory.

No shared password access controls may be used on wireless services that connect devices to the internal Wacky Widget network.

The wireless network must segment a guest network for access to public Internet only.

## File transfers

The Company allows the use of both unencrypted e.g. FTP and encrypted e.g. SFTP transfer mechanisms. It is the responsibility of the person initiating the transfer to ensure that they are using an acceptable method to protect the data being sent and that the method complies with the security policies of both the Company and the customer (where relevant).

Classification of the data must be set, and the transfer requirements of that classification must be understood, before sending the file.

## Electronic messaging

The network controls coupled with the firewall and other network security features help ensure the integrity and confidentiality of electronic messages.

Additionally, outgoing e-mail has a standard company confidentiality clause attached (in the e-mail footer).

# 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 