Logo, company name

Description automatically generated`

**Information Security Management System (ISMS) Manual**

ISO 27001:2013

Publication Date: September 25, 2021

Current Status: Published

Author(s): A.D.Jaliya

Last Reviewed: A.D.Jaliya

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version No: | Date : | Description : | Approved By: | Effected Date: |
| 1.0 | 27/09/2021 | ISMS Manual | Professor Lavanya | 29/09/2021 |

|  |  |
| --- | --- |
| Name | Designation / Role |
| Professor Vishwajith | Chairman |

**Table of Contents**

1 Introduction 3

1.1 Purpose 3

1.2 Scope of Certification 3

1.3 abbreviations, acronyms, and definitions 3

1.4 Management Commitment……………………………………………………………………4

2 establishing and maintanace of ISMS 4

2.1 asset identification and classification 4

2.2 Risk management guide lines 6

2.3 Statement of Applicability…………………………………………………………………….

2.4 Security Organization and Responsibilities……………………………………………………

*2.4.1 Management Review Forum…………………………………………………...*

*2.4.2 Information Security Forum……………………………………………………*

*2.4.3 Information Security Officer…………………………………………………..*

*2.4.4 Information Asset Owner………………………………………………………*

*2.4.5 Information Asset Users…*…………………………………………………….

2.5 Implementation Norms………………………………………………………………………….

2.6 Document And Data Control……………………………………………………………………

2.7 Internal Audits…………………………………………………………………………………..

2.8 Management Review……………………………………………………………………………

2.9 Training…………………………………………………………………………………………

2.10 Continual Improvement…………………………………………………………………………

3 Information Security Policies 7

3.1 Acceptable use policy 7

*3.1.1 Purpose………………………………………………………………………...*

*3.1.2 Scope…………………………………………………………………………..*

*3.1.3 Policy*………………………………………………………………………….

3.1.3.1 Acceptable Use……………………………………………………

3.1.3.2 Unacceptable Use…………………………………………………

3.2 Password Policy……………………………………………………………….

*3.2.1 Purpose……………………………………………………………………….*

*3.2.2 Scope……………………………………………………………………………*

*3.2.3 Policy…*…………………………………………………………………………

3.2.3.1 General……………………………………………………………..

3.2.3.2 Guidelines for Construction of Passwords………………………….

3.2.3.3 Passwords Protection Standards……………………………………

3.3 extranet policy 9

*3.3.1 Purpose………………………………………………………………………….*

*3.3.2 Scope…………………………………………………………………………..*

*3.3.3 Policy*…………………………………………………………………………..

3.3.3.1 Third Party Connection Request……………………………………

3.3.3.2 Third Party Connection Agreement………………………………..

3.3.3.3 Point of Contact……………………………………………………

3.3.3.4 Modifying or Changing Connectivity and Access…………………

3.3.3.5 Terminating Access………………………………………………..

3.4 router security policy 9

*3.4.1 Purpose………………………………………………………………………..*

*3.4.2 Scope………………………………………………………………………….*

*3.4.3 Policy*………………………………………………………………………….

3.5 network and vpn poicy 9

*3.5.1 Purpose………………………………………………………………………..*

*3.5.2 Scope…………………………………………………………………………..*

*3.5.3 Policy*……………………………………………………………………………

3.6 Clear Desk/ Cear Screen policy 10

3.6.1  *Purpose……………………………………………………………………….*

3.6.2 *Scope………………………………………………………………………….*

3.6.3  *Policy*…………………………………………………………………………..

3.7 access control policy 10

3.7.1  *Purpose…………………………………………………………………………*

3.7.2 *Scope…………………………………………………………………………..*

3.7.3  *Policy…*………………………………………………………………………..

3.8 electronic mali policy 10

3.8.1 Purpose 11

3.8.2 Scope 11

3.8.3  *Policy……………………………………………………………………………………..*

3.9 acceptable encryption policy 11

3.9.1 purpose

3.9.2 scope

3.9.3  *policy……………………………………………………………………………………….*

3.10 Mobile Computing/Laptop Policy………………………………………………………………

3.10.1  *Purpose……………………………………………………………………………*

3.10.2 *Scope……………………………………………………………………………...*

3.10.3  *Policy*…………………………………………………………………………….

4 Document operating procedure 12

1. **Introduction**

## Purpose

Tellida Information Security Management System is described in this paper (ISMS). Although most companies do not consider information security to be a core competence, it has evolved into a critical business enabler rather than just an IT choice. The capacity of the company to do business is jeopardised without a well-protected corporate network and other security measures. Any weakness may paralyse the company, stopping it from doing regular operations for days or weeks, resulting in a loss of revenue and profitability. The security risks to corporate assets are getting more complex. Advanced assaults use a variety of techniques to find, exploit, and spread network flaws. The implementation of a strict information security management system has become a corporate necessity.

Tellida is concerned with protecting its business assets from hostile acts that may have a detrimental effect on the company, in order to guarantee business continuity.

Tellida ISMS is concerned with maintaining the information base's three characteristics.

* Confidentiality – ensuring that information is accessible only to those authorized to have access
* Integrity – safeguarding the accuracy and completeness on information.
* Availability – ensuring that authorized users have access to information requires.

Tellida considers ISMS as a key component in its business operations and growth.

Following are the main executive goal of Tellida ISMS.

* Defining and executing processes and procedures to safeguard its company assets, such as deploying security solutions that enable strong and secure network infrastructures to protect assets and guarantee efficient business operations and business continuity.
* To keep track of and stay up with changing business needs and danger situations.
* Comply with legal and regulatory standards.
* To deploy security solutions that are both cost-effective and simple to use in order to achieve the aforementioned objectives.

## Scope of Certification

**ISO 27001 Certification Scope**

ISMS is responsible for providing information security services to Tellida's internal users in line with the ISMS statement of applicability. All business processes and resources connected with the information system utilised to deliver software development and maintenance are covered by the ISMS. The address of the office is:;

TELLIDA PVT LTD

32/2, Lauries Road,

Colombo 04.

Sri Lanka

This includes the communication support the LAN and up to where the client links terminated.

## Information Security Policy

Tellida is dedicated to the operation and continuous development of an Information Security Management System that is relevant to the organization's security risk.

* Maintain business continuity • Protect the confidentiality, availability, and integrity of our information assets
* Fulfill information security contractual obligations
* Comply with regulatory and legislative standards • Make employees aware of information security problems
* Prevent security breaches by taking proactive measures and implementing appropriate information security rules.

## Management Commitment

Tellida I's management has committed to implementing an ISMS in order to meet the company's information security objectives. Information security objectives must be defined in combination with business goals by management.

The management is committed to ensuring the security of information assets and will place a high priority on the establishment and implementation of a security-oriented corporate culture. Any security effort needs have active involvement from the user community and staff personnel to succeed. To ensure that security awareness pervades all levels of the company, top management should strive to offer continuous support to staff members and the information security forum. All resources needed for the formulation and successful implementation of ISMS must be provided by management. Management must attend management review meetings to assess the efficacy and appropriateness of the ISMS implementation and, if necessary, take corrective and preventative measures.

The internal processes are as follows:

• Management

• Threat Analysis

• Vulnerability Assessments

• Recommend Corrective Actions.

• Implementation Giddens

• Support and Continues Review



1. **Establishing and Maintenance of ISMS**
   1. Asset Identification and Classification

|  |  |
| --- | --- |
| Information assets | Databases, system documentation, training material, procedures, plans, information security records, contracts, guidelines, company documentation |
| Software assets | Application software, system software, development tools, utilities |
| Hardware and infrastructure assets | Computer equipment, media, buildings, furniture |
| services | Air condition, power, ISP |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Asset type | Rating | Security Parameter | | |
|  |  | Confidentiality | Availability | Integrity |
| Information asset | Low | It would be improper and inconvenient to provide information to an outside entity. | Unauthorized changes may be inconvenient and require extra work to restore integrity. | Due to a lack of availability, activities may be delayed, but there will be no external effect. |
| Information asset | Medium | Disclosure inside or outside would cause significant harm to the interest of the organization. | Unauthorized modification could have significant monetary impact on business and require significant additional effort re-establish integrity | Lack of availability could cause significant delay in execution of business activities with external impact |
| Information asset | High | Internal or external disclosure would jeopardize the organization's interests. | Unauthorized changes might result in severe financial losses as well as a loss of reputation and future business. | Failure to satisfy contractual criteria or monetary loss might result from non-availability. |
| Software asset | Low | Internally, unauthorized usage or licensing violation with minimal impact | Unauthorized modifications to a software asset's configuration have an impact on its use and need extra work to restore integrity. | Due to a lack of availability, regular company activities may be hampered, but there will be no external consequences. |
| Software asset | Medium | Externally, unauthorized usage or licensing breach with a modest impact | Unauthorized modifications to a software asset's configuration have an impact on its use and require a substantial amount of additional effort to restore integrity. | Lack of availability might create substantial delays in the execution of company activities, which could have a negative influence on the outside world. |
| Software asset | High | Externally, unauthorized usage or licensing breach with serious consequences | Unauthorized modifications to software assets and their configurations have a financial impact on the organization and need a substantial amount of additional effort to re-establish integrity. | Non-availability might result in a failure to satisfy contractual obligations or financial loss. |
| Hardware and infrastructure | Low | Physical access without authorization that has a limited impact on the company | Damage to the asset and its configuration has a negative influence on its use and necessitates more work and expense to restore integrity. | Due to a lack of availability, business operations may be delayed, although the impact on the firm will be limited. |
| Hardware and infrastructure | Medium | Physical access that is not allowed and has a minor impact on the business | Damage to the asset, or partial or whole loss of the asset, has a negative influence on its use and necessitates a substantial amount of additional time and expenditure to restore its integrity. | Due to a lack of availability, considerable delays in the execution of business operations might occur, with a moderate impact on the firm. |
| Hardware and infrastructure | High | Unauthorized physical access can have a big impact on your business. | Damage to the asset, or its partial or whole loss, has a monetary impact on the firm and necessitates a substantial amount of additional labor and expenditure to restore integrity. | Non-availability might result in a failure to satisfy contractual obligations or financial loss. |
| Services | Low | Unauthorized service access with little business effect | Inconvenience and minimal commercial effect arise from service misuse or inadequacy. | Due to a lack of availability, business operations may be delayed, although the impact on the firm will be limited. |
| Services | Medium | Unauthorized service access having a moderate effect on the business | Misuse or inadequacy of service with a minor impact on business | Due to a lack of availability, considerable delays in the execution of business operations might occur, with a moderate impact on the firm. |
| Services | High | Unauthorized access to a service may have a big impact on a company's bottom line. | Service misuse or inadequacy that has a major business impact | Failure to satisfy contractual obligations or financial loss might result from a lack of availability. |

A statement stating alone is suggested for any extremely sensitive material. It can only be accessed by those who are part of the distribution. If it is discovered by someone who is not on the distribution list, it must be returned to the owner immediately, along with the distribution list.

The owner of the sensitive or highly confidential information will be responsible for ensuring that the information is only shared with those on the distribution list who are authorized to receive it. All processes and departments must identify and categorize their assets. The asset inventory is evaluated by the information security forum on a regular basis, along with best practices.

* 1. Risk Management Guideline

Tellida's controls are based on the current list of assets and the risk associated with those assets. According to the Tellida risk assessment method, risks are identified and mitigated.

* 1. Statement of Applicability

The information security forum prepares the statement of applicability, which specifies the application of controls specified in the ISO 27001 standard as well as any other extra controls chosen. When the risk strategy is reviewed and amended, the statement of applicability is reviewed and updated.

* 1. Security Organization and Responsibilities

The following positions in the security organization will be established to define and guide the execution of security policies and procedures:

* Forum on management security
* Forum on information security
* Officer in charge of information security
* Owner of the data asset

* + 1. Management Review Forum

The MRF, which consists of the project manager or leaders, will be led by MR.The MRF's general tasks and obligations are as follows:

* Have overall responsibility for the definition and execution of the security policy, as well as reviewing and approving it.
* Approve the implementation of significant information security measures.
* Examine any new threats that may arise as a result of new technology or business practices, and analyze their impact on the company.
* Require frequent audits of the organization's information assets' security.
  + 1. information security forum
* The ultimate responsibility for administering the ISMS will be delegated to an information security forum comprised of information security managers, representatives, or project managers from each profession or function. The CEO will be in charge of this group.
* The information security forum's wide tasks include reviewing and approving the asset list and risk management strategy for all practices or functions.
* Define, manage, or support the deployment of the organization's ISMS, as well as monitor it.
* Assuring that workers, customers, and third-party service providers have access to specialist information security advice and training.
* New information assets are approved.
* Responding to the threat of securitization
  + 1. information security officer

A single officer will be in charge of the organization's full duty. This is intended to enhance security management activity ownership and coordination. The officer in charge of information security shall report to the CEO.

* The information security officer's wide responsibilities include developing and publishing standards, as well as providing counsel and assistance.
* Standards monitoring and coordination are required to meet the organization's security goals.
* Notifying the CEO of any security event or threat that may have an impact on the company's information assets and processes.
* Providing guidance to the CEO on remaining information security implementation issues
  + 1. information asset owner

Every asset in the company will have a designated owner. The owner will be in charge of preserving the assets in his possession. The organization's information assets must remain its sole property. The owner's responsibility is to accurately categorize assets according to classification standards in order to maintain adequate control over their use.

* These are the asset owner's day-to-day activities and responsibilities, which include identifying the safeguards that are required to secure information assets in conjunction with the information security forum and the head of practice or function.
* Ensure that proper security practices are followed in their area of responsibility, and that policies and procedures are followed.
  + 1. Information Assets Users

All organization workers are accountable for utilizing the organization's information assets in line with the ISMS's acceptable use policy. The ISMS rules and procedures must be understood by all workers. A security breach or event must be reported by all workers to their supervisor or information security officer.

* 1. Implementation Norms

The ISMS rules and procedures must be implemented by all practices and functions. When business operations need deviations from ISMS rules and procedures, the practice or function leader submits a request to the information security officer indicating the necessity for deviation. The risk, as well as any new controls that may be necessary, will be reviewed and approved by the information security officer in conjunction with the information security forum. The information security officer is responsible for keeping track of any deviations issued.

When a client has security needs that require different or extra controls than those listed in the ISMS, the information is transmitted to the inf.

* 1. Document and Data Control

The ISMS compromise;

* Information security manual
* Asset list / Risk management Plan
* Statement of applicability
* Guidelines
* Templates/ formats

All ISMS documents and records are defined, maintained and controlled in accordance with the defined process and guidelines.

* 1. Internal Audits

Every quarter, internal audits are done to ensure that information security processes comply with ISMS and ISO 27001 standards. The audits are carried out by trained internal auditors. Internal auditors who are not affiliated with the profession or function being audited are assigned to conduct the audit. Audits are planned and carried out in line with Tellida's internal auditing system.

In addition to these audits, management has chosen to become certified for ISO 27001 compliance. The auditing agency of choice will assign certified and experienced auditors to assess the appropriateness of the information security policy, ISMS, and its implementation in relation to the bus.

* 1. management review

Once a quarter, management reviews are done to ensure the ISMS's continued appropriateness, adequacy, and effectiveness. This assessment will entail determining where improvements may be made and whether or not adjustments to the ISMS are required.

The information security officer coordinates management reviews, which are led by the CEO. The management security meeting includes all practice leaders or function heads, as well as members of the information security forum.

The following items will be on the agenda for management review meetings:

* results of ISMS audit and reviews
* feedback from interested parties
* techniques, products or procedures, which cloud be used in the organization to improve the ISMS performance and effectiveness.
* Status of preventive and corrective actions.
* Vulnerabilities or threats not adequate address before
* Follow up actions from previous risk assessment review
* Any changes that could be effect the ISMS, recommendation for improvement.

The output of the management review shall include, any decisions and actions;

1. Improvement of the effectiveness of the ISMS
2. Modification of procedures that effect information security as necessary to respond to internal or external events that may impact on the ISMS, including changes to;
3. Business requirements
4. Security requirements
5. Business process effecting the existing business requirements
6. Levels of risk and levels of risk acceptance
7. Resource needs

The minutes of the meeting are calculated to all the management review participants. The information security officer tracks the access points to closure.

2.9 Training

Employees shall receive appropriate training on the security policy and procedures including security requirements, business controls and disciplinary actions which may result out on non-compliance. The trainings will cover appropriate use of IT facilities, security policy and other things. Employees shall be kept aware of any changes to the security policies and procedures of the organization.

Information security training requirements are identified by the practice or function head and information security forum and communicated to the training manager. Planning and execution of the training programs is in accordance with Tellida ISMS.

* 1. Continual Improvement

The organization will utilize the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventative measures, and management review to continuously enhance the efficacy of the ISMS.

The following methods are used to accomplish continuous improvement:

* Identification of root causes for non-conformities of the implementation or operation of the ISMS and taking appropriate corrective and preventive actions
* Identification of potential non-conformities their causes and implementing appropriate preventive actions
* Defining quantitative security goals and improve the ISMS to achieve the same.

All corrective and preventative activities, as well as their status and data relevant to security goals, must be tracked by information security officers. This information will be analyzed to see whether there has been an acceptable improvement in ISMS efficacy. During management reviews, the enhancement of ISMS efficacy was examined.

Security Goals

|  |  |  |
| --- | --- | --- |
| Matrix | Unix | Service level objectives |
| Incident call resolution duration | | |
| Catastrophic – S1 | Hours | 2hrs |
| Significant – S2 | Hours | 8hrs |
| Minor – S3 | Hours | 24hrs |
| Incident call response duration | | |
| Catastrophic – S1 | Hours | 5hrs |
| Significant – S2 | Hours | 4hrs |
| Minor – S3 | Hours | 8hrs |

|  |  |
| --- | --- |
| Security incident type | Description |
| Catastrophic – S1 | Unauthorized access, use, disclosure, modification or destruction of information or interference with system operations leading to substantial revenue or capital loss, third party liability, loss of reputation |
| Significant – S2 | Unauthorized access, use, disclosure modification or destruction of information or interference with system operations leading to moderate revenue, capital loss, third party liability, loss of reputation |
| Minor – S3 | Unauthorized access, use, disclosure modification or destruction of information or interference with system operation leading to insignificant revenues, capital loss, loss of reputation, third party liability |

1. Information Security Policies

3.1 Acceptable Use Policy

3.1.1 purpose

The goal of this policy is to define what constitutes appropriate computer equipment use at Tellida. These restrictions are in place to safeguard both the employee and Tellida, as improper use exposes Tellida to dangers such as malware assaults, network system and service breach, and legal difficulties.

3.1.2 Purpose

This policy applies to all Tellida employees, consultants, temporary workers, private sector employees, and other workers, including all personal connected. Tellida's equipment, whether owned or rented, is covered under this policy.

3.1.3 Policy

3.1.3.1 Acceptable Use

* While Tellida's IT department strives for a fair level of privacy, users should be aware that the data they produce on the corporate system is their own. Tellida network administration cannot guarantee the confidentiality of information stored on any Tellida network device due to the requirement to safeguard it.
* Employees are responsible for using their best judgment when it comes to personal usage. Individual functions are appropriate for establishing personal standards for using the internet, intranet, or extranet system. Employees should be directed by functional policies on personal usage in the absence of such regulations, and if they have any doubts, they should ask th
* Any information that consumers consider important or susceptible should be password secured or encrypted, according to Tellida.
* Authorized Tellida employees may monitor equipment, systems, and network traffic at any time for security and network maintenance purposes.
* Tellida reserves the right to conduct periodic network and system audits to ensure that this policy is being followed.
* To safeguard the confidentiality, integrity, and availability of this information, information asset owners should establish and implement procedures in line with ISMS.
* Passwords should be kept private, and accounts should not be shared. Passwords and accounts are the responsibility of authorized users.
* Policies and procedures apply to all users.

3.1.3.1 Unacceptable Use

Tellida employees are not permitted to engage in any conduct that is prohibited under local, state, federal, or international law while using Tellida-owned resources.

Violation of any person's or company's rights under trade secret, copy right, patent, or other intellectual property or similar laws or regulations, including but not limited to the installation or distribution of software products that are not legally licensed for Tellida's use.

Unauthorized copying of copy righted content, including but not limited to, but not limited to, but not limited to, but not limited to, but not limited to, but not limited

## 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

Controls are in place to guarantee that the documentation is accurate and up to date. The control process guarantees that it is available and acceptable for use when and when it is needed, as well as that it is sufficiently safeguarded (e.g., against loss of confidentiality, improper usage, or integrity loss). WACKY WIDGET guarantees that the recorded information is properly kept, conserved, and readable by controlling distribution, access, retrieval, and usage. Version control is used to keep track of changes to documents and to ensure that no material is used that is no longer relevant.

Externally sourced information that is required for the design and execution of the ISMS is identified as suitable and constrained.

## Management responsibility

The Chief Executive Officer (CEO) is ultimately accountable for safeguarding Wacky Widget's information security.

Wacky Widget's executive leadership, directors, and management are accountable for ensuring that their employees and those under their supervision are aware of and implement the information security policy and supporting management system's precepts.

All employees are accountable for following the information security management system's processes, which includes reporting information security events and incidents.

The Chief Information Security Officer is in charge of ensuring that the management system adheres to the guidelines in this handbook and the criteria

## 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 in charge of the ISMS's planning, implementation, and control, as well as reviewing all related processes to ensure that they are aligned with the company's needs. Management ensures that controls are applied effectively and that the requisite degree of security and business continuity is achieved.

Audits are conducted to check that the controls and processes that have been installed are working as intended, and that any actions that have been recognized as essential have been taken.

Management ensures that improvements are implemented within a set time limit when they are discovered.

### Training, awareness and competence

Management has determined the skills and information that all employees must possess in order to maintain a successful ISMS.

A training and awareness program is implemented to narrow the gap between the skills and knowledge available and the requirements specified.

When a training or awareness program is completed, it is reviewed to see if the desired knowledge transfer was accomplished.

Training records are kept in a proper manner.

## Legal and other requirements

## Wacky Widget recognizes and has access to applicable legal and regulatory requirements that are important to the Management System as well as the interests of interested parties. In developing, implementing, and maintaining the Management System, certain legal, regulatory, and other obligations were taken into account. This information is documented and updated on a regular basis. Affected workers and other interested parties are informed of new or changed legal, regulatory, and other obligations.

## Internal ISMS Audits

Management has implemented an audit program, and all components of the ISMS are audited at least once a year to ensure that it meets the following criteria:

fulfills all specified information security and business continuity needs is successfully implemented and maintained performs as intended complies to the requirements of the applicable standards and any other legal, regulatory, or contractual criteria

A program of audits, as well as audit information (such as audit reports), is kept for at least two years after it is created. Auditors are chosen and assigned based on their demonstrated expertise, objectivity, and impartiality in relation to the audit's subject.

## Management review of the ISMS

A review of the ISMS is carried out at least once a year. Wacky Widget will implement and monitor the recommendations for improvement that come out of the review. The ISM is in charge of ensuring that this review is well-organized and documented. The review's findings are delivered to Senior Management.

### 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 detects non-conformities and takes the necessary steps to eradicate the non-source. conformity's This is accomplished by reviewing the nonconformity, determining the cause(s) of the nonconformity, determining if similar nonconformities exist or could potentially occur, evaluating the need for corrective action, determining and implementing corrective action, reviewing the effectiveness of any corrective action taken, and, if necessary, making changes to the ISMS.

Any necessary action is taken, and its efficacy is evaluated, including modifications to the ISMS. The appropriate documentation of the action done is kept.

# 

# 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: 30.09.2021