**INFORMATION SECURITY POLICY**
**S2 Management T/A Leichhardt Accommodation**

**1. Purpose**
The purpose of this Information Security Policy is to protect the integrity, confidentiality, and availability of all digital and physical information assets handled by S2 Management T/A Leichhardt Accommodation (hereafter “LAV”). This policy outlines the standards and responsibilities for managing and safeguarding sensitive data related to employees, contractors, guests, suppliers, and business operations.

**2. Scope**
This policy applies to all employees, contractors, and third parties who access LAV systems, devices, or information, whether onsite or remotely.

**3. Policy Statement**

LAV is committed to safeguarding all information and systems against internal and external threats. We uphold best practices aligned with Australian Privacy Principles (APPs) and applicable laws and regulations, including the **Privacy Act 1988 (Cth)** and **Notifiable Data Breaches (NDB) Scheme**.

**4. Key Principles**

**4.1 Confidentiality**
Information must only be accessed or shared by authorised personnel with a legitimate business need.

**4.2 Integrity**
Data must be accurate, complete, and protected against unauthorised modification.

**4.3 Availability**
Information and systems must be available to users when required, with proper backups and continuity plans in place.

**5. Information Handling & Access**

* Only authorised personnel should access guest, employee, or operational data.
* All passwords must be kept secure and never shared.
* Confidential information (including guest or staff files) must not be discussed in public or open areas.
* Sensitive documents must be stored in secure locations, both physically and digitally.

**6. Device and Systems Security**

* All devices must have password protection and automatic screen locking.
* Antivirus software and system updates must be maintained on all work devices.
* Use of USB drives or external devices must be approved by management.
* Remote access to company systems must use secure connections and follow authentication procedures.

**7. Email, Internet, and Communication**

* Company email is to be used for professional communication only.
* Attachments and links in unsolicited emails must not be opened.
* Personal use of company internet must be kept to a minimum and must not involve inappropriate or illegal sites.

**8. Third Parties & Vendors**

* Any third-party access to systems or data must be authorised and documented.
* Vendors must agree to information security terms before access is granted.

**9. Data Retention & Disposal**

* Personal and business data must only be retained for as long as necessary.
* All records must be disposed of securely (shredding paper, secure deletion of digital files).

**10. Breaches & Reporting**

All staff must immediately report:

* Lost or stolen devices
* Suspected unauthorised access
* Phishing attempts
* Accidental data exposure

Reports should be directed to your Manager or sent confidentially to:
**rynaard@lavmoranbah.com.au**

Management will assess and, where required, escalate or report the breach according to the **Notifiable Data Breach Scheme**.

**11. Training & Compliance**

* All staff must complete Information Security Awareness training upon commencement and at least annually thereafter.
* Breaches of this policy may result in disciplinary action, up to and including termination of employment.

**12. Policy Review**

This policy will be reviewed **annually**, or as required due to changes in legislation, risk, or business operations.

**Authorised by:**
**S2 Management | Leichhardt Accommodation**
**Effective Date:** April 2025
**Saved Location:** OneDrive > Policies > Information Security