Mosaic Business Solutions Limited Information Security Policy

Document Control

Document ref	ISMS202102
Version	2
Dated	16/01/2021
Document author	Mike Stobbs
Document owner	Mike Stobbs, Mosaic FSI
Approved by	Mike Stobbs
Confidentiality level	Internal

Revision History

Date	Version	Description	Author
14/01/21	2	Increase scope added applicable legislation/ regulations. Update roles and responsibility added privacy officer description. Updated all policies	Russell Fielding
25/01/21	2.1	Q/A	Mike Stobbs

Distribution

Name	Title

Table of Contents

Scope and Introduction

The Information Security Policy states the types and levels of security over the information technology resources, people and capabilities that must be established and operated in order for those items to be considered secure. The information can be gathered in one or more documents.

Scope

This information security policy, having been approved by top-level management, outlines the overall security requirements and secure use of the information technology services 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 contractors 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.

Applicable Legislation/ Regulations

The following is a list of the various agencies/organisations whose laws, mandates, and regulations were incorporated into the various policy statements included in this document.

- NZ Privacy Commissioner
- Privacy Act 2020
- Financial Markets Authority
- Government Communications Security Bureau

Responsibilities

Below is a list of roles involved and their responsibilities in the enforcement of the policies in this document.

Roles	Responsibilities
Partner (to be assigned)	• Oversees compliance and the operation of information security controls as a representative of top management within Mosaic FSI and has overall responsibility for its effectiveness. • Maintain a clear and current understanding of the legislation and its implications for the business processes of Mosaic FSI.
Information Security Officer	• Reporting to the allocated partner on all security related matters on a regular and ad-hoc basis when required • Communicate the information security policy to all relevant interested parties where appropriate, including customers. • Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure that security controls are in place and documented. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Assist with disaster recovery planning. • Define improvement plans and targets for the financial year. • Monitor achievement against targets. • Establish and maintain a continual improvement action list. • Report on improvement activities • Identify and manage information security incidents according to a process. • Attend management review meetings on a regular basis. • Liaise with Cloud Service supplier and other third parties' representatives on information security-related matters.
Information Owners	• Assist with the security requirements for their specific named area. • Maintain and review security controls for allocated asset(s) • Participate in risk assessments concerning their asset(s) • Ensure the relevant entry in the asset inventory is kept up to date.
IT Security Team	• Implements and operates IT security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

Privacy Officer

- Mosaic FSI has established a Privacy Officer as required within part 9, 201 of the Privacy Act 2020. This Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of Mosaic FSI privacy policies under applicable Privacy Act 2020 The current Privacy Officer for Mosaic and their contact is Mike Stobbs mike.stobbs@mosaicfsi.com
- Under the privacy act 2020 responsibilities include—
- Encouraging Mosaic FSI to comply with the IPPs.
- Dealing with requests made to Mosaic FSI under the data privacy act 2020.
- Working with the Commissioner in relation to investigations conducted under Part 5 in relation to Mosaic FSI.
- Ensuring that Mosaic FSI complies with the provisions of the privacy act 2020.

Acceptable Use Policy

The first line of defence in data security is the individual user.

Mosaic FSI users are responsible for the security of all data which may come to them in whatever format. Mosaic FSI is responsible for maintaining ongoing training programs to inform all users of these requirements.

The management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Mosaic FSI established culture of openness, trust, and integrity.

Management is committed to protecting the employees, contractors, partners and Mosaic FSI from illegal or damaging actions by individuals, either knowingly or unknowingly. Mosaic FSI will maintain an approved list of technologies and devices and personnel with access to such devices.

Exceptions to the policies defined in any part of this document may only be authorised by the Information Security Officer. In those cases, specific procedures may be put in place to handle request and authorisation for exceptions.

Whenever a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed.

All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.

Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee or contractor will result in disciplinary action, from warnings or reprimands up to and including termination of employment or contract. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance. Civil, criminal, and equitable remedies may apply.

Acceptable Use Policy Main Points for Employees

- Employees and contractors are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees and contractors should ensure that they have appropriate credentials and authenticated for the use of technologies.
- Employees and contractors should take all necessary steps to prevent unauthorised access to confidential data which includes cardholder data.
- Employees and contractors should use technologies in acceptable network locations.
- Employees and contractors must keep passwords secure and do not share accounts.
- Authorised users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Employees and contractors should exercise special care with the information contained on portable computers.
- Postings by employees and contractors from a company e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Mosaic FSI unless posting is in the course of business duties.
- Employees and contractors must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- Employees and contractors must follow a clean desk policy which instructs that all employees must clear their desks at the end of each workday. This not only includes documents and notes, but any post-it notes, businesses cards, and removable media.
- Following a clean desk policy will help Mosaic FSI reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible in plain view.

IT Assets Policy

This section of the Security Policy lists policies for the secure handling of the IT assets.

Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets at Mosaic FSI.

Scope

The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capability involved in the provision of the IT services.

Policy Definitions

- IT assets must only be used in connection with the business activities they are assigned and / or authorised.
- Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.
- All the IT assets must be classified into one of the categories in Mosaic FSI security categories, according to the current business function they are assigned to.
- Employees and contractors are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees and contractors should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees and contractors should take all necessary steps to prevent unauthorised access to confidential data which includes cardholder data.
- Employees and contractors should ensure that technologies should be used and setup in acceptable network locations.
- Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees and contractors during yearly security training.
- Access to assets is forbidden for non-authorised personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service request management and access management processes.
- All personnel interacting with the IT assets must have the proper training.
- Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
- Access to assets at Mosaic FSI location must be restricted and properly authorized, including those accessing remotely. Company's laptops, PDAs and other equipment used at external location must be periodically checked and maintained.
- The IT Technical Teams are the sole responsible for maintaining and upgrading configurations. None other users are authorised to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
- Special care must be taken for protecting laptops, PDAs and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields and falls.
- When travelling by plane, portable equipment like laptops and PDAs must remain in possession of the user as hand luggage.
- If carrying laptops with sensitive data when outside the office secure laptop with a cable lock.
- Whenever possible, encryption and erasing technologies should be implemented in portable assets.
- Losses, theft, damages, tampering, or other incident related to assets that compromises security must be reported as soon as possible to the Information Security Officer.
- Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an Information Security Team member. Assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

Access Control Policy

This section of the Security Policy lists policies for securing access control.

Purpose

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure at Mosaic FSI.

Scope

This policy applies to all the users at Mosaic FSI, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy Definitions

- Any system that handles valuable or confidential information must be protected with a strong password. Strong passwords are defined in the following section.
- Discretionary access control list must be in place to control the access to resources for different groups of users.
- Mandatory access controls should be in place to regulate access by process operating on behalf of users.
- Access to resources should be granted on a per-group basis rather than on a per user basis.
- Access shall be granted under the principle of “less privilege”, i.e., each identity should receive the minimum rights and access to resources needed for them to be able to successfully perform their business functions.
- Whenever possible, access should be granted to centrally defined and centrally managed identities.
- Users should refrain from trying to tamper or evade the access control to gain greater access than they are assigned.
- In the future, access to SaaS applications should be through a password management system such as Okta.

Password Control Policy

This section of the Security Policy lists policies for securing password control.

Purpose

The Password Control Policy section defines the requirements for the proper and secure handling of passwords at Mosaic FSI.

Scope

This policy applies to all the users at Mosaic FSI, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy Definitions

- Any system that handles valuable information must be protected with a password-based access control system.
- Every user must have a separate, private identity for accessing IT network services.
- Identities should be centrally created and managed. Single sign-on should be used to access company services.
- Passwords should never be documented together with the username or application in clear text including in source code. If a password is communicated through digital communications, it must not be documented together with the username or application.
- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters in length and contain a mix of upper and lowercase letters, numbers, and special characters.
- Each regular user is requested not to use the same password for more than 180 days and not use the same password again for at least one year.
- Use of administrative credentials for non-administrative work is not permitted. IT administrators must have two set of credentials: one for administrative work and the other for common work.
- Passwords should not be shared. Exception to this rule may only be authorized in special cases such as to support administration functions. Where passwords are shared user access should be logged.
- Whenever a password is deemed compromised, the security officer must be notified, and the password must be changed immediately.
- For critical applications, digital certificates and digital multiple factors should be used whenever possible.
- Identities must be locked if password guessing is suspected on the account.

EMAIL POLICY

This section of the Security Policy lists policies for the secure handling of electronic mail.

Purpose

This Email Policy section defines the requirements for the proper and secure use of electronic mail at Mosaic FSI.

Scope

This policy applies to all the users at Mosaic FSI, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy Definitions

- All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of Mosaic FSI.
- Only company approved devices should be used to access company email accounts.
- Public devices such as those provided by hotel business services must not be used to access company email accounts.
- Use of Mosaic FSI resources for non-authorised advertising, external business, spam, political campaigns, and other uses unrelated to Mosaic FSI business is strictly forbidden.
- In no way may the email resources be used to reveal confidential or sensitive information from Mosaic FSI outside the authorised recipients for this information.
- Using the email resources of Mosaic FSI for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.
- Use of Mosaic FSI email resources are maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
- Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriate.
- Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged. However, only the Information Security Officer may approve the interception and disclosure of messages.
- Identities for accessing corporate email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the company's procedures for managing identities. Sharing of passwords is discouraged. Users should not impersonate another user.
- Outbound messages from corporate users should have approved signatures at the foot of the message.
- Scanning technologies for virus and malware must be in place in PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
- Security incidents must be reported and handled as soon as possible according to the incident management and Information Security processes. Users should not try to respond by themselves to security attacks.
- Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT continuity management/ BCP.

Internet Policy

This section of the Security Policy lists policies for the secure access to Internet.

Purpose

The Internet Policy section defines the requirements for the proper and secure access to Internet.

Scope

This policy applies to all the users at Mosaic FSI, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy Definitions

- Access to Internet is permitted for all users.
- Access to illegal sites, hacking sites, and other risky sites is prohibited.
- Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.
- In accessing Internet, users must behave in a way compatible with the prestige of Mosaic FSI. Attacks including denial of service, spam, phishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
- Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

Antivirus Policy

This section of the Security Policy lists policies for the implementation of anti-virus and other forms of protection.

Purpose

The Antivirus Policy section defines the requirements for the proper implementation of antivirus and other forms of protection at Mosaic FSI.

Scope

This policy applies to servers, workstations and equipment at Mosaic FSI, including portable devices like laptops and PDA that may travel outside of Mosaic FSI' facilities. Some policies apply to external computers and devices accessing the resources of Mosaic FSI.

Policy Definitions

- All computers and devices with access to Mosaic FSI' network must have an antivirus client installed, with real-time protection.
- All servers and workstations owned by Mosaic FSI or permanently in use at Mosaic FSI facilities must have an approved, antivirus. That also includes travelling devices that regularly connects to the Mosaic FSI network or that can be managed via secure channels through Internet.
- Mosaic FSI computers permanently working in other Mosaic FSI network may be exempted from the previous rule if required by the Security Policies of the other organisation, provided those computers will be protected too.
- Visitors computers and all computers that connect to Mosaic FSI network are required to stay "healthy", i.e., with a valid, updated antivirus installed.
- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms, and rootkits)
- All Workstations, servers, software, system components etc. owned by Mosaic FSI must have up-to-date system security patches installed to protect the asset from known vulnerabilities. Software must have automatic updates enabled for system patches released from their respective vendors.

Information Classification Policy

This section of the Security Policy defines a framework for the classification and use of the information according to the importance and risk.

Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality, and availability of Mosaic FSI information.

Scope

This policy applies to all the information created, owned, or managed by the Organisation, including those stored in electronic or magnetic forms and those printed in paper.

Policy Definitions

- Information owners must ensure the security of their information and the systems that support it.
- Information Security Management is responsible for ensuring the confidentiality, integrity and availability of Mosaic FSI assets, information, data and IT services.
- Any breach must be reported immediately to the Information Security Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.
- Information at Mosaic FSI is classified according to its security impact. The current categories are confidential, sensitive, shareable, public and private.
- All company documents should present the security classification in the header or footer of the document.
- Information defined as confidential has the highest level of security. Only a limited number of persons must have access to it. Management, access, and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.
- Information defined as sensitive must be handled by a greater number of persons. It is needed for the daily performing of jobs duties but should not be shared outside of the scope needed for the performing of the related function.
- Information defined as shareable can be shared outside of the limits of
- Mosaic FSI, for those clients, organizations, regulators, etc. who acquire or should get access to it.
- Information defined as public can be shared as public records, e.g., content published in the company's public Web Site.
- Information deemed as private belongs to individuals who are responsible for the maintenance and backup.
- Information is classified jointly by the Information Security Officer and the Information Owner.
- For information on records retention and protection go to Mosaic FSI records and protection policy.

Remote Access Policy

This section of the Security Policy lists policies for the secure remote access to Mosaic FSI internal resources.

Purpose

The Remote Access Policy section defines the requirements for the secure remote access to Mosaic FSI internal resources.

Scope

This policy applies to the users and devices that need access Mosaic FSI internal resources from remote locations.

Policy Definitions

- It is the responsibility of Mosaic FSI employees, contractors, vendors, and agents with remote access privileges to Mosaic FSI corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Mosaic FSI.
- To gain access to the internal resources from remote locations, users must have the required authorisation. Remote access for an employee, contractor external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
- Only secure channels with mutual authentication between server and clients must be use for remote access. Both server and clients must receive mutually trusted certificates.
- Remote access to confidential information should only be from approved devices. Exception to this rule may only be authorized in cases where is strictly needed.
- Users must not connect from public computers unless the access is for viewing public content.
- Third parties accounts with access to Mosaic FSI network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to Mosaic FSI internal networks via remote access technologies will be monitored on a regular basis.

Outsourcing Policy

This section of the Security Policy lists policies for the outsourcing of IT services, functions, and processes.

Purpose

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions, and processes.

Scope

This policy applies to Mosaic FSI; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

Policy Definitions

- Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
- Whenever possible, a bidding process should be followed to select between several service providers.
- The service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
- Audits should be planned to evaluate the performance of the service provider before and during the provision of the outsourced service, function, or process. If Mosaic FSI has not enough knowledge and resources, a specialized company should be hired to do the auditing.
- A service contract and defined service levels must be agreed between Mosaic FSI and the service provider.
- The service provider must get authorization from Mosaic FSI if it intends to hire a third party to support the outsourced service, function, or process.

ANNEX

Glossary

This section of the Security Policy provides the definitions of terms, acronyms, and abbreviations required to understand this document.

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An IT service provider that is part of a different organization from its customer.
Identity	A unique name that is used to identify a user, person or role.

Information Security Policy	The policy that governs Mosaic FSI approach to information security management
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.