**ISMS Compliance**

**Doc A18**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 ISMS Compliance 3

1.1 Scope 3

1.2 Responsibilities 3

2 Procedure 3

2.1 Legal, Statutory and other requirements - General 3

2.2 Copyright 3

2.3 Trademarks 4

2.4 Data Protection and Privacy 4

2.5 Protection of Records 5

2.6 Independent review of information security 5

2.7 Compliance with security policies and standards 5

2.8 Technical Compliance Review 5

3 Document Control and Approval 6

3.1 Distribution 6

3.2 Version Information 6

# ISMS Compliance

## Scope

The compliance process described in this document is applicable to all Wacky Widget information assets and any information assets owned by a third party that Wacky Widget supports.

## Responsibilities

All employees of Wacky Widget are responsible for complying with this procedure.

The Internal IT Manager is responsible for software and system audits.

The Directors and Managers of Wacky Widget are responsible for retention of records.

# Procedure

## Legal, Statutory and other requirements - General

The Wacky Widget Legal team retain a list of applicable statutory and regulatory requirements (REC 18.1) relevant to the company’s information systems.

Annually, the Wacky Widget legal team will review this list, updating as appropriate and ensure that any activities undertaken do not contravene any of the regulations and statutes prevailing. Appropriate staff training, and awareness is provided as necessary.

Wacky Widget will protect its own and other parties' Intellectual Property through control over access to information and the proper licensing of information and software.

Wacky Widget ensures that it has licenses for all proprietary software that is installed on Wacky Widget information assets and maintains and monitors a software license register.

## Copyright

Copying (including duplicating and any other variant of the copying concept) of anything (whether document, digital asset, software, or anything else) other than in line with relevant copyright law is explicitly forbidden.

Software and other third party copyrighted items may only be obtained through legitimate suppliers, and only on the basis that the software or copyright license terms will be complied with, including as to numbers of users / basis of sale, etc.

Wacky Widget will maintain a software and copyright asset register together with copies of software licenses, etc.

From time to time, internal audits will be carried out to ensure no unlicensed software has been installed and that the maximum number of user licenses has not been exceeded.

Wacky Widget copyright ownership of documents (including drawings, charts, etc, owned or originated by Wacky Widget, or contributed to or originated by third parties under contract to Wacky Widget, including contractors, teleworkers and employees during their employment) should be established through contracts.

Wacky Widget copyright ownership of software (including code, code contributions, applications, etc, owned or originated by Wacky Widget, or contributed to or originated by third parties under contract to Wacky Widget, including contractors, teleworkers and staff during their employment) should be established through contracts.

Wacky Widget will ensure that it complies with all legal requirements relating to Copyrights.

Any use of unlicensed and improperly obtained software or unauthorized use of proprietary information whether belonging to Wacky Widget or a third-party is strictly prohibited and will be treated as a serious disciplinary breach.

## Trademarks

The Wacky Widget legal team will identify where it is appropriate for Wacky Widget to register trademarks.

All trademarks, whether or not registered, are listed and these will be managed by the Wacky Widget legal team.

The Wacky Widget legal team will take appropriate action, including legal action where necessary, to protect its trademarks from infringement.

## Data Protection and Privacy

Personal Data means data relating to a living individual who can be identified from that data

(or from that data and other information in our possession).

Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as performance appraisal).

Personal data is classified as Personally Identifiable Information (PII), and is available only to those who need to deal with it (see DOC 8.2 Classification and handling for further details)

Staff must not use or disclose Personal Data for a purpose other than the purpose for which the data was obtained.

All uses of this information should be notified to the Risk and Compliance Manager who maintains the Company’s official registration. All managers must ensure that they review and update the information on databases under their control annually.

Wacky Widget is committed to compliance with all national and, where appropriate, international laws relating to the protection of personal data and individual privacy.

All staff will be provided with training to ensure that they understand Wacky Widget policies and the procedures it has put into place.

The disciplinary process will be invoked in circumstances where policies may have been transgressed.

## Protection of Records

Records are retained as documented in REC A4.

## Independent review of information security

Wacky Widget conducts internal audits on the information security management system and retains records of such audits.

Any issues identified during audits are addressed as per the corrective action and improvement processes.

## Compliance with security policies and standards

Managers continuously review their area of operations for compliance and should any non-compliance be identified the manager determines the cause, evaluates the actions necessary, implements appropriate actions and reviews the outcome to ensure the non-conformance does not recur.

Where the manager notes a recurrence of minor infractions or where there is a potential breach or incident then the Manager records the issue either in a report to the Information Security Manager, an Incident Report or, if more appropriate, an internal departmental record.

Such reports are shared with auditors as appropriate during internal audits.

## Technical Compliance Review

Manual penetration testing is conducted by a 3rd party service supplier for some systems based on a risk assessment or customer requirement. Technical specialists in relevant teams review the reports and take appropriate corrective action. The managers directly responsible for products and / or software development in consultation with the Risk and Compliance team (as necessary) carry out the risk assessment and are responsible for this process for their products and / or software.

Automatic vulnerability scanning is conducted by a 3rd party service for some systems based on a risk assessment of customer requirement. Technical specialists in relevant teams review the reports and take appropriate corrective action. The Internal IT Manager is responsible for this process.

# Document Control and Approval

The Risk and Compliance 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 