**ISMS Organization**

**Doc A6.1**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 ISMS Organisation 3

1.1 Scope 3

1.2 Responsibilities 3

2 Procedure 3

2.1 Information security roles and responsibilities 3

2.2 Segregation of duties 5

2.3 Contact with authorities and special interest groups 5

2.4 Information security in project management 5

3 Document Control and Approval 6

3.1 Distribution 6

3.2 Version Information 6

Annex A 7

# ISMS Organization

## Scope

This document describes the Organization of the Information Security Management System (ISMS) within Wacky Widget (see Annex A for the names of the people associated with ISMS roles).

## Responsibilities

Directors and managers are responsible for ensuring the provisions of this document are understood and adhered to by all staff and others as appropriate.

The CISO acting in the role of Information Security Manager (ISM) is responsible for developing and maintaining this procedure.

# Procedure

## Information security roles and responsibilities

**Officers**

This term refers to Chief Officers of Wacky Widget. Officers are responsible for setting the overall strategy for Information Security within the Company including providing clear direction, demonstrated commitment and explicit assignment and acknowledgement of information security responsibilities.

**President**

The President has overall responsibility for information security including authorization of the Information Security Policy and requiring that all executives, directors, managers and staff are aware of this policy and adherence to its provisions and the information security management system that supports this policy.

The President is the only individual who can give can give approval for business specific exceptions to an ISMS policy as required.

Approval must be given by the President or the Chief Technology Officer before any of the Company’s data that is classified as Company Secret is transmitted outside of Wacky Widget.

**Chief Technical Officer (CTO)**

The Chief Technical Officer is responsible for ensuring that the systems are compliant with the information security management system and to keep informed on the threat environment.

The CTO is responsible for reviewing policies, agreeing on any changes to policy, and in particular, agreeing on all exceptions to the policy.

The CTO is the only individual who can give approval for technology specific exceptions to an ISMS policy as required.

Approval must be given by the President or the Chief Technology Officer before any of the Company’s data that is classified as Company Secret is transmitted outside of Wacky Widget.

**EVP, VP, GM, and Directors**

EVP, VP, and Directors are responsible for the adherence to policies by staff in their area of responsibility.

Directors are responsible for correcting any nonconformities or deficiencies in performance that are identified and for supporting or assisting with continuous improvement efforts of the ISMS.

**Information Security Manager (ISM)**

This term refers to the CISO acting in the role of Information Security Manager. This role may be backed by the CTO where necessary.

The Information Security Manager develops the Information Security Management system (ISMS), its objectives and strategy.

The ISM is responsible for

i) Ensuring that the information security management system complies with company requirements including compliance with ISO 27001

ii) Coordinating and managing the internal ISMS audits in consultation with the Quality System manager

iii) Coordinating and managing corrective actions and response to security incidents

iv) Reporting on performance of the information security management system to top management

Questions regarding the content or application of the ISMS should be directed to the Information Security Manager.

The Information Security Manager may grant a temporary exemption to the Information Security policy for up to 1 month where this is deemed an acceptable low risk.

**Quality Management System Manager (QMS)**

The Quality Manager is the “Management Representative”, as defined in ISO 9001, and has responsibility for monitoring the performance of the Quality Management System (coordinating the internal audits across the QMS and ISMS in consultation with the ISM manager) and reporting his / her findings in meetings with the various management groups as part of the Management Review.

**Internal IT Department**

The Internal IT Department is responsible for establishing the effective use of computer resources located in the Wacky Widget offices and by employees in the field.

The Internal IT Department may give technical approval for the use of non-company devices. An ISMS policy exception would still need to be approved by the CTO.

Managers in Internal IT can give permission for the removal of IT equipment from a Wacky Widget office.

**Managers**

Managers are responsible for ensuring that their staff, and contractors over which they exercise control, are aware of, and comply with, the information security policy and the supporting information security management system (ISMS).

Managers are responsible for correcting any nonconformities or deficiencies in performance that are identified and for supporting and assisting with continuous improvement efforts of the ISMS.

**Staff and contractors**

Staff and contractors are responsible for complying with the information security management system and policy.

Staff and contractors are also responsible for reporting information security weaknesses and incidents in line with company procedures.

## Segregation of duties

Duties are segregated according to the organization chart with staff members having their roles identified in contracts of employment and responsibilities laid out in supporting documentation. Users are only provided with access to the network and network services that they have been specifically authorized to use.

Developers, QA teams and all business teams are not allowed to have access to the production environment. An exception may be granted by technology leadership by the configuration management manager or higher, for emergency purposes only.

## Contact with authorities and special interest groups

Contact with authorities and special interest groups is maintained. These contacts are listed in *XYZ Document* *(usually a supporting BCP document of some sort).* The ISM maintains an overview of this listing and ensures it is kept up to date.

## Information security in project management

Projects must adhere to processes set out in the *XYZ Document (If you are also ISO9001 certified, that standard will have a project management process document in the QMS)*.

All projects must consider security aspects to ensure that information security risks are identified and addressed as part of the project.

In particular, for any new project, the Project Manager is required to ensure that information security objectives are included in project objectives. The project is subject to an information security risk assessment at the initiation of the project, in order to identify necessary controls.

Information security is reviewed at the relevant project reviews.

Responsibilities for information security should be defined and allocated to specified roles during the project initiation phase.

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

# 

# Annex A

The matrix below shows the names of the people associated with the ISMS roles defined above (correct at the time of publication).

|  |  |
| --- | --- |
| **Role** | ***Responsible Person(s)*** |
| Officers | John Smith Sr  John Smith  Jane Smith  Jolene Smith  John Smith Jr |
| CEO | John Smith Sr |
| President | John Smith |
| CTO | Jolene Smith |
| CISO / Information Security Manager | Mike Woolard |
| Internal IT | John Smith Jr |
| EVP, VP, GM, and Directors | Alvin Apple  Barry Banana  Carrie Cantaloupe  Paul Pear  Georgia Grape  Wally Watermelon  Olivia Orange |