PINEAPPLE PARTNERS

Data Backup Procedure

Title of Policy Document **Issue Date and Version**	Data Backup Procedure January 2026 (Version 1)
Author / Department	Compliance Manager
Signed off by	 Director
Next review date	January 2027
Distribution	All services
First issue date	January 2026

1. Purpose

This procedure describes how Pineapple Partners protects its business data against loss, whether through hardware failure, accident, theft or malicious action, and how we restore it when something goes wrong.

2. What is backed up

- Core business systems: our CRM and candidate database, which are cloud-hosted with the provider's own resilience, plus our independent scheduled exports.
- Documents and email: held in cloud services (Microsoft 365) with provider-side redundancy and versioning.
- Website and policy library: source files and documents held both locally and in the hosting platform, redeployable at any time.

3. How and how often

Automated backups run daily for database systems, with full weekly cycles retained on a rolling basis. Backup copies are retained for three months before being overwritten, so any accidental change or deletion within that window can be recovered. Backups are stored encrypted, in a separate location from the live data, and access is limited to authorised staff.

4. Restoring data

Data can be restored quickly, typically within minutes of a completed backup for database content. Restores are requested through the Director, carried out by an authorised person, and logged: what was restored, from which point in time, by whom and why.

5. Testing and review

We test restores periodically rather than assuming backups work, an untested backup is a hope, not a plan. The procedure is reviewed annually, and immediately after any incident in which data recovery was needed, so lessons are built back in. Responsibility for this procedure sits with the Director, Mathew Vandermotten.