
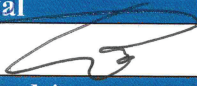
	Document ID:
	MIS-PROCEDURE-008
	Revision:
	A

Information Security Policy

Originator Approval	Date Approval
Ryan Shih 	12/01/2022
Manager Approval	Date Approval
Edward Zhang 	12/01/2022
Management Approval *	Date Approval

Revision History

Revision	Description of Change	Affected Section	Release Date	Originator
A	Initial Release	ALL	06/01/2020	Ryan Shih

Policy

The Management of AMAX, located at 1565 Reliance Way Fremont, CA 94539, is committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets throughout their organization in order to preserve its competitive edge, cash flow, profitability, legal, regulatory, and contractual compliance, and commercial image. Information and information security requirements will continue to be aligned with AMAX's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

AMAX has appointed the Head of MIS to oversee the implementation and management of information and cybersecurity processes, especially with regard to compliance with relevant laws and regulations.

AMAX's current strategic business plan and risk management framework provides the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability, and Risk Treatment Plan identify how information-related risks are controlled. The Head of Risk is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Fundamental to this policy are:

- Safeguarding the personal information of employees and consumers
- Information security generally
- Data governance and classification
- Asset inventories and device management
- Access controls and identity management
- Business continuity and contingency plans, and disaster recovery planning and resources
- Systems operations and availability
- Systems and network security
- Systems and network monitoring
- Systems and application development and quality assurance
- Physical security and environmental controls
- Vendor and third-party service provider management
- Risk assessment
- Data backup procedures

- Anti-malware and control of mobile and malicious code
- Information security incident reporting

AMAX aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organization, the results of risk assessments, and the risk treatment plan.

All Employees are expected to comply with this policy and with the ISMS that implements this policy. All Employees will receive training. The consequences of breaching the information security policy are set out in the organization's disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

In this policy, 'personal information' is defined as:

A natural person's first and last name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to a person's financial account.

In this policy, 'information security' is defined as:

Preserving

This means management, all full-time or part-time Employees/Staff, sub-contractors, project consultants, and any external parties have been, and will be, made aware of their responsibilities (defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in Section 16 of the Manual), and to act in accordance with the requirements of the ISMS. All Employees/Staff will receive information security awareness training and more specialized Employees/Staff will receive appropriately specialized information security training.

the availability,

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient and AMAX must be able to [detect and] respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information. There must be appropriate business continuity plans. [Add any other specific control/compliance requirements.]

confidentiality,

This involves ensuring information is only accessible to those authorized to access it, thereby preventing both deliberate and accidental unauthorized access to AMAX's information [and proprietary knowledge] and its systems [including its network(s), website(s), extranet(s), and e-commerce systems]. [Add any other specific control/compliance requirements.]

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification of either physical assets or electronic data. There must be appropriate contingency [including for network(s), e-commerce system(s), website(s), extranet(s)] and data backup plans and security incident reporting. AMAX must comply with all relevant data-related legislation in those jurisdictions within which it operates. [Add any other specific control/compliance requirements.]

of the physical (assets)

The physical assets of AMAX, including, but not limited to, computer hardware, data cabling, telephone systems, filing systems, and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones, and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes, and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

of AMAX.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a breakdown in the availability, confidentiality, or integrity of the physical or electronic information assets of AMAX. [AMAX, will document the responsive actions taken in connection with any incident involving a security breach, and conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.]