**ISMS Objectives**

**Doc A5.1**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 ISMS Objectives 3

1.1 Scope 3

1.2 Responsibilities 3

2 Procedure 3

2.1 Information Security Objectives 3

2.1.1 Objectives and measures for ISMS implementation and maintenance 3

2.1.1.1 Compliance with ISO 27001:2013 3

2.1.1.2 Completion of scheduled events 3

2.1.1.3 Improvement of ISMS 3

2.1.1.4 Awareness program 4

2.2 Objectives and measures for ISMS performance 4

2.3 Additional Objectives and measures for ISMS Risk Treatment Controls 4

3 Document Control and Approval 5

3.1 Distribution 5

3.2 Version Information 5

# 

# ISMS Objectives

## Scope

This document sets out Wacky Widgets’s measurable objectives for information security.  These are used to provide management with information on the effectiveness of the ISMS.

All controls identified in the Statement of Applicability are within the scope of this procedure.

## Responsibilities

The Chief Information Security Officer is responsible for ensuring that ISMS objectives are measured, and that results are reported for management review

# Procedure

## Information Security Objectives

Achievement of these objectives will be monitored and measured on a regular basis.  Measures to be used are bulleted below each objective.  All measurements are recorded on a quarterly basis unless stated otherwise.

### Objectives and measures for ISMS implementation and maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| Compliance with ISO 27001:2013 | | | |
|  | Number of nonconformities to the standard raised during int/ext audits | | |
|  | | *Source:* | Internal and external audit reports and findings |
|  | | *Frequency:* | On-going as Internal and External are conducted |
|  | | *Target:* | All Minor Non-Conformities raised are addressed within 180 days  All Major Non-Conformities raised are addressed within 90 days |
| Completion of scheduled events | | | |
|  | Internal audits completed to schedule | | |
|  | | *Source:* | Quality Manager |
|  | | *Frequency:* | Scheduled based on a 3-year cycle, measured annually |
|  | | *Target:* | Audits completed on schedule |
|  | Internal audit coverage of all ISMS processes and controls at least annually | | |
|  | | *Source:* | Quality Manager; Valid ISMS, Internal Auditors |
|  | | *Frequency:* | Scheduled based on a 3-year cycle, measured annually |
|  | | *Target:* | 100% of all offices audited against 100% of controls every 3 years. |
|  | Review of ISMS completed at least annually | | |
|  | | *Source:* | Valid ISMS. Risk and Compliance team. Management review team |
|  | | *Frequency:* | At least annually |
|  | | *Target:* | Ensure that the ISMS remain in-line with the requirement of both the top level management and regulatory obligations. |
|  | Review of Risk Assessment completed at least annually | | |
|  | | *Source:* | Valid risk register; asset owners, accountable persons. |
|  | | *Frequency:* | At least annually |
|  | | *Target:* | Ensure that existing asset and supplier risk assessments are reviewed annually.  Ensure new risks are evaluated and added to the register. |
| Improvement of ISMS | | | |
|  | System improvements implemented via the Corrective Action process | | |
|  | | *Source:* | Internal and external audit reports and findings. Risk and Compliance team. |
|  | | *Frequency:* | As defined by the internal and external auditors |
|  | | *Target:* | Demonstrable improvement of the ISMS |
|  | Awareness improvements implemented via the Incident Management process | | |
|  | | *Source:* | Incident reporting system; Risk and Compliance team; staff awareness program |
|  | | *Frequency:* | As and when required (depending on incidents raised). |
|  | | *Target:* | To use output from reported incidents to drive the awareness program |
| Awareness program | | | |
|  | Percentage of employees completing annual ISMS awareness training | | |
|  | | *Source:* | Valid awareness program; lessons learned input; Incident reporting input; asset risk assessment input |
|  | | *Frequency:* | Continuous awareness for staff |
|  | | *Target:* | 100% staff 100% completion of all courses |

## Objectives and measures for ISMS performance

1. **Confidentiality**

* Number of confirmed security breaches relating to confidentiality

1. **Integrity**

* Number of confirmed security breaches relating to integrity

1. **Availability**

* System up-time as a percentage of service hours (monthly)
  + System backups completed as planned

## Additional Objectives and measures for ISMS Risk Treatment Controls

In addition to the aforementioned objectives, ISO/IEC 27001:2013 Annex A includes control objectives for risk treatment controls.  Where such controls are implemented, Chief Information Security Officer and the relevant risk owner decide the necessity for monitoring and measurement of the controls, and achievement of the objectives.

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

# 