



Information Security Policy

Purpose

Attra recognises that information and the associated processes, systems and networks as valuable assets. Through the company's security policies, procedures and structures, the management will facilitate the secure an uninterrupted flow of information, both within the company and in external communications. The company believes that security is an integral part of the information sharing which is essential to **Attra** and its corporate endeavours and the policies outlined below are intended to support Information Security measures throughout the company.

This policy is based on recommendations contained in **AS/NZS ISO/IEC 27001:2006**–Information Security Management System.

Definition

For the purposes of this document, Information Security is defined as the preservation of:

Confidentiality: protecting information from unauthorised access and disclosure;

Integrity: safeguarding the accuracy and completeness of information and processing methods; and

Availability: ensuring that information and associated services are available to authorised users when required.

Information exists in many forms such as, printed or written on paper, stored electronically, transmitted by post or using electronic means, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

Protection of Data

Attra holds and processes information about employees, contractors, and core business practices of financial, legal and operational for administrative and commercial purposes. When handling such information, all employees or others who process or use any such information, must comply with the responsibilities set out in the information security policy.

Information Security Responsibilities

The company believes that Information Security is the responsibility of all employees of **Attra**. Every person handling information or using company information systems is expected to observe the Information Security policies and procedures, at all times.

This policy is the responsibility of all employees, and the administration of the policy will be undertaken by the **Senior Management**. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of the Information Security Policy is managed through the **Infrastructure Manager** and other designated personnel with security responsibilities in specified areas of the Company.

Information Security Education and Training

Attra recognises the need for all employees and other users of company systems to be aware of information security threats and concerns, and to be equipped to support the company's Information Security Policy in the course of their job duties. The **Infrastructure Manager** shall implement a training programme for each class of users and, at the request of the company's senior management, shall provide further training in Information Security matters to specific requirements.

Compliance Requirements

Authorised Use

Attra IT facilities shall only be used for authorised purposes by authorized personnel. The **Infrastructure Manager** may periodically monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

Monitoring of Operational Logs

The **Infrastructure Manager** shall maintain operational logs and permit their inspection to specific administrative staff identified by **Senior Management**. The Information Security Policy and its procedures shall be monitored by periodic audits for compliance with security implementation standards.

Access to Records & Documentation

In general, the privacy of users' files will be respected but the company reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with company policies and regulations, and to determine which records are essential for the Company to function. Authorisation for access must be obtained from the **Chief Executive Officer** or nominee, and shall be limited to the perusal of contents and the action necessary to resolve the situation.

Protection of Software

To ensure that all software and licensed products used within the company comply with the Copyright Act, the company will perform audits regularly to ensure that only authorised products are being used, and will keep a record of the results of those audits. Unauthorised copying of software or use of unauthorised products may be subjected to disciplinary, and where appropriate, legal proceedings.

Virus Control

Attra will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of company systems, computers, including laptops, shall comply with best practice, in order to ensure that up-to-date virus protection is maintained on their machines.

Retention and Disposal of Information

All employees of **Attra** have a responsibility to consider security when disposing of information. Senior Management shall establish procedures appropriate to the information held and processed by them and ensure that all employees are aware of those procedures. Retention periods for all information inclusive of personal information are identified as per information disposal and retention guidelines as documented in the Procedures for Control of Documents and Records.

Reporting

All employees of **Attra** and other users are expected to report immediately by electronic or verbal means to the **Infrastructure Manager**:

- Any observed or suspected security incidents where a breach of the company's security policies has occurred,
- Any security weaknesses in, or threats to, systems or services.
- Any Software malfunctions

Business Continuity

Attra will implement, and regularly update, a business continuity management process to counteract interruptions to normal company activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

Customer Data

Where ever authorized employees having access to customer data or others who process or use any such data must comply with the responsibilities set out in the information security policy. Therefore, the specific implications of the above data management policy apply to when accessing or processing of customer data.

When ever the customer request and specifies additional safeguard measures agreed upon at or during the contract / project period (by the customer to Attra), all employees are expected to abide by these measures as specified by the customer. Such customer data management requests must be communicated to the business and all project staff via internal memo and continual reinforcement by project managers during the contract period.