Cyber Security Policy & Procedure

Reference: ISO 27001:2022 ISMS Clause A.8; FAIM (FIDI) requirements as per FD5
Applies To: MLPL operations – Logistics & Relocations

1. Purpose

The purpose of this policy/procedure is to protect the confidentiality, integrity, and availability of client, employee, and company information, including data collection, transfer, storage, and disposal within MLPL operations.

2. Scope

This procedure is applicable to MLPL operations covering logistics and relocations.

3. Reference

- ISO 27001:2022 ISMS Clause A.8
- FAIM (FIDI) requirements as per FD5

4. Responsibility And Governance

- This procedure is reviewed by the CTO.
- This procedure/policy is approved by DGM – HR & Administration.
- Concerned departmental personnel are responsible for implementation in the organisation.
- Issued and controlled by the CISO.

5. Abbreviations

Term	**Abbreviation**
Maxwell Logistics Private Limited	MAXWELL / MLPL
Chief Information Security Officer	CISO
Chief Technical Officer	CTO

Information Security Management System	ISMS
Information Security Management System Manual	ISMSM
Deputy General Manager	DGM

6. Policy

Management has decided to protect and maintain IT assets and data with confidentiality, integrity, and availability as required for business operations and protection from information security risks.

7. Procedure

Cyber security protects and maintains information using the CIA principles to manage information security risks, ensuring proper authorisation for handling information across Maxwell operations.

Cybersecurity controls apply across different areas and levels of operations.

8. Access Control

Reference Document: MLPL-IT-PR-04 (Access Control)

Access is provided to authorised personnel based on job requirements to complete assigned work.

Security controls include:

- Multi-factor authentication (MFA)
- Physical access controls
- Logical access controls

9. Network & System Security

Reference Document: MLPL-IT-PR-19 (Network Security)

Network and system security procedures define controls for protecting systems and networks against unauthorised access and security threats.

10. Incident Management

Reference Document: MLPL-IT-PR-15 (Information Incidents Management)

Information security incidents are managed through defined reporting and response procedures to ensure timely containment, investigation, and resolution.

11. Data Protection

Reference Document: MLPL-IT-PR-11 (Data Protection and Privacy)

Data protection procedures define secure practices for data collection, transfer, storage, retention, and disposal, including privacy measures where required.

12. Vendor And Partner Security

Reference Document: MAXWELL-SOP-01/PUR (Purchasing Procedure)

Supplier management includes:

- supplier selection controls
- supplier performance monitoring
- communication of relevant policies, including FIDI requirements, to approved suppliers

13. Backup And Recovery

Reference Document: MLPL-IT-PR-02 (Backup & Restoration)

Backup and restoration procedures ensure critical operational data and systems can be recovered in case of disruption.

14. Employee Awareness

Reference Document: MLPL-HR-SOP-01 (HR & Admin Procedures)

New employees receive induction training after joining formalities and completion of required documentation. Ongoing awareness is supported through internal communication and training where needed.