Integrated Management System (IMS) Manual

Important Notes:

1. This manual has been documented around Mango Limited’s certified ISO 9001 and ISO 27001 Management System.
2. It is designed to meet the following international standards:
	1. ISO 9001
	2. ISO 27001
3. The secret, confidential and internal information has been removed from the original IMS manual. The information in this document is for public consumption.
4. It is a template only.
5. You should modify it to reflect your organisation.



Contents

[1 Introduction 5](#_Toc528585318)

[1.1 Company Overview, Context, Scope 5](#_Toc528585319)

[1.2 Integrated Management System (IMS) Structure 7](#_Toc528585320)

[1.3 Process Flow 10](#_Toc528585321)

[2 Leadership 11](#_Toc528585322)

[2.1 Leadership and Commitment 11](#_Toc528585323)

[2.2 Organisation Roles, Responsibilities and Authorities 13](#_Toc528585324)

[2.3 Quality Policy 16](#_Toc528585325)

[2.3 Information Security Policy 17](#_Toc528585326)

[3 Risk and Opportunity 18](#_Toc528585327)

[3.1 Actions to Address Risks and Opportunities 18](#_Toc528585328)

[3.2 Legal and Other Requirements 20](#_Toc528585329)

[3.3 Objectives, Target and Plans 21](#_Toc528585330)

[4 Support 22](#_Toc528585331)

[4.1 Resources, Assets and Infrastructure 22](#_Toc528585332)

[4.2 Recruitment, Training, Competency, Discipline, Termination and Knowledge Management 24](#_Toc528585333)

[4.3 Communication, Consultation and Awareness 27](#_Toc528585334)

[4.4 Documented Information and Control of Documents 28](#_Toc528585335)

[5.0 Operations – Marketing 30](#_Toc528585336)

[5.0.1 Marketing - How to Publish a Blog 30](#_Toc528585337)

[5.0.2 How to Manage Webinars 30](#_Toc528585338)

[5.0.3 How to Publish Release Notes 30](#_Toc528585339)

[5.0.4 Reporting End of Month Marketing Lead Performance 31](#_Toc528585340)

[5.1 Operations – Sales and Partnering 32](#_Toc528585341)

[5.1.1 Sales 32](#_Toc528585342)

[5.1.2 Partner Process 32](#_Toc528585343)

[5.2 Operations - Development 33](#_Toc528585344)

[5.2.1 Developers Documentation 33](#_Toc528585345)

[5.2.2 Development Requests and Bugs 34](#_Toc528585346)

[5.2.3 Mango Application 36](#_Toc528585347)

[5.3 Operations – Support and Testing 37](#_Toc528585348)

[5.3.1 Mango Testing 37](#_Toc528585349)

[5.3.2 Communication of Releases 38](#_Toc528585350)

[5.3.4 Support 39](#_Toc528585351)

[5.3.5 Implementation 40](#_Toc528585352)

[5.4 Operations - Accounting 41](#_Toc528585353)

[5.5 Operations - Information Security – A5 Information security policies 42](#_Toc528585354)

[5.6.1 Information Security Policy 42](#_Toc528585355)

[5.6 Operations - Information Security - A6 Organisation of information security 43](#_Toc528585356)

[5.6.1 Information Security Responsibilities 43](#_Toc528585357)

[5.6.2 Mobile Devices Policy 44](#_Toc528585358)

[5.6.3 Remote Working Policy 45](#_Toc528585359)

[5.6.4 Mobile Device Procedure 46](#_Toc528585360)

[5.7 Operations – Information Security – A7 Human Resource Security 47](#_Toc528585361)

[5.7.1 Human Resource Security 47](#_Toc528585362)

[5.8 Operations - Information Security - A8 Asset Management 48](#_Toc528585363)

[5.8.1 Asset Management 48](#_Toc528585364)

[5.8.2 Acceptable Use Policy 50](#_Toc528585365)

[5.9 Operations – Information Security – A9 Access Control 51](#_Toc528585366)

[5.9.1 Access Control Policy 51](#_Toc528585367)

[5.9.2 Access Control 52](#_Toc528585368)

[5.10 Operations – Information Security – A9 Cryptography 55](#_Toc528585369)

[5.10.1 Cryptographic Controls 55](#_Toc528585370)

[5.11 Operations – Information Security – Physical and environmental security 57](#_Toc528585371)

[5.11.1 Physical and environmental security 57](#_Toc528585372)

[5.11.2 Clean Desk Policy 58](#_Toc528585373)

[5.12 Operations – A12 Operations Security 59](#_Toc528585374)

[5.12.1 Operations security 59](#_Toc528585375)

[5.13 Operations – Information Security – A13 Communications Security 63](#_Toc528585376)

[5.13.1 Communications Security 63](#_Toc528585377)

[5.14 Operations – Information Security - System acquisition, development and maintenance 65](#_Toc528585378)

[5.14.1 System acquisition, development and maintenance 65](#_Toc528585379)

[5.15 Operations – Information Security - Supplier Relationships 67](#_Toc528585380)

[5.15.1 Supplier Relationships 67](#_Toc528585381)

[5.16 Operations – Information Security - Information Security Incident Management 68](#_Toc528585382)

[5.16.1 Information Security Incident Management 68](#_Toc528585383)

[5.17 Operations – Information Security - Information security aspects of business continuity management 69](#_Toc528585384)

[5.17.1 Business Continuity Planning 69](#_Toc528585385)

[5.18 Operations – Information Security - Compliance 70](#_Toc528585386)

[5.18.1 Compliance 70](#_Toc528585387)

[6 Supplier and Contractor Management 71](#_Toc528585388)

[6.1 Supplier Evaluation and Control 71](#_Toc528585389)

[7 Performance Evaluation 73](#_Toc528585390)

[7.1 Monitoring, Measurement and Evaluation 73](#_Toc528585391)

[7.2 Audits and Inspections 74](#_Toc528585392)

[7.3 Management Review and Operations Meeting 75](#_Toc528585393)

[8 Improvement 76](#_Toc528585394)

[8.1 Improvement and Corrective Actions 76](#_Toc528585395)

# 1 Introduction

## 1.1 Company Overview, Context, Scope

Established in 2002, Mango Limited delivers the application Mango to our clients to manage their compliance requirements.

Mango enables our clients to easily meet their compliance and certification requirements.

Compliance could be against the requirements of legislation, regulations and/or standards.

The legislation, regulations and standards includes:

* Quality (ISO 9001)
* Health and Safety (ISO 45001, AS/NZS 4801, OHSAS 18001, Country and State legislation, regulation and codes of practise)
* Environmental (ISO 14001)
* Information security (ISO 27001)
* Food industry specific (ISO 22000, HACCP, BRC, RMP, Tesco, Woolworths, Coles, Waitrose etc.)
* Shipping (ISM Code)
* Medical (ISO 13485)
* Manufacturing (GMP)
* Local Councils (Building Consent Accreditation)

Mango is sold to clients either via a Partner network or directly by Mango Limited. There are Mango Partners are in the following countries:

* New Zealand
* Australia
* South Africa
* United Kingdom
* United States

Mango Limited is committed to providing:

* Great software
* Great marketing
* Great support

In supporting this commitment, we have developed an Integrated Management System (IMS) to act as a framework for the business and as a model for continuous improvement.

This IMS will serve to formalise the policies, processes and operating standards that will apply to all employees, partners, suppliers and contractors.

**Context and Issues**

Mango Limited determines the external and internal issues that are relevant to its purpose and strategic direction and that affect its ability to achieve the intended results of the IMS.

Consideration is given to the:

* Positive and negative factors or conditions.
* External context and issues, such as legal, regulatory, technological, competitive, cultural, social, political and economic environments.
* Internal context and issues, such as values, culture, organisation structure, knowledge and performance of the business.
* Determination and requirements of the needs and expectations of interested parties relevant to the IMS.
* Authority and ability to exercise control and influence.
* Activities, products and services relevant to the business.

Documented information is retained as evidence to support that the context of the organisation has been taken into account in the IMS.

**System Scope**

The IMS describes how the Mango Limited requirements are to be addressed throughout its operations and addresses the requirements of ISO 9001:2015 and ISO 27001:2013.

Mango Limited's health and safety requirements are also managed in Mango but is not part of the system scope.

The scope is: "Provision of marketing, sales, support, development and implementation of SaaS software solutions and the supporting security operations"

**Location**

Unit 5, 340 Durham Street North.

Christchurch

New Zealand

**References and classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 4.1 4.2 4.3 | 4.1 4.2 4.3 | Public |

## 1.2 Integrated Management System (IMS) Structure

**Interaction between processes of the Integrated Management System (IMS)**

Mango Limited's IMS complies with the requirements of ISO 9001 and ISO 27001 and consists of the following levels of documented information:

* Policies.
* System management procedures.
* Control, Mango Modules workflows, operational procedures and work instructions.
* Forms, registers and records.

A diagram of the structure of the IMS structure is presented below.



Policies are documents that demonstrate the overall commitment to improving quality performance and are authorised by the Directors.

System management procedures are documents that define the activities that are to be fulfilled to ensure that an IMS that complies with ISO 9001 and ISO 27001 is established, documented, implemented and continually improved.

Control and operational procedures are documents that have been developed to:

* Meet customers’ requirements.
* Provide supplementary guidance and instructions to support the intent of the IMS.
* Ensure that the requirements of the IMS will be adequately addressed within the organisation.

Forms and registers are documents that need to be completed when complying with the IMS.

**Information Security Registers**

The information security asset, classification and risk structure is detailed as:

1. Asset Register
	1. Assets are detailed in the Plant/Equipment module in Mango.
	2. These assets are categorised into:
		1. Software
		2. Computer CPU
		3. Monitor
		4. Network
		5. Office Equipment
		6. Phones
		7. Tablets
	3. An owner is assigned to each asset and is held responsible for managing the asset.
2. Information Classification Register
	1. Outputs from the assets will be listed in this register and a classification applied.
	2. The classification will be:



1. Information security risk register
	1. The risks and the associated vulnerabilities are listed in a risk register.
	2. Any associated controls from ISO 27001 Annex A will be listed on the register.



**Mango compliance software solution**

* Provides automated workflows for the effective and efficient operation of the IMS.
* Underpins the IMS and serves as the main retention application for all documented information.
* Workflows and modules replace written procedures and forms associated with the process.
* They include the following:

|  |  |
| --- | --- |
| **Module** | **Actions** |
| Accident/Incident | Controls all near miss, accident, incident or injury reporting. The workflow securely manages the process including corrective and preventive actions. |
| Audit/Inspection | Controls the internal audit process. Actions from the process automatically update other modules |
| Compliance | Controls the compliance items the company needs to meet. These include Legislation, Regulations, Standards, Codes of Practise |
| Documents | Controls and securely maintains the approval, publication and status of all documentation within the module. |
| Environmental/Incident | Controls spills, discharges and incident reporting, recoding and investigation. The workflow securely manages the process including corrective and preventive actions. |
| Event Management | Control mechanism to ensure time-based critical activities can be managed, monitored and records kept. |
| Human Recourses | Controls employee's competency, qualifications, training records, PPE, health monitoring, access rights and document acknowledgements. Security restrictions on information are applied in this module. |
| Improvement | Controls any recording, investigation, corrective action and preventive actions for any improvements. The workflow securely manages the lifecycle of the process. |
| Plant/Equipment | Controls and manages the company's assets. |
| Risk Management | Controls the identification, assessment and management of risks. The workflow securely manages the process. |
| Supplier | Securely controls all external suppliers’ details. Their performance is captured and reviewed. |
| System Administration | Controls the setup and maintenance of the modules including employee access rights. |

Where a process or requirement can't be managed within the Mango Software other software solutions can be used to manage specific processes and procedures

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 4.4.1 | 4.4.1 | Public |

## 1.3 Process Flow

**Purpose and Scope**

To describe the interaction of process through the customer journey.

**Process**



**Reference and Classification**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 0.3.1 | 0.1 | Public |

# 2 Leadership

## 2.1 Leadership and Commitment

**Purpose and Scope**

To define how the Company demonstrates leadership and commitment to its IMS, it's customers and information security.

**Associated Documents**

Position Descriptions

**Procedure**

Leadership and Commitment

1. The managers will take responsibility for the ensuring the effectiveness of the IMS and will demonstrate their commitment to the IMS by:
	1. Defining roles, allocating responsibilities and accountabilities, and delegating authorities, to facilitate effective IMS management.
	2. Roles and Responsibilities are documented in IMS - Leadership - Organisation Roles, Responsibilities and Authorities and through position descriptions, and any IMS policies and procedures where applicable.
	3. Ensuring:
		1. That relevant policies and objectives are established for the IMS and that these are aligned with the context and strategic direction of the Company.
		2. The integration of the IMS requirements into the organisation's business processes.
		3. That resources needed for the IMS are available.
		4. The IMS achieves its intended results.
		5. The process approach and risk management is promoted.
		6. Communicating the importance of effective management and of conforming to the IMS requirements.
		7. Engaging, directing and supporting personnel to contribute to the effectiveness of the IMS.
		8. Improvement is promoting.
		9. Other relevant management roles are supported to demonstrate their leadership as it applies to their areas of responsibility.

Customer Focus

1. Management is committed to our customers and enhancing customer satisfaction. This commitment is demonstrated by:
* Ensuring that applicable customer and statutory requirements are determined, understood and met throughout the business.
* Ensuring the risks and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed.
* Exercising due care with our customer's property (data) whilst it is under the control of the company (refer Privacy Policy, Security Statement, End User Agreement and documented procedures within the ISM manual).
* Monitoring customer's perceptions of the degree to which their needs and expectations have been fulfilled.
* The methods for obtaining, monitoring and reviewing this information can include:

|  |
| --- |
| Support questions received directly or via support within the software. |
| Listening to customers voice |
| Pingdom Software alert |
| Measure outages for availability of service to the customer. |
| Bugs fixes and product enhancement from customer request |
| Release notes including enhancement requested by customers |
| Post implementation communication  |
| Monitor the customer post -implementation |
| Video Data |
| Measures the customer inaction with Mango around compliance knowledge delivery |
| CRR (Customer Retention Rate) data  |
| Measure the retention of customers |
| Mango usage data |
| The deployment of Mango within a customer account and aid in assisting partner to deliver targeted help. |

1. The key aspects of the customer information and data generated through the effective implementation of the IMS processes are collected and collated by the Management Representative and Information Security Officer presented at each Management meeting.

Information Security

Management is committed to protecting information assets. As information security risks and the effectiveness of controls change depending on shifting circumstances, Management is committed to:

1. Monitoring and evaluating the effectiveness of implemented controls and procedures;
2. Identify emerging risks to be treated; and
3. Selecting, implementing and improving appropriate controls as needed.

**References:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 5.1.1, 5.1.2, 5.3, 5.5.3 | 5.1.1, 5.1.2, 5.3, 8.5.3 | Public |

## 2.2 Organisation Roles, Responsibilities and Authorities

**Purpose and Scope**

To describe the responsibilities and authorities for the Company’s IMS and to define the organisation structure for the effective operation of the IMS.

**Associated Documents**

Job/Position Descriptions.

Employee Agreements.

Human Resources Module.

Access Rights Sub-Module.

**Procedure**

General Requirements

1. The responsibility, accountability and authority of all personnel involved in the IMS are defined, documented and communicated in order to facilitate effective IMS. This is to include any responsibilities and accountability that is imposed by legislation.
2. Responsibilities, accountabilities and authorities are documented in both position descriptions and throughout the IMS in policies and procedures.
3. Where suppliers are involved, their responsibilities and accountabilities are to be clarified and documented by the responsible employee with the appropriate authority.
4. All employees and suppliers will comply with their responsibilities.

The Senior Management are to:

1. Ensure organisation-wide compliance to the IMS.
2. Appoint the IMS Management Representative.
3. Ensure that the assigned roles, responsibilities and authorities are communicated and understood.
4. Communicate the importance of meeting customer, statutory and regulatory requirements.
5. Establish appropriate policies that include a commitment to continual improvement of the IMS.
6. Establish IMS objectives.
7. Ensure that persons doing work are aware of:
	* All Policies.
	* Current IMS objectives, targets and plans.
	* The importance of compliance with the IMS.
	* Their contribution to the effectiveness of the IMS, including the benefits of improved performance.
	* Potential consequences of non-compliance with the IMS requirements.
8. Hold people accountable for carrying out assigned responsibilities and the results delivered.
9. Make resources available.
10. Participate in IMS meetings including the Management Review.
11. Utilise Mango for the effective control of the IMS.
12. Actively promote and participate in IMS initiatives.

The Management Representative is to:

1. Ensure that the:
* IMS is established implemented and maintained in accordance with the requirements of the ISO 9001 and ISO 27001.
* IMS processes are delivering their intended outputs.
* Promotion of customer focus and information security throughout their Company.
* Integrity of the IMS is maintained when changes to the IMS are planned and implemented.
1. Report on the performance of the IMS for review and as a basis for continual improvement.
2. Perform the role of Mango Administrator which has the authority to ensure access rights in Mango, for individuals, are in-line with their levels of authorities and responsibility in the organisation.
3. Monitor, communicate and incorporate changes in the legal and other requirements in the IMS.
4. Communicate amendments to the IMS.
5. Advise and provide guidance to ensure compliance to the IMS is maintained.
6. Provide guidance in developing action plans and conducting management system reviews.
7. Ensure that audits and inspections are conducted in accordance with the schedule.
8. Ensure that Mango is effectively utilised to administer and control the IMS.
9. Provide and or arrange for ongoing training and coaching to personnel with respect to IMS matters.
10. Coordinate and participate in IMS meetings including the Management Review.
11. Publish and control all IMS documents.
12. Actively promote and participate in IMS initiatives.

The Information Security Officer is to:

1. Facilitate compliance with ISM policies and procedures
2. Liaise with the Management Representative on security matters
3. Complete security-related risk assessments as required
4. Complete client's security policy questionnaires
5. Complete regular security and compliance reporting
6. Assist with protection of information assets, and client's private data
7. Manage the security awareness campaigns
8. Ensure security of business applications, appropriate access control, incident management handling, and logging and monitoring of system activity
9. Perform internal systems/process control audits and drive action plans to mitigate risks
10. Communicate with co-workers, team members, management, clients and others in a courteous and professional manner.
11. Conform with and abide by all regulations, policies, work procedures and instructions.
12. Coordinate and administer arrangements with the certification body.

Employees are to:

1. Ensure that the IMS is effectively implemented and maintained within their area of responsibility.
2. Actively encourage all personnel to contribute towards the continual improvement of the IMS.
3. Incorporate the IMS as part of site and departmental inspections and reviews.
4. Determine and escalate the need for resource requirements for the effective operation of the IMS.
5. Participate in IMS meetings including the Management Review.
6. Utilise Mango for the effective control of the IMS.
7. Actively promote and participate in IMS initiatives.
8. Promptly report any unsafe working conditions, faulty equipment, hazards/risks, injuries and security issues or incidents.

Suppliers are to:

1. Comply with the requirements of the IMS and participate in IMS promotions.
2. Promptly report any unsafe working conditions, faulty equipment, hazards/risks, injuries and security issues or incidents.

Organisation Structure

1. The Company recognises that the structure of the organisation needs to constantly evolve in order to meet the changing needs of clients, the market and our compliance obligations.
2. The Directors are responsible for ensuring the structure of the organisation is appropriate to the current business needs and will ensure that the organisation chart is regularly reviewed and maintained.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 5.1.1, 5.3, 7.3 | 5.1.1, 5.3, 7.3 | Internal |

## 2.3 Quality Policy

Mango Limited is committed to providing and delivering the customer great product, great support and great marketing to make the management of our customer's compliance an easy and enjoyable experience.

We are committed to:

* Meeting legal requirements.
* Continually improving our Quality Management System.
* Meeting the needs and expectations of interested parties.

To achieve this we will:

* Provide our customers with a quality product for the management of their compliance needs.
* Provide our customers with free content, information and industry insight to improve their compliance knowledge.
* Provide timely and accurate support to our customers
* Listen to our customers when developing and enhancing Mango.
* Provide an environment where staff can grow and learn new skills.
* Provide a return to shareholders

We will measure our progress through:

* Setting objectives
* Documenting plans
* Reviewing performance

We will enable this by:

* Training our employees
* Training our Partners
* Improving Mango
* Investing in resources
* Investigating new technologies

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 5.2.1 5.2.2 |  | Public |

## 2.3 Information Security Policy

The information security policy provides an overarching governance for the security and management of information.

Information will be classified according to an appropriate level of confidentiality, integrity and availability.

Management and Employees, with particular responsibilities for information, handle information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.

Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.

The company is committed to adhering to all current legislation as well as a variety of regulatory and contractual requirements.

The company has set information security objectives.

The company is committed to the continual improvement of the information security management system.

Information security policies and objectives will be regularly reviewed during management meetings and during internal audits.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 27001** | **ISO 27001** | **Classification** |
|  | 5.2 | Public |

# 3 Risk and Opportunity

## 3.1 Actions to Address Risks and Opportunities

**Purpose and Scope**

To describe the manner in which risks and opportunities are managed the within the business.

**Associated Documents**

Risk Management Module.

Supplier Module.

Events Management Module.

Human Resources Module.

Organisation Context.

**Procedure**

General Requirements

1. The Company is committed to identifying and addressing relevant risks and opportunities as a means for:
* Increasing the effectiveness of the IMS.
* Improving performance.
* Preventing or mitigating negative effects.
* Protecting information assets against the loss of availability, confidentiality and integrity.
1. When undertaking risk management activities the Company must give consideration to the:
* Positive and negative factors or conditions.
* External context and issues, such as legal, regulatory, technological, competitive, cultural, social, political and economic environments.
* Internal context and issues, such as values, culture, organisation structure, knowledge and performance of the business.
* Determination of the requirements and needs and expectations of interested parties relevant to the IMS.
* Authority and ability to exercise control and influence.
* Activities, products and services relevant to the business.
1. The Company may adopt any or a combination of the following risk options:
* Avoid the risk.
* Eliminate the risk source.
* Take the risk to pursue an opportunity.
* Change the likelihood or consequences of the risk.
* Share the risk.
* Retain the risk by informed decision.
1. Opportunities identified may lead to:
* Adoption of new and improved processes.
* Launching new products or services.
* Pursuing new markets.
* Utilising new technology.
* Improved ways of addressing customer needs.
1. Risk and opportunities will be managed by:
* Ongoing effective leadership and commitment to the IMS.
* Discussing risks and opportunities in the Board meeting and at Management meetings.
* Effective management and control of suppliers and contractors.
* Effective training of personnel to ensure they are competent to perform relevant tasks safely.
* By monitoring, measurement and review of relevant processes and outputs.

Risk and Opportunity Process

The Risk Management module in Mango will step through the process for identifying, analysing, evaluating and treating risks and opportunities. The risk criteria includes the acceptance criteria and the criteria for performing information security risk assessments.

Risk registers are documented in Mango.

The Improvement module in Mango will step through the process for identifying, analysing, evaluating and treating opportunities.

The improvement register in Mango will list these opportunities.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 4.1, 4.2, 6.1.1, 6.1.2 | 4.1, 4.2, 6.1.1, 6.1.2, 6.1.3  | Internal |

## 3.2 Legal and Other Requirements

**Purpose and Scope**

To describe how the Company ensures that it has identified, complies with and verifies compliance with all of the relevant legislative, regulatory and other requirements that apply to the activities conducted by the company employees and contractors within its operations.

**Associated Documents**

Compliance Module

**Procedure**

General Requirements

1. The Directors are to ensure that all relevant legislative and other requirements are identified.
2. Legislative and other requirements may include, but are not limited to:
* Acts and Regulations.
* Codes of Practice.
* Guidelines.
* Standards.
* Agreements with clients, communities or public authorities.
* Corporate requirements.
* Industry standards or codes.
* Voluntary commitments.
1. Details of all relevant legislative and other requirements are to be contained within the Compliance Module. These will include mitigations and control methods. The verification of compliance will be reviewed by the Board.

Monitoring Changes

1. The Directors are to ensure that where possible, they are notified of changes and/or additions to legal and other requirements as those changes occur.
2. The means of ensuring notification of changes and/or additions may include:
* Agreements with external legal or consulting organisations to monitor and advise of changes.
* Registering with Standards New Zealand.
* Advice from employer or industry associations.
1. When changes and/or additions occur they are to be included in the Compliance module and the means of verifying compliance is to be defined as previously described.
2. A review of the Compliance module will be conducted as per the annual work plan in the Board meeting. These will include:
* Confirm that all updates to applicable legal and other requirements have been captured and included.
* Confirm that the means of ensuring and verifying compliance are appropriate.
1. The Directors are to ensure that all changes, additions and updates to the Compliance module are communicated to relevant employees, contractors and other stakeholders.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 4.1, 5.1.1 | 4.2, A18.1 | Internal |

## 3.3 Objectives, Target and Plans

**Purpose and Scope**

To define the processes for establishing measurable objectives and targets, for establishing plans to achieve those objectives and targets and for periodically monitoring performance in achieving each objective and target.

**Associated Documents**

Mango Data

Management Review Minutes.

Objective, Target and Plans Form

**Procedure**

General Requirements

1. The Company will establish measurable objectives and targets in relation to its performance.
2. The established objectives and targets must be:
* Consistent with the applicable Company policies.
* Measurable.
* Monitored and updated.
* Effectively communicated to relevant parties.
* Ensure they meet Information Security requirements.
1. Once measurable objectives and targets have been established, plans for achieving those measurable objectives and targets are to be established.
2. Performance in achieving each measurable objective and target are periodically monitored at Management meetings.
3. The company will create the following plans:
* Annual budget (Financial year)
* Sales and Marketing Plan (Calendar year)

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 5.1.1(b), 6.2.1, 6.2.2, 6.3 | 6.2, 8.1, 9.3 | Internal |

# 4 Support

## 4.1 Resources, Assets and Infrastructure

**Purpose and Scope**

To describe how the resources, assets and infrastructure are used to establish, implement, maintain and continually improve the effectiveness of the IMS and to protect the information security.

**Associated Documents**

Plant/Equipment Module

Acceptable use policy

Mobile devices policy

**Procedure**

General Requirements

1. Resources include:
2. Human resources
3. Infrastructure
4. Technology, and
5. Financial resources.
6. Assets will include information assets and all other assets. Note: an information asset is a body of knowledge that is organized and managed by Mango. Information assets have financial value.
7. The Directors will provide the organisational infrastructure, technology and financial resources. They are to review the adequacy of the resources as part of BOD meetings. As new technology becomes available, the possibility of introducing it to improve the IMS will be considered.
8. The Directors are to prioritise the financial resources available and allocate them to the various departments to provide the resources needed.
9. The Management Representative is to identify the resources required to establish and maintain the IMS.
10. Each department is to identify the resources required and to provide adequate support when planning work. They are to identify the infrastructure needed to implement and continually improve the IMS and meet requirements.
11. Directors will determine and maintain an appropriate work environment needed to achieve conformity to the product or service requirements and to the security of the information assets.

Purchasing of Resources, Assets and Infrastructure

All resources, assets and infrastructure will be approved at the BOD meeting. If it is deemed critical or requires major expense, it may appear on CAPEX register.

On receipt of the information asset it will be entered into the Plant/Equipment module and will have an Asset Number attached/assigned to the asset.

Inventory of Assets

1. Details of information assets used by Mango that can display, transmit, reproduce and communicate with external sources will be recorded in the Plant /Equipment module.
2. The information assets will be assigned to an Owner and will display an Asset number.
3. Annually Mango will conduct an audit of information assets.
4. The details will include:
5. Name
6. Asset Number
7. Serial/Rego Number
8. Supplier of the Plant/Equipment
9. Issued to
10. P/E category
11. Location information
12. When an asset is purchased it is recorded in the Plant/Equipment and who it was issued to.
13. When a person leaves the list of assets assigned to them will be reviewed and the items returned.
14. Assets will be then reissued or disposed of.
15. The Plant /Equipment will be updated with the new person or if to be disposed will be suspend. If an asset is to be disposed of a record of how it was disposed of is recorded (notes in the Plant/Equipment module) before suspending it.
16. When an assets has been issued, the person must comply with the Acceptable Use Policy and Mobile Devices Policy.

Repairs

All repairs must be carried out:

1. In accordance with any regulatory and the original manufacturer’s requirements.
2. By appropriately trained, qualified, competent and experienced personnel.
3. All records of maintenance are recorded on the suppliers invoice

Return

When an Employee leaves:

1. All resources, assets and infrastructure used by Employees are to be returned prior to leaving their employment.
2. Access to the organisation storage removed
3. Access to systems restricted
4. Passwords will be reset
5. Keys will be returned
6. Records of these activities will recorded on the exiting form.

Re-use

1. If the asset will be re-used it will be:
2. Cleaned
3. Repaired
4. Updated with data removed and/or deleted.
5. The assets record will have a note added of what was done.
6. If the asset is to be removed from use but re-gifted, the asset will be returned to factory sets and all data removed.
7. If the asset is to be removed from use and to be disposed of, the asset will be returned to factory sets, all data removed and destroyed.

Building security

Mango offices are secured to prevent unauthorised access. The offices are alarmed.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5 | 7.1, A8.1.1 A8.1.2 A8.1.4 | Internal |

## 4.2 Recruitment, Training, Competency, Discipline, Termination and Knowledge Management

**Purpose and Scope**

To ensure all relevant personnel are adequately trained, competent and informed in accordance with their position and IMS requirements.

**Associated Documents**

Position (Job) Description

Individual Employment Agreement

Induction Checklist

Human Resources Module.

Event Management Module.

Police Screening Forms

**Procedure**

Recruitment

Once a vacancy has been identified by the Board, the process for employing staff shall comprise the following steps:

1. Ensuring job description identifies key competencies appropriate to the position.
2. Advertise the role
3. Evaluate applicant’s suitability for vacancy by assessing the documentation supplied by applicant identifying relevant skills in line with the job description.
4. New applicants shall be assessed in a formal interview.
5. Suitable candidates will be screened with background verification checks performed with two referees. The background verification checks will be carried out in accordance with relevant laws, regulations and ethics. The Manager shall take into account the business requirements, the classification of the information to be accessed and the perceived risks.

Commencement and Induction of New Employees

1. Before a new employee commences work, the employee's Manager conducts induction training with the induction checklist.
2. During the induction any training needs will be identified and logged in Mango.
3. Once completed the induction checklist must be signed and dated by both the new employee and the employee’s manager.
4. Employee setup in Mango
5. A record of the induction is to be maintained in Mango.

Initial Employee Assessment

1. The initial employee assessment is conducted using Mango and involves the following steps:

* The employee’s manager assesses the employee’s competency against the skill set that has been established within the Skills/Qualifications Module in Mango.
* The employee and the manager agree current competency and future training needs.
* The Skills/Qualifications Module for that employee is updated by the employee’s manager or delegate. Any supporting records are also loaded into Mango at this time.
* The next review date for any further assessment of the employee's competency and training needs is to be scheduled in the Mango Events Management Module. Mango will automatically generate an email advising the manager and employee of the next review.
* Scheduled training is also able to be captured within the Mango Events Management Module, if necessary.
* The employee’s manager is to ensure that training identified is undertaken, and whilst under training the employee is appropriately supervised, as may be required.

Employee Competency and Training Needs

1. The employee’s manager is responsible for conducting:
2. 90 day performance reviews.
3. Ongoing performance reviews.

Further assessment of employee competency and training needs.

1. The further assessments of employee competency and training needs are conducted using Mango and involves the following steps:
* Upon email notification by Mango, the manager will conduct an assessment of the employee.
* The employee and manager agree current competency, review training undertaken during the previous year and evaluate the effectiveness of it and decide on future training needs.
* The Skills/Qualifications Module for that employee is updated by the Manager. Any supporting records are also loaded into Mango at this time.
* The next review date for assessment of the employee's competency and training needs is to be scheduled in the Mango Events Management Module.
* Scheduled training is also able to be captured within the Mango Events Management Module, if necessary.
* The Manager is to ensure that training identified is undertaken, and whilst under training the employee is appropriately supervised.

Disciplinary Procedures

The disciplinary procedure is described in the Individual Employment Agreement. The section: "Resolving Employment Relationship Problems" details the necessary actions.

Termination and change of employment

The termination and change of employment procedure is described in the Individual Employment Agreement. The section: "Termination of Employment" details the necessary actions.

Training Providers

1. In-house training is to be conducted by appropriately skilled and competent trainers with relevant experience, depending upon the subject matter.
2. Training may be performed on behalf of Mango Limited by suitably trained, qualified and experienced external service providers.

Knowledge Management

The following items are how we capture knowledge:

* Management meetings
* Scrum meetings
* Weekly development meetings
* Weekly marketing meetings
* Use of Wiki by the development team
* Use of Mango by all staff and partners
* Use of CRM and Marketing platforms
* Use of bug tracking software
* Use of accounting system
* Use of online training portal

We capture this knowledge in each of these tools and share it amongst the company to ensure the knowledge is used in giving the customer value.

We review the effectiveness and efficiency of these sources monthly in the Management Review.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 7.2, 7.3, 8.4 | 7.2, 7.3, A7.1.1, A7.1.2 | Internal |

## 4.3 Communication, Consultation and Awareness

**Purpose and Scope**

This outlines the framework for communication, consultation and awareness with employees, suppliers, contractors and external parties in relation to IMS issues and initiatives.

The main objectives are to ensure personnel at all levels and functions are:

* Are aware of IMS requirements and are effectively involved in the development, implementation and review of policies and procedures.
* Consulted when there are any changes that affect the workplace and or IMS systems.

**Associated Documents**

Management Meeting Minutes

Event Management Module

Scrum Meeting Records

Partner Communication Module

**Procedure**

Communication of IMS Information with the Board

The IMS and legal requirements are communicated and discussed at the board level. The BOD minutes record what items have been discussed and actions to be done. Where required actions will be assigned to the Monthly Operations Meeting and Management Meeting.

Communication and Awareness of IMS Information with Internal Parties

1. The IMS communication and consultation processes will occur at the monthly management meetings run by the Management Rep and attended by all employees.
2. The meeting details are here: Integrated Management System (IMS) Manual - Performance Evaluation - Management Review
3. An email from Mango will notify the owner when meetings are due and will be signed off the event including relevant evidence attached.

The company has ad-hoc meetings support the consultation processes:

|  |  |
| --- | --- |
| **Forum** | **Attended by** |
| Development Meeting | Development Team |
| Scrum Meetings | Development Team + Management |
| Marketing Meeting | Marketing Department (usually weekly) |
| Support | Support Team + Management |
| Operations Meeting | Support + Marketing + Management (usually monthly) |
| Partner Meetings | Partners + Management |

The company uses Mango to formally communicate changes to the product with the Partner Communication Module.

Communication and Awareness of IMS Information to External Parties

The company will communicate information externally about its IMS performance based on their enquiry.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 5.1.1, 5.2.2, 7.3, 7.4 | 5.1, 5.2, 7.4, A5.1.1 | Internal |

## 4.4 Documented Information and Control of Documents

**Purpose and Scope**

To describe the methods to control and manage documented information critical to the IMS.

**Associated Documents**

Records

Mango Documents Module.

Mango Improvement Module.

Developers Documentation

Operations Security (Backup)

**Procedure**

General Requirements

1. Documented information includes manuals, policies, procedures, work instructions, forms, registers, flow charts, records and other IMS document requirements.
2. The Management Representative is responsible for ensuring that all IMS documented information is effectively controlled.
3. All employees are responsible for ensuring they are always up to date with all IMS documented information available through Mango.
4. Copies of procedures, policies and other documented information may be printed from Mango, but these printouts will be deemed "uncontrolled", unless the form Mango is printed and completed as part of the process this will become a record.
5. To prevent the unintended use of obsolete documented information, superseded documents are automatically identified and removed from general view through the Mango workflow. Obsolete documents are only able to be accessed by personnel, with the required access levels, through the "History" button in the Mango Documents Module.

Editing, Approval, Publishing and acknowledge of Documents

The Documents module workflow manages the following document control activities:

* Creation and editing
* Approval
* Publishing
* Acknowledge
* Retention of previous version
* Revision numbering
* Control of approvers and publisher.
* Notifications

The Mango FAQ describes the process in more detail.

Requests for changes

All requests for changes to policies or procedures are raised as an improvement once the IMS has become live.

Notification of Changes

1. When a change is made or new document added, personnel are able to be notified by email automatically generated through Mango at the time of publication.
2. Changes can also be communicated via monthly meetings as deemed appropriate.
3. Changes to all IMS documents can be tracked through the Document Change History Sub Module in Mango.

Maintenance of IMS Documents

1. All IMS documents are to be reviewed at least once every three years, revised as necessary and approved for adequacy.
2. This review is to be coordinated by the Management Representative in conjunction with the relevant competent and responsible personnel as determined by the Management Representative at the time of review.

External Documents

1. It is the responsibility of the Management Representative to review, implement and maintain external documents and verify that they remain current.
2. External documents are kept in the Manage Files Module in Mango or managed on Dropbox.
3. All external documents are verified as current and when necessary have their distribution controlled through Mango.
4. The Management Representative subscribes to relevant external regulators, agencies and bodies who may provide periodic advice of changes to their specific documents. Upon receiving advice of changes to an external document the Management Representative will action this change in Mango and ensure the change is communicated to relevant parties.

Records Management

1. IMS records are retained in Mango for as long as the company uses the Mango Software solution.
2. IMS procedures and forms are maintained within the Mango Documents Module.
3. Access to working files are maintained by the Directors.
4. Records associated with financial transactions are held within the accounting package.
5. Our marketing platform has marketing documentation including leads lists, website CMS and marketing automation.
6. We use an online video programme for video control.
7. We use source code control.
8. We use bug tracking software.
9. The Management Representative is responsible for the management of records with respect to the IMS.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 6.1.1, 7.5.1, 7.5.2 | 7.5 | Internal |

# 5.0 Operations – Marketing

## 5.0.1 Marketing - How to Publish a Blog

**Purpose and Scope**

To describe how the company publishes a blog.

**Procedure**

Step 1 - Create image for blog

Step 2 - Clone previous blog

Step 3 – Create Blog

Step 4 – Edit the Settings section

Step 5 – Publish or Schedule

## 5.0.2 How to Manage Webinars

**Purpose and Scope**

To describe how the company manages a webinar. This includes, pre and post webinar steps.

**Procedure**

Pre-Webinar

Step 1 -Create webinar in Go-to-Webinar

Step 2 - Integrate the webinar

Step 3 - Create Landing Page

Step 4 - Create an Email invitation to attend webinar

Step 5 – Webinar Presenter arranges planning

Post Webinar

Step 1 - Transport Webinar Recoding

Step 2 - Create Lists – attendees and non-attendees

Step 3 - Create a blog with webinar recording

Step 4 - Email a recording of the webinar to each list

## 5.0.3 How to Publish Release Notes

**Purpose and Scope**

To describe how the company publishes release notes so customers/evangelists are aware of any new Mango updates. This procedure takes place once Support gives marketing the release notes.

**Procedure**

Step 1 – Create a new Mango News

Step 2 – Disable previous release notes news

Step 3 – Upload the FAQ into Mango (Support may assist with this)

Step 4 – Send out email to customers/evangelists to inform them of release

## 5.0.4 Reporting End of Month Marketing Lead Performance

**Purpose and Scope**

To describe how to report on the marketing leads at the end of each month. Reporting on this allows us to keep track on how marketing is performing.

**Procedure**

Step 1 – Open up spreadsheet of leads

Step 2 – Get numbers of leads

Step 3 – Record the numbers on spreadsheet

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.1, 8.2 |  | Internal |

# 5.1 Operations – Sales and Partnering

## 5.1.1 Sales

**Purpose and Scope**

To describe how the company controls and Manages sales enquiries.

**Procedure**

Step 1 - Receipt of Leads

Step 2 - Verifying of Leads

Step 3 - Demo

Step 4 - Negotiation

Step 5 - Won

Step 6 - Closed/Lost Disengaged

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.1, 8.2 |  | Confidential |

## 5.1.2 Partner Process

**Purpose and Scope**

To describe the steps in the partner process.

**Procedure**

At the end of each step the Lead is notified.

Step 1 - Partner Enquiry

Step 2 - Partner Pack

Step 3 - Demo

Step 4 - Agreement

Step 5 - Sales and Marketing Plans

Step 6 - Training

Step 7 - Support, Monitoring and Communication

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.1, 8.2 |  | Confidential |

# 5.2 Operations - Development

## 5.2.1 Developers Documentation

**Purpose and Scope**

To describe where and how the development team maintain shared technical information.

**Associated Documents**

Mango Wiki

**Procedure**

The development team maintain a Wiki.

The CTO determines what information will be maintained in the Wiki to enable the development team to

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.3 | 8.1 | Confidential |

## 5.2.2 Development Requests and Bugs

**Purpose and Scope**

To describe now development requests and bugs are managed and controlled.

**Associated Documents**

Dev Request Module.

Support Module.

MRS (Mango Requirement Specification)

**Procedure**

Please add you own design and development procedures.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.3 | 8.1, A14 | Confidential |

#

# 5.3 Operations – Support and Testing

## 5.3.1 Mango Testing

**Purpose and Scope**

To describe the procedures/processes for testing updates prior to release.

**Procedure**

1. Feature is raised for development or bug fix
2. Feature is scheduled
3. Feature is coded and committed to test environment
4. Create Test plan
	1. Where the development dictates, a comprehensive test plan will be created
	2. Where there is minor work, no test plan is required
5. Test development against the Feature
	1. Where the testing fails, document the issues and change status to 'Failed Test'
	2. Where testing has been successful, document testing completed
6. Release notes written
7. Code committed to live environment
8. Testing completed again in live environment
9. When the testing is successful, close the issue

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.3 | 8.1, A14 | Confidential |

## 5.3.2 Communication of Releases

**Purpose and Scope**

To describe the communication of Mango releases and updates.

**Procedure**

1. Testing has been completed and passed
2. Download list of items for release.
3. Insert additional information as required to clarify
4. RSS Created and Updates communicated to Partners
5. FAQs updated and FAQ Release notes written
6. List of items relevant for client communication sent to Marketing.
7. Marketing Releases Mango News and sends out email with notes written
8. FAQ and Release notes published

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 7.4 | 7.4 | Internal |

## 5.3.3 Support

**Purpose and Scope**

To describe the procedures/processes for responding to support queries.

**Procedure**

1. Query received from Client
2. Make contact with client and supply information as required
3. Update support query in Mango with Module details, owner and a summary of the communication - such that it may be a useful resource for the client if they refer back to it at a later stage.
4. If the support query requires further development, convert Support request to a Dev Request
5. Close support query and archive If support query has been addressed
6. Report produced monthly on support queries received

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
|  8.2 | 8.1 | Internal |

## 5.3.5 Implementation

**Purpose and Scope**

To describe the processes for implementing Mango.

**Procedure**

1. Client signs up to Mango
2. Make contact with client to welcome them to Mango and supply upload spreadsheets
3. Create Implementation kit
4. Upload information to client account as information sheets are returned
5. Arrange implementation date(s)
6. Complete implementation following the Client Implementation Guide
7. Create Action list of items to be addressed by client and/or Mango and document on Post Implementation Action List
8. Create monthly event to follow up with client until implementation is secure or the client no longer requires regular contact
9. Archive Event and file client details

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.5 | 8.1 | Internal |

# 5.4 Operations - Accounting

NA

# 5.5 Operations - Information Security – A5 Information security policies

## 5.6.1 Information Security Policy

Refer to: 2.4 Information Security Policy

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A5 | Public |

# 5.6 Operations - Information Security - A6 Organisation of information security

## 5.6.1 Information Security Responsibilities

Refer to: 2.2 Organisation Roles, Responsibilities and Authorities

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A6 | Internal |

## 5.6.2 Mobile Devices Policy

Your mobile devices must use a PIN code or password at the login screen for access.

Your mobile devices must be kept up to date with manufacturer or network provided patches or releases. As a minimum patches and releases you should check weekly.

Your apps must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden.

If you suspect that unauthorized access to company data has taken place on your mobile device you must report the incident in the improvement module.

If your Mobile Device has been stolen you must report it immediately to the Information Security Officer. The Information Security Officer will determine if the device needs to be locked, barred or deletion of data, an improvement must be raised.

You must only load data essential to your role onto your mobile device(s).

Your mobile devices must not be “jailbroken” or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

You must not load pirated software or illegal content onto your mobile devices.

Your mobile devices must not be connected to a PC which does not have up-to-date and enabled anti-malware and anti-virus protection.

You must be cautious about the merging of personal and work email accounts on their devices.

You must take particular care to ensure that company data is only sent through the company's email system.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A6.2.1 | Public |

## 5.6.3 Remote Working Policy

This policy applies to employees whose primary work location is not at our offices.

You may work remotely on a permanent or temporary basis, if approved by Management.

To ensure that your performance will not suffer in remote work arrangements, we advise that you to:

* Choose a quiet and distraction-free working space.
* Have an internet connection that’s adequate for their job.
* Dedicate your full attention to their job duties during working hours.
* Adhere to break and attendance schedules agreed upon.
* Ensure your schedules overlap with those of your team members for as long as is necessary to complete their job duties effectively.

Team members and managers should determine long-term and short-term goals. They should frequently meet (either online or in-person when possible) to discuss progress and results.

Remote employees must follow our company’s policies like their office-based colleagues.

We will provide you with equipment that is essential to you duties. Equipment that we provide is company property. You must keep it safe and avoid any misuse. Specifically, you must:

* Keep their equipment password protected.
* Store equipment in a safe and clean space when not in use.
* Follow all integrated management system policies and procedures.
* Refrain from downloading suspicious, unauthorized or illegal software.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A6.2.2 | Public |

## 5.6.4 Mobile Device Procedure

**Purpose and Scope**

To describe the process taken when a Mobile device has been stolen or lost.

**Procedure/Process**

If a Mobile device has been reported stolen or lost an improvement is raised.

The Information Security Officer will determine what action will be performed based on the risk to the organisation.

The following table describes the steps to be performed:

|  |  |
| --- | --- |
| **Devices** | **Actions** |
| Mobile Phones | 1. Change work application user names and passwords
2. Contract Vodafone to advise them which phone is to be suspended or deleted
 |
| Tablets | Change work application user names and passwords |
| Laptops | Change work application user names and passwords |

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A6.2.1 | Internal |

# 5.7 Operations – Information Security – A7 Human Resource Security

## 5.7.1 Human Resource Security

Refer to: 4.2 Recruitment, Training, Competency, Discipline, Termination and Knowledge Management

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A7.1.1 | Internal |

# 5.8 Operations - Information Security - A8 Asset Management

## 5.8.1 Asset Management

**Purpose and Scope**

To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation and to prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

**Associated Documents**

Risk Management Module

**Procedure**

Information Classification

The information is classified in the Risk Management Module.

The process for recording and classifying information is as follows:

* New Information/assets identified and entered into the Classification Register template in the Risk Management module
* The Classification criteria and controls are based on the following table:



Handling of Media

USB Flash Drives:

* Any media received from a unknown source will be destroyed
* Media received from a known external source on removable media will be scanned for viruses, malware and other security risks.
* Data will be removed and stored within the Mango environment.
* Device will be returned to the sender or destroyed.
* Mango only uses USB flash drives that have been approved by the Information Security Officer and supplied by the approved Network IT Provider.

External Drives:

* Any media received from a unknown source will be destroyed
* Media received from a known external source on removable media will be scanned for viruses, malware and other security risks.
* Data will be removed and stored within the Mango environment.

Internal drives:

* Old hard drives will be removed from the premises and destroyed.

Disposal of Media

* Management must approve the disposal of any media device.
* Items to be destroyed will be recorded in the management minutes and the Plant/Equipment module.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A8 | Internal  |

## 5.8.2 Acceptable Use Policy

You must use resources responsibly, efficiently and in an ethical manner, and with due regard to the rights of others.

You must guard against any misuse which aims to disrupt resources at the company or beyond.

For the avoidance of doubt, unacceptable conduct includes, but is not limited to:

* Using resources in a way that interferes with the reasonable use of resources by other users
* Using resources in a way that hinders the company meeting its legal obligations
* Assuming another person’s identity or role
* Communicating on behalf of the company the user does not have the authority to represent
* Accessing, using, destroying, altering, dismantling or disfiguring resources without appropriate authority or other lawful excuse
* Breaching any of the company or third party copyright or patent protection and authorisations, including licence agreements and other contracts
* Breaching the privacy of individuals without appropriate authority or other lawful excuse
* Using resources to bully, harass or victimise any other person

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A8.1.3 | Public |

# 5.9 Operations – Information Security – A9 Access Control

## 5.9.1 Access Control Policy

Information security is the protection of information against accidental or malicious disclosure, modification or destruction.

Information is an important, valuable asset of Mango Limited which must be managed with care. However, not all of this information has an equal value or requires the same level of protection.

We have established specific requirements for protecting information and information systems against unauthorised access, the controls effectively communicate the need for information and information system access control.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A9.1.1 | Public |

## 5.9.2 Access Control

**Purpose and Scope**

To describe the physical and logical access controls across networks, IT systems and services. This will provide authorised, granular, auditable and appropriate user access.

**Associated Documents**

Information Classification

Remote Working Policy

Access Control Policy

**Procedure**

Access Privileges

1. Mango will provide all employees, partners and contracted third parties with on-site access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.
2. The allocation of privilege rights is restricted and controlled and not provided by default.
3. Authorisation for the use of such accounts shall only be provided by the Information Security Officer.
4. The CTO will guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity (i.e. Ransomware attacks).
5. Access rights will be accorded following the principles of least privilege and need to know.
6. Every user should understand the sensitivity of their data and treat them accordingly.
7. The Information Classification procedure enables users to classify data appropriately and gives guidance on how to store it, irrespective of security mechanisms that may or may not be in place.
8. Users electing to place information on non-Mango managed systems and databases, digital media, cloud storage, or removable storage devices are advised by Mango only do so where such an action is in accord with the information’s security classification.
9. Users are to report instances of non-compliance in the improvement module.

Access Control Authorisation

1. Access to Mango resources and services will be given through the provision of a unique user accounts and complex passwords.
2. Third parties are provided with accounts that solely provide access to the systems and / or data they are contracted to handle, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or when no longer required. Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.
3. User registration and de-registration:
4. Development: When a new user joins, they will be giving access to source control, bug tracking system, email and wiki. Each user will be given different set of controls in each environment based on their role in the environment. When a user leaves Mango, the access to the environments will be removed by the CTO.
5. General: When a new user joins, they will be giving access to appropriate environments. Each user will giving different set of controls in each environment based on their role in the environment. When a user leave Mango, the access to the environments will be removed.

Access to Secret, Confidential and Internal Use information

1. Access to this Secret, Confidential and Internal Use information will be limited to authorised persons whose job responsibilities require it, as determined by law, contractual agreement or the Information Security Policy. The responsibility to implement access restrictions lies with the environment owners.
2. There are no restrictions on the access to ‘Public’ information.

Access for remote users

1. Access for remote users shall be subject to authorisation by the Information Security Officer and be provided in accordance with the Remote Working Policy and the Information Security Policy.
2. No uncontrolled external access shall be permitted to any network device or networked system.

Physical access control

1. Physical access to the Mango office is restricted with key access and alarmed with a PIN code.
2. Visitors must be escorted by an employee. Visitors must have an appointment.

Access Control Methods

1. Access to data is variously and appropriately controlled according to the information classification levels.
2. Access control methods include:
	1. Put your controls here.
3. Access to the source control environment is protected by user account.
4. The Mango employees are not to share their user account for each environment.

Cloud Systems

1. The use of cloud-based systems must meet the access control provisions laid out in this policy.
2. Evaluation of access controls implemented in any cloud system is performed during the vendor assessment and implementation stages of any project.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A9 | Confidential |

# 5.10 Operations – Information Security – A9 Cryptography

## 5.10.1 Cryptographic Controls

**Purpose and Scope**

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information in the company.

**Associated Documents**

Mango

SSL Certificate

**Procedure**

Cryptographic controls

The following is the approved encryption methods for data at rest in the Mango application:

* Add you details here.

Key Management

* Add you details here.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A10 | Confidential |

# 5.11 Operations – Information Security – Physical and environmental security

## 5.11.1 Physical and environmental security

Refer to: 4.1 Resources, Assets and Infrastructure

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A11 | Confidential |

## 5.11.2 Clean Desk Policy

Mango Limited has adopted a Clean Desk Policy for computer and printer workstations to improve the security and confidentiality of information, This ensures that all secret and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use.

This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

Whenever a desk is unoccupied for an extended period of time the following will apply:

1. All secret and confidential paperwork must be removed from the desk and locked away. This includes mass storage devices such as CDs, DVDs, and USB drives.
2. All secret or confidential information if not being used or locked away will be shredded.
3. Computer workstations and servers must be locked when shut down at the end of the work day or when the office is unattended.
4. Any secret and confidential information sent to the printer should be retrieved from the printer immediately.
5. All secret and confidential information paperwork left over at the end of the work day will be properly disposed of.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A11 | Public |

# 5.12 Operations – A12 Operations Security

## 5.12.1 Operations security

**Purpose and Scope**

This describes the following:

* The correct and secure operations of information processing facilities.
* To ensure that information and information processing facilities are protected against malware.
* To protect against loss of data.
* To record events (logging) and generate evidence (monitoring).
* To ensure the integrity of operational systems.
* To prevent exploitation of technical vulnerabilities.
* To minimise the impact of audit activities on operational systems.

**Associated Documents**

Management Review

Management Minutes

**Procedures**

Protection from Malware and Hacking

Receiving and sending of emails

1. Add you details here.

Default Passwords

1. Add you details here.

Mango Application Protection

* Add you details here.

Backup Procedures

1. Add you details here.

Event Logging and Monitoring

* Add you details here.

Control of Operational Software

* Add you details here.

Technical Vulnerabilities

* Add you details here.

Information system audit controls

* Add you details here.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A12 | Confidential |

# 5.13 Operations – Information Security – A13 Communications Security

## 5.13.1 Communications Security

**Purpose and Scope**

To ensure the protection of information in networks and its supporting information processing facilities. To maintain the security of information transferred within an organization and with any external entity.

**Associated Documents**

..

**Procedures**

Network Security Management

|  |  |  |
| --- | --- | --- |
| **Networks** | **Network Controls** | **Segregation** |
| Add you details here. |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Communications

Real time communication:

* Add you details here.

Mango Application

* Add you details here.

Mango Limited

* Add you details here.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A9 | Confidential |

# 5.14 Operations – Information Security - System acquisition, development and maintenance

## 5.14.1 System acquisition, development and maintenance

**Purpose and Scope**

To ensure that the security of information systems across the entire lifecycle is integrated, designed, implemented and tested.

**Associated Documents**

..

**Procedure**

Information security requirements analysis and specification

1. Add you details here.

Securing application services on public networks and protecting application services transactions

1. Add you details here.

Security in development and support processes

* Add you details here.

System change control procedures

1. Add you details here.

Technical review of applications after operating platform changes

* Add you details here.

Restrictions on changes to software packages

1. Add you details here.

Secure system engineering principles

* Add you details here.

Secure development environment

* Add you details here.

Outsourced development

* Add you details here.

System security testing and System acceptance testing

1. Add you details here.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A14 | Confidential |

# 5.15 Operations – Information Security - Supplier Relationships

## 5.15.1 Supplier Relationships

Refer to: 6.1 Supplier Evaluation and Control

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A15 | Confidential |

# 5.16 Operations – Information Security - Information Security Incident Management

## 5.16.1 Information Security Incident Management

**Purpose and Scope**

To ensure a consistent and effective approach to the management of information security related incidents and the communication of security events and weaknesses.

**Definition**

Information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

**Associated Documents**

Improvement Module

**Procedure**

1. All information security issues are to be reported and managed through the Improvement module in Mango.
2. This includes suspected security weaknesses in systems or services.
3. The Improvements module will manage the communication to relevant employees and managers
4. Information security events will be assessed to identify whether they are classified as Information Security Incidents.
5. All evidence relating to the investigation will be captured in the Improvement record

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A16 | Confidential |

# 5.17 Operations – Information Security - Information security aspects of business continuity management

## 5.17.1 Business Continuity Planning

**Purpose and Scope**

To describe the procedure for business continuity planning.

**Associated Documents**

Business Continuity Plan

**Procedure/Process**

1. Add you details here.

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A17 | Confidential |

# 5.18 Operations – Information Security - Compliance

## 5.18.1 Compliance

Refer to: 3.2 Legal and Other Requirements

**References and Classification:**

|  |  |
| --- | --- |
| **ISO 27001** | **Classification** |
| A18 | Confidential |

# 6 Supplier and Contractor Management

## 6.1 Supplier Evaluation and Control

**Purpose and Scope**

To describe the process and method by which suppliers (the term also includes contractors and subcontractors) are evaluated, selected and controlled. The scope includes the outsourcing requirements.

**Associated Documents**

Mango Suppliers Module.

Supplier Evaluation Form

**Procedure**

General Requirements

1. The selection criteria for suppliers is as follows:
* Ability and preparedness to meet IMS requirements.
* Ability and capability to meet legislative obligations and relevant industry and government standards and codes.
* Qualifications, experience and capability within the scope they are contracted for.
* Quality, consistency and reliability of product or service provided.
* Delivery performance.
* Price of product or service including commercial arrangements.
* Quality, environmental, health and safety management systems.
* Past performance including health, safety and environmental record.
1. Suppliers are classified on the basis of the potential risk their products or services may pose to:
* Products or services.
* Workplace health and safety.
* The environment.
1. Consideration needs to be given to whether:
* Failure of the supplier to deliver agreed products or services will impact upon profitability?
* Failure of the supplier to deliver agreed products or services will result in failure to meet any contractual, legislative and statutory obligations for delivery of products and services?
* The supplier will introduce or potentially introduce any high risk hazards or significant environmental impacts to the workplace?
1. Suppliers and outsourced activities that are identified as having the potential to significantly affect activities, products or services are deemed “critical” and must undergo a thorough documented evaluation and re-evaluation process. Non-critical suppliers are required to be evaluated but not necessarily to the same extent as those deemed to be critical. Examples of critical suppliers and outsourced activities would include:
* Suppliers of software hosting services.
* Suppliers of IT services.
* Supplier of financial services.

All critical suppliers and outsourced activities must have a written contract.

1. The following rating system will be used for suppliers:
* Critical
* Approved
* Approved and inducted
* Back-up
1. Where applicable, suppliers must have current and appropriate insurance arrangements in place. Certificates of currency for required insurances are to be provided as part of the formal evaluation process.
2. Products and services essential to meet contract requirements shall only be purchased from qualified and approved suppliers.
3. The details of suppliers are specified in the Suppliers Module within Mango, inclusive of their rating.

Supplier Induction

1. All suppliers and their staff, who conduct work on behalf of Mango Limited, are to be effectively inducted, including training with respect to specific site procedure requirements. Refer to 4.2 procedure for further details.
2. A record of the induction training conducted in to be retained in Mango.

Re-Evaluation

1. Once evaluated and approved, suppliers are to be subjected to formal periodic re-evaluation. Re-evaluations are scheduled within the Supplier Module within Mango.
2. Re-evaluation is to take place at least once every two years or sooner if reasons apply. Some reasons for early re-evaluation are:
	1. Incidents and/or poor performance involving the supplier or contractor.
	2. Change in circumstances or structure such as new ownership, or change of location or key personnel.
	3. Change in scope of services.

3. Re-evaluation is to follow the same process as for the initial evaluation.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 6.1, 8.4.1, 8.4.2, 8.4.3 | A15 | Internal |

# 7 Performance Evaluation

## 7.1 Monitoring, Measurement and Evaluation

**Purpose and Scope**

To describe how we will monitor, measure, analyse and evaluate the IMS in order to identify and take suitable action to ensure the continual improvement of the management system.

**Associated Documents**

Mango Events Management Module.

Mango Reports.

**Procedure**

General Requirements

1. The Directors will determine:
	1. The aspects of the IMS that will be monitored and measured.
	2. The responsibilities, frequency and methods for monitoring, measurement, analysis and evaluation needed.
	3. The criteria against which we will evaluate its IMS performance. When the monitoring and measuring:
		1. Will be performed.
		2. Results will be analysed and evaluated.
2. The results of the analysis and evaluation conducted is to evaluate the:
	1. Degree of customer satisfaction.
	2. Conformity of products and services.
	3. Performance and effectiveness of the IMS including the environment, health and safety, quality and information security.
	4. If planning has been effectively implemented.
	5. Effectiveness of actions taken to address risks and opportunities.
	6. Performance of external providers.
	7. Need for improvements to the IMS.
3. Appropriate documented information must be retained as evidence of the monitoring, measurement, analysis and evaluation that is conducted.

Monitoring Arrangements

1. Generally, individual procedures within the IMS describe the specific; monitoring, measurement, analysis and evaluation requirements to be met.
2. Whenever required, an event will manage the process.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 9.1.1, 9.1.2, 9.1.3 | A15 | Internal |

## 7.2 Audits and Inspections

**Purpose and Scope**

To describe the responsibilities and methods used to evaluate the effectiveness of the implementation and maintenance of the IMS.

Audits and inspections are completed for the following purposes:

* To identify the compliance status against Mango Limited policies, procedures, legal requirements and other obligations,
* To identify areas where IMS performance needs to be improved or changed.
* To identify leading practice, so as such practices can be communicated and implemented in other Mango Limited activities.

**Associated Documents**

Internal and External Audit Reports.

Mango Events Management Module.

Mango Improvement Module.

Mango Audit / Inspection Module.

Mango Compliance module.

**Procedure**

1. Mango will use the DIME matrix methodology for internal audits.
2. This will be an audit of the system based on the ISO 9001 and ISO 27001 clauses.
3. We will audit using and excel spreadsheet and the compliance module to capture the records of DIME (documented, implemented. monitored, evidence/effective).
4. An event will remind Management when the audit is due.
5. The Audit team will audit the assigned section of the IMS.
6. An auditor cannot audit a core function they are responsible for.
7. Once complete, the event will be signed off and a copy of the DIME report uploaded.
8. An improvement will be raised for each non-conformance identified.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 8.5.6, 9.1, 9.2, 9.3 | 9.1, 9.2 | Internal |

## 7.3 Management Review and Operations Meeting

**Purpose and Scope**

To describe the requirements to be followed to ensure that the IMS is effectively reviewed on a regular basis with the purpose to:

* Ensure its continuing suitability, adequacy, effectiveness and alignment with the strategic direction of Mango Limited.
* Consider relevant changes in external and internal issues, including changes to legislative and other requirements.
* Ensure all employees are aware of the current status of IMS performance and changes to the IMS system and procedures.
* Allow for all employees to provide suggestions, direction and resources for the continual improvement of IMS performance.
* Ensure the operations of the company are being performed effectively and efficiently

**Associated Documents**

Management Review Meeting Minutes.

Operations Meeting minutes

Data in Mango.

**Procedure**

Management Review

1. A formal review of the IMS is to be conducted every month
2. All staff are invited and expected to attend in person or via appropriate communication.
3. An event has been setup to ensure the Management Review happens.
4. The Management Representative will run, minutes and publish the Management review in Mango.
5. The Management review will follow the standard agenda format in the minutes. The agenda includes, but not limited to.
	1. Previous minutes
	2. Policies, objectives, targets and plans
	3. Risks and issues
	4. Marketing, Sales, Support and Development
	5. Improvement and performance
	6. Audits
	7. Process Improvement (including feedback from interested parties)
6. Actions are assigned and recorded on the Management Minutes with agreed timeframes.

Operations Meeting

1. An operational review of the company is conducted every month.
2. It is attended by the Operations Manager, CMO, CFO, Marketing Specialist
3. An event has been setup to ensure the operational meeting happens.
4. The CMO will run, minutes and publish the minutes in Mango.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| ISO 9001 | ISO 27001 | Classification |
| 4.1, 4.2, 4.4.1, 5.1, 6.2, 9.3, 9.1.2, 9.1.3, 10.3 | 9.3 | Internal |

# 8 Improvement

## 8.1 Improvement and Corrective Actions

**Purpose and Scope**

To ensure that improvements, non-conformities and corrective actions are reported, recorded, investigated and followed up.

The procedure also ensures that non-conforming products or services are identified, reported, recorded, investigated and controlled.

**Associated Documents**

Mango Improvement Module.

**Procedure**

General Requirements

1. Employees must report improvement opportunities, non-conformances, failures and any other IMS issues.
2. Improvements can be initiated by any employee when any of the following issues are identified:
* To initiate a change to the IMS.
* To initiate an improvement to the performance and effectiveness of the IMS.
* When an innovation or improvement opportunity is identified.
* When a non-conformance is identified at any time. (Software Bugs are handled via Mantis software)
* When a discrepancy, non-conformance or improvement is identified during auditing.
* When a customer complaint or any significant customer feedback is received (including compliments).
1. Improvements are to be retained in Mango including associated documents and records with respect to the improvement
2. The improvement workflow will manage the improvement process
3. Findings will be reported to the Management Review meeting including their status.

**References and Classification:**

|  |  |  |
| --- | --- | --- |
| **ISO 9001** | **ISO 27001** | **Classification** |
| 6.1, 8.7, 9.1, 9.3.2, 10.1, 10.2, 10.3 | 10.1, 10.2 | Internal |