Privacy and Cyber Security Policy

FR8 — Information Systems & Data Protection

Client / Data Controller	FR8 (Vanuatu)
Prepared by	ODC Ltd — IT Managed Services Provider
Document owner	Ted Fines, General Manager, ODC Ltd
Contact	ted@odc.vu | +678 755-3332
Version	1.0
Date issued	15 June 2026
Review cycle	Annual, or on material change to systems or law
Status	Active

1. Purpose and Scope

This document sets out the privacy and cyber security controls applied to the information systems of FR8 (“the Company”). These systems are administered on the Company’s behalf by ODC Ltd (“ODC”) under a managed services arrangement.

The policy describes the technical and organisational measures in place to protect personal and client information held or processed by the Company, including data exchanged with international moving and logistics partners. It is intended to demonstrate, to the Company’s partners and to third parties conducting due diligence, that client data is protected throughout its handling.

Scope covers all Company email, file storage, endpoints (workstations and mobile devices), network infrastructure, and the cloud services used to conduct business.

2. Cyber Security Protocols

ODC applies a layered set of controls across the Company’s systems:

- Multi-factor authentication (MFA) is enforced on email and other key business systems, so that a password alone is not sufficient to gain access.
- A business-grade firewall is maintained at the network perimeter, controlling traffic into and out of the Company network.
- Managed endpoint protection (antivirus and anti-malware) is installed on all workstations and servers, centrally monitored and kept current.
- Inbound email is filtered for spam, malware, and known phishing threats before delivery to users.
- Systems are centrally monitored through a remote monitoring and management (RMM) platform, which is also used to apply security updates and operating-system and application patches in a timely manner.
- Administrative access to systems is limited to ODC personnel responsible for support and is itself protected by MFA.

3. Storage of Personal Information

The Company's data is held in access-controlled, cloud-hosted business systems (Microsoft 365). These services are operated in enterprise data centres with their own physical and infrastructure security controls.

- Access to information is granted on a role basis — staff are given access only to the data they need to perform their duties.
- Data in Microsoft 365 is encrypted in transit and at rest by the platform.
- Backups of business-critical data are taken on a regular basis and held securely, to support recovery in the event of loss, corruption, or a security incident.
- Where data is shared with overseas partners in the course of a move, it is limited to the information necessary for that engagement.

4. Password and Access Management

Credential controls applied across Company accounts:

- Minimum length and complexity requirements are enforced on passwords.
- Credentials are not shared between users, and reuse of passwords across accounts is not permitted.
- Multi-factor authentication is applied on top of passwords for email and key systems.
- Accounts for staff who leave the Company are disabled promptly as part of the off-boarding process.

5. Legal and Regulatory Compliance

Vanuatu has enacted data protection legislation. The Data Protection and Privacy Act No. 13 of 2024 came into force on 2 January 2025 and applies to both the private and public sectors.

The Act establishes principles for the lawful handling of personal data, including lawful and fair processing, purpose limitation, data minimisation, accuracy, and security of personal data, together with rights for individuals whose data is held. The controls described in this policy are applied in line with these principles.

The Company and ODC monitor developments in this area, including the standing-up of the supervisory authority, and will adjust practices as required to remain compliant.

6. Privacy and Cyber Security Policy Status

This document constitutes the Company's formal written privacy and cyber security policy. The controls set out here reflect the practices applied to the Company's systems on an ongoing basis by ODC as its IT provider.

The policy is reviewed at least annually, and following any material change to the Company's systems, its partner requirements, or applicable law.

7. Security Certifications

The Company does not currently hold a formal information-security certification such as ISO/IEC 27001.

As a small business operating in Vanuatu, the Company's security posture is delivered through the managed controls described in this policy rather than through a formal certification scheme. ODC, as IT provider, implements and maintains these controls and can provide further detail or evidence on request. Where a partner requires a specific assurance format, ODC will work with the Company to address it.

8. Incident Handling

In the event of a suspected security incident or data breach, ODC investigates, works to contain and remediate the issue, and supports the Company in meeting any notification obligations to affected parties and to the relevant authority. Affected partners are informed where their data may be involved.

9. Roles and Responsibilities

FR8	Owns the data; sets business requirements; ensures staff follow acceptable-use and access practices.
ODC Ltd	Implements, maintains, and monitors the technical controls described in this policy; provides support and advises on security matters.
All users	Protect their credentials, use MFA, and report suspected security issues promptly.

Issued by

ODC Ltd — IT Managed Services Provider to FR8

Ted Fines, General Manager

ted@odc.vu | +678 755-3332