**ISMS Manual**

**Doc A1**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 ISMS Manual 3

1.1 Terms and definitions 3

1.2 Scope Statement 3

1.3 Introduction to Wacky Widget 3

2 Management System 4

2.1 Context 4

2.2 Requirements of interested parties 6

3 Documentation 7

3.1 General 7

3.2 Control of Documented information 8

3.3 Management responsibility 9

3.4 Management commitment 9

3.5 Resource management 9

3.5.1 Provision of resources 9

3.5.2 Training, awareness and competence 10

3.6 Legal and other requirements 10

3.7 Internal ISMS Audits 10

3.8 Management review of the ISMS 10

3.8.1 Review input 11

3.8.2 Review output 11

3.9 ISMS improvement 11

3.9.1 Continual improvement 11

3.9.2 Corrective Action 11

4 Document Control and Approval 12

4.1 Distribution 12

4.2 Version Information 12

# ISMS Manual

## Terms and definitions

Terms used are those defined in standards wherever appropriate. The standards used as reference include ISO 27000.

In particular, the Information Security Management System (ISMS) is a set of interrelated and interacting elements to establish policies, objectives and processes to achieve those objectives. This includes structure, roles and responsibilities, planning and operation. It takes into account risk to the information and information processing as practiced by Wacky Widget and manages such risk in accordance with top management’s requirements.

## Scope Statement

The scope of Wacky Widget’s ISMS is:

Development and supply - from offices within the United States, Europe and India to the widget industry - of software products, information technology services and consultancy, technical data management services, and distance learning programs. In accordance with the latest version of the Statement of Applicability.

This includes:

* Information, other assets associated with information and information processing facilities managed by Wacky Widget.
* Services and Support provided to Clients.
* Data provided by Clients.
* All Staff and Contractors under the control of Wacky Widget.

Locations:

* Chicago
* Spain
* France
* India

## Introduction to Wacky Widget

Wacky Widget is a market leading provider of global solutions to the widget service market.

Operations is spread out among 6 offices, in 5 countries, on 3 continents.

The offices and operations in scope produce the widgets from top to bottom. The office left out of scope handle administration and call center functions of the business.

# Management System

## Context

Wacky Widget has clients, suppliers and other stakeholders. Interested parties are primarily those shown in the following figure. The context of the organization is as shown:

Outsourced service supplier

Clients (e.g. Manufacturers, traders or leasing companies)

Customers and End Users

Legal & Regulatory bodies

Partners /

Channels

Landlords

**Wacky Widget**

IT Suppliers

General suppliers

Staff

Board of Directors

Internet connectivity/

Comms.

Hosting suppliers

Consultants (Professional Services)

Shareholders

The internal processes are as follows:

* Marketing
* Sales
* Development
* Delivery
* Post Delivery
* Finance
* Legal & regulatory governance
* Strategy
* Governance

Internal processes and their interaction with external parties are shown below

## Requirements of interested parties

|  |  |
| --- | --- |
| **Interested party** | **Requirements of the interested party relevant to the ISMS** |
| External |  |
| Clients | Keeping client data secure (C, I and A)  Compliance with relevant legislation and regulations  Compliance with contract (SLAs etc.) and maintaining commercial relationship |
| Business Clients |
| Partners/ Channels |
| Regulatory bodies (ICO, geographic regulations) | Comply with relevant laws and regulations within that legal jurisdiction |
| Professional service suppliers | Act upon advice |
| Consultants |
| Professional services |
| Landlord | Comply with contract / agreement, be a ‘good’ tenant |
| Software licensing companies | Comply with copyright laws pertaining to software use |
| Internet connectivity/ ISP | Be Security compliant  Maintain Confidentiality  Duty of care  Inform them of correct processes & ‘rules’  Supply / disposal of equipment – supply chain  Clear contract for supply of goods and/or services |
| General suppliers |
| Cloud Based service suppliers |
| Hosting suppliers |

|  |  |
| --- | --- |
| **Interested party** | **Requirements of the interested party relevant to the ISMS** |
| Internal |  |
| Board of Directors | Complete service with accuracy, profitability and integrity  Comply with legal requirements  Protect the reputation of the organization  Protect company information (financial data, intellectual property etc.) |
| Staff | Duty of care  Provide policies, processes and relevant training  Provide systems, software and tools that are fit for purpose and provide feedback mechanisms where performance is not as required |

# Documentation

## General

Wacky Widget has defined a policy statement that addresses both information security and business continuity aspects. This policy is stated in DOC A5

Improvements in processes within the ISMS are made using an appropriate improvement model. The preferred model is the Plan-Do-Check-Act cycle explained as

**PLAN**

Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). When possible start on a small scale to test possible effects.

**DO**

Implement the plan, execute the process, and make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

**CHECK**

Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do".

**ACT**

Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product.

This cycle is repeated as necessary until the desired results are consistently achieved.

Although this is the preferred model, other improvement models may be used as appropriate.

High level objectives shown in the policy are supported by the following subsidiary objectives:

* Consistency in practices across the organization
* Ensuring information security is considered in defining and assessing Wacky Widget’s relationship with partners, suppliers, etc.
* Ensuring timeliness of reporting and response to incidents and non-conformities
* Continuing compliance with appropriate regulatory, legal, contractual and other relevant requirements.

These objectives will require, amongst other measures, that:

* Information security training is available to all staff and contractors
* All breaches of information security, actual or suspected, are reported and investigated.

The Statement of Applicability is contained in DOC SoA and includes control objectives and controls as identified as necessary both as deduced from the risk assessment and from other inputs.

To support the ISMS the following information is available in documented form:-

* Risk methodology and acceptance criteria
* Internal audit process
* Control of information (documents and records)
* Risk assessment
* Business Impact Analysis
* Measures of effectiveness
* Non-conformance, Corrective action and improvement processes
* Legal, Regulatory and other relevant requirements
* Other information as determined as necessary for the effective operation of the ISMS
* Records as relevant – records are protected and controlled as necessary to demonstrate effective operation and improvement of the ISMS

This information is documented as necessary within the ISMS system

## Control of Documented information

Documented information is controlled to ensure that it remains appropriate and up to date. The control process ensures it is available and suitable for use, where and when it is needed and that it is adequately protected (e.g. from loss of conﬁdentiality, improper use, or loss of integrity).

WACKY WIDGET ensures that distribution, access, retrieval and use is controlled and that the documented information is appropriately stored, preserved and legible. Changes to documents are controlled by version control and that obsolete information is prevented from use.

Documented information of external origin necessary for the planning and operation of the ISMS is identified as appropriate and controlled.

## Management responsibility

The Chief Executive Officer (CEO) is ultimately responsible for ensuring information security is maintained at Wacky Widget.

The Executive leadership, Directors and management of Wacky Widget are responsible for ensuring that their staff and those working under their control are aware of and follow the tenets of the information security policy and the supporting management system.

All staff are responsible for complying with the information security management system including reporting of information security events and incidents in accordance with procedures.

The Chief Information Security Officer is responsible for ensuring that the management system complies with this manual and the supporting documentation and reporting on performance to top management.

Please refer to the organizational chart on the Intranet for organization structure.

## Management commitment

Management are committed to the establishment, implementation, operation, review, maintenance and improvement of the ISMS

* A policy for information security is established
* Objectives and plans for the ISMS have been established
* Responsibilities for specific processes are clearly defined throughout the ISMS, and are documented in individual job descriptions or otherwise where necessary
* The importance of meeting objectives and conforming to the policy, its responsibilities under the law and the need for continual improvement is communicated to the organization
* Resources are provided to establish, implement, operate, monitor, review, maintain and improve the ISMS
* An acceptable level of risk has been decided for accepting risks
* Internal ISMS audits are conducted
* Management reviews the ISMS, including the policies
* Appropriate records of the above activities are retained.

## Resource management

### Provision of resources

The Chief Information Security Officer is responsible for the planning, implementation and control of the ISMS and reviews all relevant procedures to ensure that they are aligned and support the requirements of the business.

Management ensures that where controls are implemented, they are implemented correctly and achieve the level of security and business continuity required

Audits are performed to ensure those controls and processes which have been implemented are functioning as expected and actions taken where identified as necessary

Where improvements are identified, management ensures that these are actioned within an agreed time-frame.

### Training, awareness and competence

Management have identified the skills and knowledge required by all staff to ensure an effective ISMS.

Where there is a gap between the skills and knowledge available and the requirements determined, a training and awareness program is undertaken to close this gap.

Where a training or awareness program has been undertaken, it is evaluated to ensure that the required knowledge transfer has been successful.

Appropriate records of training are retained.

## Legal and other requirements

Wacky Widget identifies, and has access to, applicable legal and regulatory requirements relevant to the Management System and the interests of relevant interested parties. These legal, regulatory and other requirements have been taken into account in establishing, implementing and maintaining the Management System. This information is documented and kept up to date. New or variations to legal, regulatory and other requirements are communicated to affected employees and other interested parties.

## 

## Internal ISMS Audits

Management have put an audit program in place and all sections of the ISMS are audited at least once a year to ensure that the ISMS:

* conforms to the requirements of the relevant standards and any other legal, regulatory or contractual requirements
* meets all identified information security and business continuity requirements
* is effectively implemented and maintained
* performs as expected

A program of audits and audit information (such as audit reports) is retained for a minimum of two years after creation. Auditors are selected and assigned based upon identified competence and objectivity and impartiality regarding the subject audit.

## Management review of the ISMS

A review is undertaken at least once a year to review the ISMS. The review shall make recommendations for improvement which shall then be implemented and monitored by Wacky Widget. The ISM is responsible for ensuring this review is organized and recorded. The Senior Management receives the output from the review.

### Review input

To ensure an informed view, management shall review documentation including, but not limited to:

* results of ISMS audits and reviews including those of key suppliers and partners where appropriate
* feedback from interested parties
* techniques, products or procedures, which could be used in Wacky Widget to improve the ISMS performance and effectiveness
* status of corrective actions and improvements
* risks not adequately addressed in the previous risk assessments
* results from effectiveness measurements and objectives
* follow up actions from previous reviews
* any changes that could affect the ISMS
* recommendations for improvement and emerging good practice and guidance
* adequacy of policy and objectives.

### Review output

Management shall record decisions and actions related to:

* the improvement of the ISMS
* updating of the risk assessment and risk treatment plan as appropriate
* the modification of procedures and controls in response to changes in requirements
* resource needs
* improvements to how the effectiveness of controls and objectives are measured

## ISMS improvement

### Continual improvement

Management ensures that the ISMS is continually improved wherever opportunity arises.

### Corrective Action

Wacky Widget identifies non-conformities and takes appropriate action to eliminate the cause of the non-conformity. This is achieved by reviewing the nonconformity, determining the cause(s) of the nonconformity wherever possible, determining if similar nonconformities exist, or could potentially occur, evaluating the need for corrective action, determining and implementing corrective action needed, reviewing the effectiveness of any corrective action taken, making changes to the ISMS, if necessary.

Any action needed is implemented and such action reviewed for effectiveness including changes to the ISMS. Appropriate documented information on the action taken is retained.

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

# 