

	Maxwell Logistics Private Limited Cyber Security - Policy & Procedure	QMS & ISMS
---	--	------------

1.0 Purpose

The purpose of this Policy/ procedure is to protect Confidentiality, integrity and availability of client, Employees and Company information including data collection, transfer, storage and disposal in MLPL operations.

2.0 Scope

This procedure is applicable to MLPL operations – Logistics & Relocations.

3.0 Reference

ISO 27001:2022 ISMS Clause no: A.8
FAIM (FIDI) requirements as per FD5

4.0 Responsibility

- This procedure is reviewed by CTO.
- This procedure/ policy approved by DGM- HR &Admin.
- Concerned Dept personnel are responsible to implement in Org.
- Issued and Controlled by CISO.

5.0 Abbreviations

Term	Abbreviation
MAXWELL/ MLPL	Maxwell Logistics Private Limited
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
ISMS	Information Security Management System
ISMSM	Information Security Management System Manual
DGM	Deputy General Manager

6.0 Policy

Management decided to protect and maintain IT Assets including data with Confidentiality, Integrity and availability as required to complete business operations and protect from Information security Risks.

7.0 Procedure

Cybersecurity is to protect and maintain the Information with CIA from Information Security Risks and maintain with proper authorization for handling of information in MAXWELL.

Cyber Security involves at different areas of operations and different levels in MAXWELL operations.

	Maxwell Logistics Private Limited Cyber Security - Policy & Procedure	QMS & ISMS
---	--	------------

7.1 Access Control

- Refer Document number: MLPL-IT-PR-04 for access control details in MLPL operations.
- In brief, Access given to concerned personnel based on nature of Job to complete their work
- Multi Factor Authentication (MFA), Physical Access, Logical Access also defined and provided for authorized users.

7.2 Network & System Security

- Refer Document number: MLPL-IT-PR-19 for network security procedure details in MLPL operations

7.3 Incident Management

- Refer Document number: MLPL-IT-PR-15 for Information Incidents Management procedure details in MLPL operations

7.4 Data Protection

- Refer Document number: MLPL-IT-PR-11 for Data protection and Privacy procedure details in MLPL

7.5 Vendor and Partner Security

- Refer Document number: MAXWELL-SOP-01/PUR for Purchasing procedure details in MLPL
- Covered about Supplier Management including selection, Suppliers performance monitoring, communication about FIDI policies to approved Suppliers etc.

7.6 Backup and Recovery

- Refer Document number: MLPL-IT-PR-02 for Backup & Restoration details in MLPL operations

7.7 Employee Awareness

- Refer Document number: MLPL-HR-SOP-01 for HR & Admin Procedures details in MLPL.
- For New Employees Induction will be provided after completion of joining formalities and collection of new employee's documents.
- For present existing Employees, Trainings will be identified, planned and documented as Training Plan/ Calendar on annual basis.
- FAIM Policies also will be communicated about established Policies and procedures to improve their awareness and for effective implementation.

	Maxwell Logistics Private Limited Cyber Security - Policy & Procedure	QMS & ISMS
---	--	------------

8.0 Output / Record

Retention Period

Access Reports	03 Years
Employee Training Records	03 Years
Information Incident Reports	03 Years
Information Incident Investigation Reports	03 Years

Reviewed By CTO	Approved by DGM – HR & Admin	Issued and Controlled by CISO
--------------------	---------------------------------	----------------------------------

	Maxwell Logistics Private Limited Backup and Restoration - Policy & Procedure	ISO 27001:2022
---	--	----------------

1.0 Purpose

The purpose of the Data Backup & Restoration Policy/ procedure is to establish and implement procedures to create and maintain retrievable organizational information that are necessary for recovery activities.

2.0 Scope

Backup / restore of the data is strictly limited to organization information only. No personal data will be entertained. Applicable to MLPL operations at Secunderabad.

3.0 Reference

ISMS Manual section– MLPL-ISMSM-08, ISO 27001:2022 Clause no: A.8.13

4.0 Responsibility

- This procedure is reviewed by CTO.
- This procedure/ policy approved by DGM- HR &Admin.
- Concerned Dept personnel are responsible to implement in Org.
- Issued and Controlled by CISO.

5.0 Abbreviations

Term	Abbreviation
MLPL	Maxwell Logistics Private Limited
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
ISMS	Information Security Management System
ISMSM	Information Security Management System Manual
DGM	Deputy General Manager

5.0 Policy

- 5.1 To ensure proper storage of Information in secure manner and without loss of data.
- 5.2 Information generated during MLPL operations/ activities, interaction with Customers, external service providers to be handled without loss of data by storing secure manner and maintain information security.

6.0 Procedure

- At present based on MLPL Operations there is no specific Local Server to take Backup of the Work performed on daily basis.
- MLPL management being taken service from external Service provider to host and maintain Server. MLPL Server being maintained by CtrlS at Hyderabad location.
- All users will connect to MLPL Server, which was located at CtrlS location.

	Maxwell Logistics Private Limited Backup and Restoration - Policy & Procedure	ISO 27001:2022
---	--	----------------

- Regarding the E-Mail communication data, Email service is taken from Google and no need to take Backup. As per agreement made with Cloud service provider data backup maintaining responsibility lies with them.
- However, MLPL operations related data pertaining to daily routine operations back up is taking in external HDD and storing.
- This HDD is tentatively once in 15 days/ 30 days period will be taken away from Office premises and kept at DGM-IT residence. This is full backup.
- Incremental back up is taking and is storing in MLPL IT HOD PC, at Hyderabad office premises.
- All users will update in respective folders in Server. IT team members will take backup from the server.
- Randomly data will be restored from Backup HDD / from MLPL Server.
- Related records are being maintained by IT team.

6.0 Output / Record

- Maintaining the required data in secured and make available whenever required.

Reviewed By CTO	Approved by DGM – HR & Admin	Issued and Controlled by CISO
--------------------	---------------------------------	----------------------------------

	Maxwell Logistics Private Limited Access Control - Policy & Procedure	ISO 27001:2022
---	--	----------------

1.0 PURPOSE

Established this procedure to provide guidelines to prevent unauthorized access to the MLPL's information systems.

2.0 SCOPE

The scope of the Procedure is applicable to the communications and operational process information across the MLPL.

3.0 RESPONSIBILITIES

This procedure reviewed by CTO

Approved by DGM-HR & Admin

All employees are responsible for implementing this procedure.

Issued and Controlled by CISO.

4.0 REFERENCES

ISO 27001 – 2022 Standard Clause No **A.5.15, A 5.18, A8.3, A8.5, A8.11**

5.0 POLICY

- Management decided to provide access to concerned personnel (i.e. Employees/ visitors etc) as required to fulfill their responsibilities.
- This access includes the Internet facility, Network access etc.

6.0 PROCESS /PROCEDURE

To control access to information.

Access will be controlled on the basis of business and security requirements and the user's role in the MLPL operations.

To prevent unauthorized access, users will be made aware of their responsibilities for maintaining effective access controls, particularly with regard to the use of passwords and the security of equipment and security facilities should be used to restrict access within application systems.

Controlling access to information is one of the key elements of MLPL's security controls. Access control works on two levels, the physical control and the system control.

System access control policy statements:

The following statements are the rules that will be applied to controlling access to any information system within MLPL, by employed staff and third parties.

- Controls will be applied to all IT systems to ensure that access to information is in line with the rules in this policy section. The responsibility for determining which controls are applied lies with HR & IT.
- Access to systems and information will be on a need to know and need to use basis.

	Maxwell Logistics Private Limited Access Control - Policy & Procedure	ISO 27001:2022
---	--	----------------

- Access controls will be based on user roles and departments.

6.1 User access management

6.1.1 User registration

- Allocation of a unique User ID, Email ID.
- Authorization of the access request from line manager, who is responsible for confirming the provisional user has a 'need to use' and 'need to know' the information contained within the system that is accessible via their user role.
- Access revocation procedure, authorized by HR management, initiated by user leaving or other request for revocation (changed role – no longer needed)
- As soon as an individual leaves the MLPL's employment, all his/her system logons are revoked. As part of the employee termination process, will be followed exit formalities.

6.1.2 Privilege management

Allocation and use of privileges will be restricted and controlled. Privileges are allowed to the system manager or systems programmers, allowing access to sensitive area.

Logistics related Software access privileges defined based on user type like Super User, Normal Users.

All defined users can access data through Logistics Software Package to complete their responsibilities effectively. Application is hosted in MLPL Server which was located at CtrlS.

The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached

All requests for access outside normal services must be supported by a request from the head of the department (Manager).

6.1.3 User password management

- CISO ensure that users are aware of the need to change passwords and are provided with written guidance on password confidentiality, construction, changing, storage and action to take when a password is forgotten.
- Initial passwords are issued in person by means of face to face contact (ideally at initial system training) where identity can be checked.
- Re-issue forgotten passwords following positive identification of the user

6.1.4 Reviews of user access rights

CISO will review access rights at regular intervals (at least once in 06 months) or whenever change in employees i.e. new staff is recruited or existing staff Left MLPL.

	Maxwell Logistics Private Limited Access Control - Policy & Procedure	ISO 27001:2022
---	--	----------------

6.2 User responsibilities

6.2.1 Password use

All users will be advised to:

- Keep passwords confidential
- Avoid keeping paper records of passwords
- Change passwords if they believe they have been compromised

(Informing the CISO) and when requested by a system

- Select passwords that are easy to remember, but not based on anything easy to guess, free of consecutive identical characters.
- Change temporary passwords at first log on.

6.2.2 Unattended user equipment and Data

All users will be advised to:

- Log out of PCs/Laptops when finished or leaving the desk or activate a password protected screen saver
- Printers are securely located in order that unauthorized users cannot see the data sent to the machine.

ABBREVIATIONS

Term	Abbreviation
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
DGM	Deputy General Manager
HR	Human Resources
ISMS	Information Security Management system
IT	Information Technology
MLPL	Maxwell Logistics Private Limited
NDA	Non Disclosure agreement

Records

Access Control records

Retention Period

3 years

Reviewed By CTO	Approved by DGM- HR & Admin	Issued and Controlled by CISO
--------------------	--------------------------------	----------------------------------

	Maxwell Logistics Private Limited Data Protection and Privacy - Policy & Procedure	ISO 27001:2022
---	---	----------------

1.0 Purpose

The purpose of this document is to define collection, protection, and usage of personal data & Company confidential information as per applicable laws and regulations. Personally Identifiable Information (PII) can be either collected by MLPL directly from employees or through its customers as part of business process engagements.

2.0 Scope

This policy & Procedure is applicable to MLPL operations at Secunderabad but not limited to;

- 2.1 Critical and Sensitive data such as MLPL's employee data and or Customer/Business partner data including personal data (Personally Identifiable Information or Non-public personal information).
- 2.2 Data residing in IT assets such as desktops, laptops, mobile devices, removable media, Cloud networks or in any appliance.
- 2.3 All Data storage, communication and transactions.

3.0 Reference

- ISMS Manual Sections MLPL-ISMSM-05, MLPL-ISMSM-08
- ISO 27001:2022 ISMS Clause no: A.5.33, A.5.34, A.8.7
- Information Security Incident Management - Policy and Procedure (MLPL-IT-PR-15)
- Asset Management policy and Procedure (MLPL-IT-PR-01)
- Information Classification, Labeling and handling procedure (MLPL-IT-PR-17)
- Intellectual Property Rights Policy & Procedure (MLPL-IT-PR-16)
- Backup & Restoration Policy & Procedure (MLPL-IT-PR-02)
- Acceptable Removable Media Usage Policy & Procedure (MLPL-IT-PR-09)
- Change Management Policy & Procedure (MLPL-ISMS-SOP-04)
- Acceptable E-Mail and Internet Usage Policy & Procedure (MLPL-IT-PR-08)
- Physical Security Policy & Procedure (MLPL-IT-PR-18)

4.0 Responsibility

- This procedure is reviewed by CTO.
- This procedure/ policy approved by DGM- HR &Admin.
- Concerned Dept personnel are responsible to implement in Org.
- Issued and Controlled by CISO.

5.0 Abbreviations

Term	Abbreviation
MLPL	Maxwell Logistics Private Limited
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
ISMS	Information Security Management System
ISMSM	Information Security Management System Manual
DGM	Deputy General Manager

	Maxwell Logistics Private Limited Data Protection and Privacy - Policy & Procedure	ISO 27001:2022
---	---	----------------

5.0 Policy

- 5.1 Management decided to maintain the data protection from undesired events like theft, data breach, missing, lost etc which was collected and stored in different means/ ways.
- 5.2 Established process to data protection and prevention from misuse with proper access/ authorization in MLPL operations.
- 5.3 Data shall be protected during the stages of - creation, collection, storage, access, disclosure, transmission, retention and deletion

6.0 Procedure

- 6.1 Confidentiality of data is based on the criticality of data which may be generated in MLPL operations / collected from Employees/ external Organizations etc.
- 6.2 Classification of data according to the sensitivity level and business impact shall be carried out as per the information classification policy and procedures
- 6.3 All Customers' personal data collected & processed shall be retained & disposed of as per the contract requirements
- 6.4 Data Shall be
 - 6.4.1 Fairly and lawfully processed – Access, consent, enforcement, notice and security in line with legal requirements
 - 6.4.2 Secured through the implementation of necessary controls to safeguard the Confidentiality, Integrity and availability
 - 6.4.3 Transferred to other jurisdictions only with adequate protection, as required
 - 6.4.4 Third party contract shall have clauses defined to ensure the security and privacy of the personal information
- 6.5 Data protection requirements shall be reviewed especially during contractual sign-off with customers on engagements involving confidential data access
- 6.6 While outsourcing sensitive work to Third party vendors or partnering with vendors especially involving processing of confidential data (personal, business) ; vendor assessment shall be carried out in line with the Third party security policy. In addition, confidentiality agreement shall be entered into with Third Party vendors for protecting the confidentiality of data
- 6.7 Users and custodians shall take reasonable steps to ensure that data is reliable, accurate, complete, and current for its intended use
- 6.8 Only authorized individuals will have access to the confidential data as required by them for fulfilling their job responsibilities

- 6.9 Users handling confidential data shall be made aware of the repercussions of breach or loss of data to the Organization and its business partners
- 6.10 Information security risk assessment will be conducted to assess any perceived or on-field information security risks related to the confidential personal and business information. Risk Assessment shall be carried out irrespective of hosting such data with MLPL or with Third party hosting Service providers/Cloud Service providers. Identified security risks shall be addressed.
- 6.11 User's access to the application processing & storing confidential data will be granted based on business requirements on a "need to access" and "need-to-know" basis only
- 6.12 Data Loss prevention can be done, but not limited to
 - 6.12.1 Necessary technology controls for monitoring loss of confidential data through commonly used communication channels such as E-mail, Instant Messaging and Internet connection from MLPL network to outside shall be implemented depending on the business requirement
 - 6.12.2 Workplace monitoring with the aim to protect confidential data will be carried out with proper access.
 - 6.12.3 Any loss, breach or unauthorized access of confidential data processed by MLPL will be reported by Users through the Incident Reporting procedure.

7.0 Output / Record

Retention Period

- | | |
|---|-------------------|
| • Incident Report/ Incident Investigation Reports | 3 Years |
| • Contractual Agreements | Validity + 1 year |

Reviewed By CTO	Approved by DGM – HR & Admin	Issued and Controlled by CISO
--------------------	---------------------------------	----------------------------------

	Maxwell Logistics Private Limited Information Security Incident Management - Policy & Procedure	ISO 27001:2022
---	---	----------------

1.0 Purpose

The purpose of this procedure is to provide guidelines to ensure secure handling of the information security incidents in MLPL Operations.

2.0 Scope

The scope of this procedure is applicable across the DCTI's information security boundaries for securing and handling the information security incidents at MLPL operations, Secunderabad.

3.0 Reference

ISO 27001:2022 ISMS Clause no: A 5.24, A 5.25, A 5.26, A5.27 & A 8.16

4.0 Responsibility

- This procedure is reviewed by CTO.
- This procedure/ policy approved by DGM- HR &Admin.
- Concerned Dept personnel are responsible to implement in Org.
- Issued and Controlled by CISO.

5.0 Abbreviations

Term	Abbreviation
MLPL	Maxwell Logistics Private Limited
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
ISMS	Information Security Management System
ISMSM	Information Security Management System Manual
DGM	Deputy General Manager

5.0 Policy

5.1 Management decided to capture, investigate and Root cause analysis to take appropriate actions to reduce risk including identified potential Information / Physical security Incidents.

6.0 Procedure

6.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESS

• Reporting Information Security Events/ Incidents

In case of any event/ problem connected with software, hardware, Virus, hacking, network access, HR related issues/ events following steps are performed.

- All the employees are required to report any incident to CISO / CTO by Email, if they encounter any of the problems listed above.

	Maxwell Logistics Private Limited Information Security Incident Management - Policy & Procedure	ISO 27001:2022
---	---	----------------

- The reported incident will be forwarded to the concerned department/ team for their actions. The department/ team records in the incident report based on the impact to the organization. Suitable Root cause analysis is done to prevent re-occurrence.
- Third parties/ suppliers/ customers are required to report the incidents through e-mail to CISO or CTO or verbally or in visitors register at reception.

Associates can propose corrective action for the nonconformity they addressed.

- **Reporting Information Security Weakness**

- All the employees, customers and Third party users are required to report the Security weaknesses observed or suspected in the information systems or services to the Incident Management Team / HR Team.
- The Incident Management Team identifies the risks and agree upon appropriate control with the concerned Dept and incorporate into the contract in case of using external facilities.

Information obtained from the above are taken as corrective actions and implemented based on the impact.

- **MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS**

- **Responsibility**

CISO / CTO/ DGM-IT / DGM- HR & Admin is responsible to act for the identified incidents in MLPL.

Potential incidents are given below for reference;

- Accidental deletion of data / information in storage systems,
- Virus Attacks,
- Power failure for sensitive systems (or) group of computers
- Internet dis-connectivity.
- E-mail problems etc.
- Strikes / Political Disturbances

- **Investigation of Incidents**

- Root cause analysis is performed for security incidents. The appropriate corrective actions are taken for the issues.
- Incident Management forum will monitor the effectiveness of the actions taken and record as part of incident investigation report format **(MLPL-IT-FT-07)**.
- When the Issues are closed, a formal mail will be replied to the concerned employee.
- Will update the Incidents details in defined Incident Tacker format **(MLPL-IT-FT-08)**

	Maxwell Logistics Private Limited Information Security Incident Management - Policy & Procedure	ISO 27001:2022
---	---	----------------

- Learning from Information Security Incidents
Incident Management Team collects the information of the security incidents from the concerned team and evaluates the number of events occurred under each type. The frequency and the impact for the concerned as also recorded.
- Collection of Evidence
The Incident Management Team collects the evidence relating to an information security breach to comply with the statutory, regulatory or contractual obligations and avoid breaches of criminal or civil law.

6.0 Output / Record

Retention Period

Incident Tracker Format (MLPL-IT-FT-08)	03 Years
Incident Investigation Report Format (MLPL-IT-FT-07)	03 Years
Corrective Action Report Format (MLPL-IT-FT-06)	03 Years

Reviewed By CTO	Approved by DGM – HR & Admin	Issued and Controlled by CISO
--------------------	---------------------------------	----------------------------------

	Maxwell Logistics Private Limited Network Security - Policy & Procedure	ISO 27001:2022
---	--	----------------

1.0 Purpose

The purpose of this Policy/ procedure is to provide guidelines to establish & implement operational procedure to maintain secure communication in MLPL network.

2.0 Scope

This procedure is applicable to MLPL network at Secunderabad.

3.0 Reference

ISO 27001:2022 ISMS Clause no: A.8.20

MLPL-ISMS-DOC-10 : Contact with Special Interest Group

4.0 Responsibility

- This procedure is reviewed by CTO.
- This procedure/ policy approved by DGM- HR &Admin.
- Concerned Dept personnel are responsible to implement in Org.
- Issued and Controlled by CISO.

5.0 Abbreviations

Term	Abbreviation
MLPL	Maxwell Logistics Private Limited
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
ISMS	Information Security Management System
ISMSM	Information Security Management System Manual
DGM	Deputy General Manager
SIG	Special Interest Group

5.0 Policy

5.1 Management defined policy aims to safeguard the integrity and confidentiality of data and information transfer, ensuring protection from potential risks, threats and unauthorized access.

5.2 By securing the network's communication links, the policy will help mitigate the propagation of network-related vulnerabilities and ensure the continuous and safe operation of communication.

6.0 Procedure

Network Security Control

6.1 The IT department will ensure established security procedures and controls are deployed to ensure security of the information and software being exchanged through insecure communication lines.

	Maxwell Logistics Private Limited Network Security - Policy & Procedure	ISO 27001:2022
---	--	----------------

- 6.2 The IT department will be responsible for the administration of the MLPL IT Infrastructure devices.
- 6.3 CTO/ The IT Infrastructure Administrator will maintain a list of privileged users from the IT department; the third-party vendors and others who can access the routers, switches, firewalls, servers and other network devices including security devices.
- 6.4 CTO/ IT Executive will be responsible for monitoring security measures and ensuring the smooth operation of the network and based on Cyber security updates from SIG.
- 6.5 Administrative privilege to all the devices of MLPL will be provided to the authorized users by management only.
- 6.6 Access to local system control utilities (e.g. Batch Files, Unix Scripts etc.) will be controlled. These utilities will be installed on local PCs and will be intended for use by the IT department only to assist end-users in troubleshooting and problem solving.

6.0 Output / Record

- Nil

Reviewed By CTO	Approved by DGM – HR & Admin	Issued and Controlled by CISO
--------------------	---------------------------------	----------------------------------