Altaira Information Technology (IT) Policy

1. Policy Statement & Purpose

Altaira is committed to providing a secure and reliable IT environment to support our business operations and protect our data, assets, and reputation. This policy outlines the acceptable use of Altaira's IT resources and the responsibilities of all users to ensure the **confidentiality**, **integrity**, and **availability** of our information systems. The purpose is to minimise security risks, prevent data breaches, and ensure legal and regulatory compliance across all our locations, including our offshore offices.

2. Scope

This policy applies to **all Altaira employees**, contractors, and third-party agents, regardless of their location (onshore or offshore). It covers all company-owned or leased IT assets, including but not limited to:

- Desktops, laptops, and mobile devices
- Servers and network infrastructure
- Software, applications, and cloud services (e.g., Microsoft 365)
- Company-provided internet and network access
- All corporate and client data

3. Acceptable Use of IT Resources

3.1 General Use

- Company IT resources are provided for business purposes. **Limited personal use** is permitted, provided it does not interfere with job performance, consume significant resources, interfere with IT operations, or violate any other section of this policy.
- Users must not engage in any activity that is illegal, unethical, or could harm Altaira's reputation. This includes but is not limited to harassment, accessing or distributing offensive material, and violating copyright laws.

3.2 Email and Communications

- All communications conducted via Altaira's systems are considered company records and may be subject to monitoring.
- Do not send unsolicited bulk emails (spam) or engage in phishing attempts.

- Be cautious of suspicious emails. Report any potential phishing attacks to the IT Department immediately using the designated procedure.

3.3 Internet Access

- Accessing or downloading illegal, malicious, or inappropriate content is **strictly prohibited**.
- The use of peer-to-peer file-sharing software is forbidden on the corporate network.
- Users should have no expectation of privacy when using company internet resources.

4. Data Security & Management

4.1 Data Classification

All company data must be classified as **Public**, **Internal**, **Confidential**, or **Restricted**.

- **Restricted:** Data that relates to the high level financial/operational aspects of the business that would catastrophic if disclosed to unauthorised individuals. Access should be limited to members of the executive team and only then, those members who have a need to know.
- **Confidential:** Highly sensitive data (e.g., client health records, financial data). Requires a high level of protection and is not to be shared with employees who are not cleared to access confidential information.
- **Internal:** Data for internal business use that is not intended for public disclosure (e.g., internal reports, project plans, employee details). This is information used on a day to day basis by employees to perform key functions of their jobs.
- **Public:** Information approved for public release (e.g., marketing materials).

4.2 Data Handling

- **Data labelled Internal or above** must not be copied to unauthorised devices, personal cloud storage (like personal Google Drive or Dropbox), or sent via unauthorised email providers.
- Use company-approved secure file transfer methods for sharing sensitive information.
- All laptops and mobile devices containing confidential data **must be encrypted**.
- Securely dispose of sensitive physical documents by shredding them.

4.3 Access Control

- Access to data and systems will be granted based on the **Principle of Least Privilege**, meaning users will only have access to the information necessary to perform their job duties.
- Passwords must be complex (minimum 12 characters, including uppercase, lowercase, numbers, and symbols) and changed every 90 days.
- **Multi-Factor Authentication (MFA)** is mandatory for all remote access and access to critical cloud

services.

5. Software & Hardware Management

5.1 Software

- Only software that has been approved and licensed by Altaira may be installed on company devices.
- **Unauthorised software installation is prohibited** to prevent malware and licensing issues.
- All software must be kept up-to-date with the latest security patches.

5.2 Hardware

- All company-provided hardware is the property of Altaira and must be returned upon termination of employment.
- Users are responsible for the physical security of their assigned devices. Devices must not be left unattended in public places.
- Any lost or stolen device must be reported to the IT Department and your manager **within one hour** of discovery.

6. Offshore Office Considerations

Altaira's commitment to security and compliance extends equally to our offshore operations. The following provisions are critical:

6.1 International Data Transfer

- All transfers of personal or confidential client data between Australia and the offshore office must comply with the Australian Privacy Principles (APPs).
- Data will be transferred only through **secure, encrypted channels** (e.g., company VPN, secure FTP).
- The offshore office is prohibited from storing sensitive Australian client data on local servers unless explicitly approved and secured in line with Australian standards.

6.2 Compliance with Local and Australian Law

- The offshore office must adhere to all local data security and privacy laws in its jurisdiction.
- Where local laws conflict with this policy or Australian law, the **stricter standard shall apply**. The legal department must be consulted in such cases.

6.3 Secure Remote Access

- All connections from the offshore office to Altaira's primary network in Australia **must be made via the corporate VPN**.

- Split-tunnelling on the VPN is disabled to ensure all internet traffic from offshore company devices is routed through Altaira's security infrastructure for monitoring and filtering.

6.4 Physical Security

- The offshore office must meet Altaira's standards for physical security, including secure access controls (e.g., swipe cards), surveillance systems, and a clean desk policy.
- Access to server rooms or network closets must be restricted to authorised IT personnel only.

7. Policy Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract. Illegal activities will be reported to the relevant authorities.

The IT Department will conduct regular audits to ensure compliance with this policy. By using Altaira's IT resources, you agree to abide by the terms outlined in this document.