MOSAIC™
Financial Services Infrastructure

Mosaic Business Solutions Limited, Information Security Management Systems

Document Control

Document ref	ISMS202101
Version	4
Dated	11/01/2021
Document author	Russell Fielding/ Mike Stobbs
Document owner	Mike Stobbs, Mosaic FSI
Approved by	Mike Stobbs
Confidentiality level	Internal

Revision History

Date	Version	Description	Author
14/01/21	4	Increase scope, turn document more into a signpost document outlining ISMS and linking to all relevant ISMS documents and added ISO 27001 checklist.	Russell Fielding
25/01/21	4.1	Q/A	Mike Stobbs

Distribution

Name	Title

Table of Contents

Scope and Introduction

This information security management system (ISMS), having been approved by top-level management, outlines the overall security management framework for Mosaic FSI and needs to be read by all Mosaic FSI employees and contractors. After reading the document in its entirety employees and contractors must sign the form confirming they have read and understood this policy thoroughly.

This document will be reviewed and updated by management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it to all employees and contracts as applicable.

This policy applies to all systems, people and processes that constitute the organisation's information system, including board members, directors, employees, contractors, suppliers and other third parties who have access to Mosaic FSI systems.

This ISMS methodology is based on the ISO 27001 standard, the methodology and checklist can be found between pages 10 – 12.

The ISMS document is a signpost document and is linked with the following Mosaic FSI documents

- Information Security Policy
- ISO 27001 Statement of Applicability
- ISO 27001 Risk Assessment Methodology including appendix 1 – Risk Assessment Table spreadsheet and appendix 2 – Risk Treatment Table spreadsheet
- IT and Social Media Policy including social media threats awareness.
- Cyber Security and Phishing Awareness
- Data Protection Policy including data privacy awareness.
- Data Breach Notification Plan
- Business Continuity Plan
- Incident Management Procedures
- Internal audit checklist
- Internal audit report

Human Resource Privacy Documents

- Confidentiality agreement
- Consent form for new employees uses of data.
- Consent form for unsuccessful job applicants
- Consent form for the use of data for existing employees
- Consent form for employees who is leaving.
- AML onboarding policy
- Anti-Bribery policy

Purchasing

- Supplier Assessment

Record Keeping

- Records Retention and Protection Policy
- Mosaic FSI Security Log
- Document Control Procedure

System Overview

Systems that are used by Mosaic Business Solutions Limited:

System	Primary Use	Risk Level
Office 365	Email and shared document storage	High
Drop Box Professional	File storage	High
Harvest	Time tracking	Medium
Xero	Accounting software	High
KiwiBank - online	Banking services provider	High
IRD – myIR portal	Filing of returns	High
Freeparking	Domain Name	Medium
Wordpress	Website	Medium
Cloudways	Website Hosting	Medium
Burst SMS	Txt messaging	Medium
Job Adder	Human resource	Medium
Vetting.co.nz	Ministry of Justice checks, credit checks, pre employment checks	Medium
Trello	Task management	Low
Hubspot	CRM	Medium
PaySauce	Payroll	High
LinkedIn	Social network for business	Medium

For information on Risk Assessment Methodology go to the Mosaic FSI risk assessment methodology document which includes two separate spreadsheet documents the risk assessment table and the risk treatment table.

Critical System

The following systems are considered critical due to their high-risk level in the above table.

Office 365

- Outlook for email communications.
- OneDrive for document sharing and storage in the cloud.
- Teams for communicating via chat and video call.

Xero

- Accounting software managed by a contract accountant for Mosaic Business Solutions Limited and Mosaic Business Solutions Limited.
- Payments to suppliers and contractors requiring approval by delegated signatories Myles Allan and Mike Stobbs
- Payroll requiring approval by delegated signatories Myles Allan and Mike Stobbs

Kiwibank

- Receipt of client payments
- Reconciliation with Xero
- Payments to staff, contractors, and suppliers

IRD

- Key returns
- ACC & KS
- Various tax obligations

DropBox Professional

- File and document storage and sharing

Freeparking

- Domain name hosting for Mosaic and mail flow to Office 365 suppliers

Paysauce

- Payroll for all employees
- Integrated with Xero

System Access

A register of systems, users and associated access levels is maintained on the Mosaic Business Solutions Limited OneDrive.

Access rights are immediately removed for all terminated staff.

Security Controls

Office 365

Access

- All users with Administrator rights are required to use multi-factor authentication (system enforced).
- User accounts are automatically locked after ten failed login attempts (standard feature in Microsoft Office 365 as outlined here):
  - After 10 unsuccessful logon attempts (wrong password), the user will need to solve a CAPTCHA dialog as part of logon.
  - After a further 10 unsuccessful logon attempts (wrong password) and correct solving of the CAPTCHA dialog, the user will be locked out for a time period. Further incorrect passwords will result in an exponential increase in the lockout time period.
- Temporary staff & contractors are restricted to browser access only, they are not permitted to configure Office 365 access on their own devices.
- Malware and Phishing reports, these should be generated monthly and investigations on delivered items or quarantined items.

Security Patches

- All security and critical patches are deployed within 30 days of being released.

Xero

- All users are required to use multi-factor authentication.

KiwiBank

- All users are required to use multi-factor authentication.

IRD

- All users are required to use multi-factor authentication.

DropBox Professional

- All users are required to use multi-factor authentication.

General Password Requirements

- All passwords are required to be a minimum of eight characters including letters, numbers and symbols.
- All passwords are required to be changed every six months. Where available, systems are set to require this.
- Passwords are required to be stored and shared in a secure password service like LastPass or OnePassword where there is a Mosaic Business Solutions Limited Team set up in order to share Mosaic Business Solutions Limited related passwords.
- Passwords should NOT be shared by email, Spreadsheets, Whatsapp, any social media platforms or other written forms.

Data Backup

Email communications and documents are stored in Office 365 which is a cloud-based system and therefore continually backed up.

All staff should save all Mosaic Business Solutions Limited documents to the Mosaic Business Solutions Limited OneDrive folder, where it is continually backed up by Microsoft. In exceptional

cases, where Mosaic Business Solutions Limited data is stored on a device or a pen drive, this data should also be backed up on the Mosaic Business Solutions Limited OneDrive.

Data is currently being stored and shared via DropBox Professional.

Website

The Mosaic Business Solutions Limited website is hosted by Cloudways, and the following domains are managed via Freeparking:

- mosaicfsi.com
- mbsnz.com

Social Media

Mosaic FSI has a LinkedIn profile Mosaic FSI | LinkedIn

Refer to the Mosaic FSI IT and social media policy document for detailed information ISMS202107.

Home, Office Guidelines

- Some Mosaic Business Solutions Limited staff work from home offices, and therefore are required to ensure adherence to the following rules concerning their workplaces and personal devices:
- All default passwords on internet connected devices should be changed from their factory settings (e.g., routers, printers, IOT).
- For staff using personal laptops and phones, these devices should be password protected, and in the case of loss, devices should be able to be locked and/or passwords should be able to be reset remotely.
- In the case a device with access to Mosaic Business Solutions Limited data is lost, the loss should be reported immediately to Mike Stobbs or Sean O'Connor who can revoke access to Office 365 and any other systems to which the user had access.
- All internet access points to the Mosaic Business Solutions Limited network should be secured by firewalls. This is checked by our IT Manager whenever a new employee is given access to Microsoft 365.
- All on-line devices should be locked any time you walk away from your terminal, whether in the office or home – no exceptions.
- Work devices should not be utilised for any personal use.
- Web site browsing should only be performed where it supports work related activity i.e., research, booking travel, accommodation, competitor information.
- Social media platform access should be limited to either business platforms such as linked-in or the web site administrator using platforms for recruitment, brand awareness etc.

More detailed information on remote access policy can be found in the information security policy document number ISMS202102.

Incident Management Procedures

Refer to the Mosaic FSI incident management procedures document for detailed information ISMS202106.

Business Continuity Plan

Refer to the Mosaic FSI business continuity plan document for detailed information ISMS202105.

Employee Education

Employees and contractors play a critical role in ensuring the integrity and security of Mosaic Business Solutions Limited's data.

Employees and contractors are kept up to date with cyber threats in the following ways:

- The below information is included in the Mosaic Business Solutions Limited Onboarding online training for all new staff.
- IT Manager sends bi-annual emails (or more frequently if needed) to staff outlining any new or trending threats to be aware of, how they may pose a risk to Mosaic Business Solutions Limited and how to ensure our data is kept safe.

Online Training

- Online employee and contractor training includes:
- Mosaic FSI information security management system (This document)
- Information Security Policy
- IT and Social Media Policy including social media threats awareness.
- Cyber Security and phishing awareness
- Data protection policy included data privacy awareness.
- Information security and data privacy is incorporated within all onboarding documents when relevant.

Customer Premises Guidelines

Most Mosaic Business Solutions Limited staff work on customer premises and therefore are required to ensure adherence to the following rules concerning these workplaces:

- Follow the same standards as home office if you are using your Mosaic provided device or personal device (in the case of contractors)
- In many cases you can only use the customer provided device and associated access tokens
- Strictly adhere to all customer mandated rules and guidelines and additionally
- Never print out work related material unless necessary and do not take home unless required, but with prior approval.
- Do not use the customer provided device for any personal use or browsing.
- Do not insert any remote devices such as USB's as these may contain a virus.
- Never share your password or remote access device with another member of you project team.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

More detailed information on remote access policy can be found in the information security policy document number ISMS202102.

IT Department Escalation Contacts

All IT concerns should be directed to partner/ founder Myles Allan in the first instance:

Email: myles.allan@mosaicfsi.com

Mobile: +64 21 411 956

Or Partner/ Information Security Officer Mike Stobbs

Email: mike.stobbs@mosaicfsi.com

Mobile: +64 021 428 858

IT concerns will be escalated by Myles as follows:

Tier 2 IT Support – outsourced to Sean O'Connor of O'Connor Ltd:

- Email: sean@seanoconnor.co.nz
- Phone/Whatsapp: +6421655133

ISMS Methodology

The methodology has been extracted from the ISO 27001 standard.

See Risk Assessment Methodology document for Risk methodology including appendix 1 – Risk Assessment Table spreadsheet and appendix 2 – Risk Treatment Table spreadsheet.

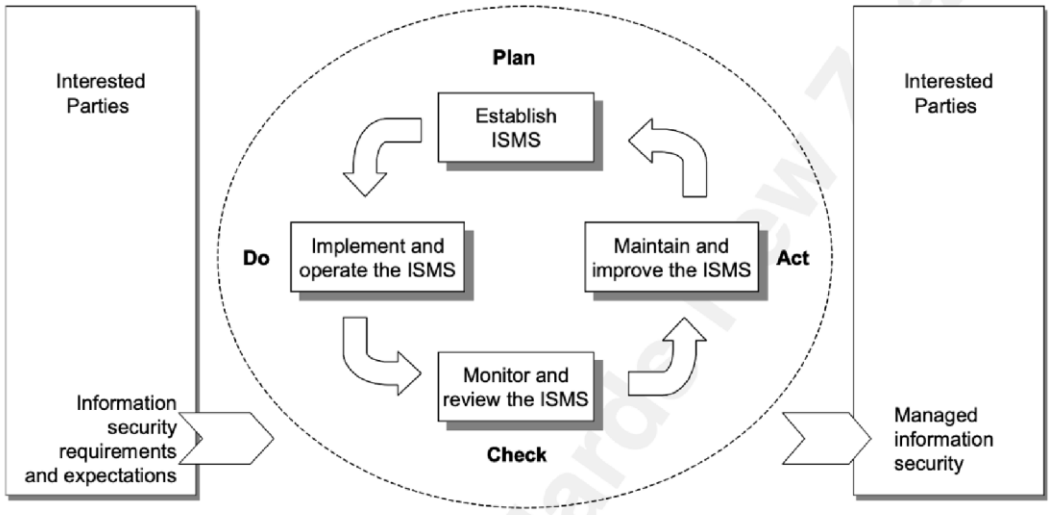

Figure 1 — PDCA model applied to ISMS processes

ISO 27001 Checklist

Key

Y – Yes Mandatory policies, procedures for ISO 27001:2013.

Y RK - Mandatory record keeping for maintaining ISO 27001:2013.

N R - Non-mandatory documents but recommended and commonly used.

Requirement	Clause number	Mandatory	Mosaic FSI document
Scope of the ISMS	4.3	Y	ISMS page 3.
Information security policy and objectives	5.2, 6.2	Y	ISMS and information security policy.
Risk assessment and risk treatment methodology	6.1.2	Y	Risk Assessment Methodology document.
Statement of Applicability	6.1.3-d	Y	Statement of applicability document and ISMS page 11 -12
Risk treatment plan	6.1.3-e, 6.2	Y	Risk Assessment Methodology document, Appendix
Risk assessment and risk treatment report	8.2, 8.3	Y	Risk Assessment Methodology document, Appendix
Definition of security roles and responsibilities	A.7.1.2, A.13.2.4	Y	Information Security Policy page 5-6
Inventory of assets	A.8.1.1	Y	Information Security Policy
Acceptable use of assets	A.8.1.3	Y	Information Security Policy
Access control policy	A.9.1.1	Y	Risk Assessment Methodology and Information Security Policy
Operating procedures for IT management	A.12.1.1	Y	Information Security Policy
Secure system engineering principles	A.14.2.5	Y	Information Security Policy and ISMS
Supplier security policy	A.15.1.1	Y	Supplier Assessment
Incident management procedure	A.16.1.5	Y	Data Breach Notification Plan/ Incident management procedure document.
Business continuity procedures.	A.17.1.2	Y	Business Continuity Procedures (BCP)
Legal, regulatory, and contractual requirements	A.18.1.1	Y	Information Security Policy
Records of training, skills, experience and qualifications	7.2	Y RK	HR department, on-boarding and training checklist
Monitoring and measurement results	9.1	Y RK	Statement of applicability,
Internal audit program	9.2	Y RK	Internal Audit Checklist

Results of internal audits	9.2	Y RK	Internal Audit Report
Results of the management review	9.3	Y RK	Internal Audit Report and ISMS
Results of corrective actions	10.1	Y RK	Including in normal house keeping HR documents
Logs of user activities, exceptions, and security events	A.12.4.1, A.12.4.3	Y RK	BCP, Security Log
Procedure for document control	7.5	N R	Document Control Procedure
Controls for managing records	7.5	N R	Record retention and protection policy
Procedure for internal audit	9.2	N R	Internal Audit Checklist
Bring your own device policy	A.6.2.1	N R	IT and social media policy and information security policy
Mobile device and teleworking policy	A.6.2.1	N R	IT and social media policy and information security policy.
Information classification policy	A.8.2.1, A.8.2.2, A.8.2.3	N R	information security policy.
Password policy	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1	N R	IT and social media policy and information security policy.
Disposal and destruction policy	A.8.3.2, A.11.2.7	N R	Records retention and protection policy.
Clear desk and clear screen policy	A.11.2.9	N R	Information Security Policy section 2.2.
Change management policy	A.12.1.2, A.14.2.4	N R	Standard HR documents including document control procedures.
Backup policy	A.12.3.1	N R	Dropbox
Information transfer policy	A.13.2.1, A13.2.2, A.13.2.3	N R	Data protection policy, data breach policy
Business impact analysis	A.17.1.1	N R	BCP
Exercising and testing plan	A.17.1.3	N R	Statement of applicability
Maintenance and review plan	A.17.1.3	N R	ISMS Action plan, statement of applicability

See statement of applicability for full details showing which controls are appropriate to be implemented in Mosaic FSI, also the objectives of these controls and how they are implemented and approve residual risks and formally approve the implementation of the controls.