1. PURPOSE - The purpose of this policy is to establish a structured and controlled framework for protection of information assets so that confidentiality, integrity, and availability of information are maintained at all times.

This policy ensures that all information systems, data, and communication are protected against unauthorized access, misuse, loss, or damage and that risks to information assets are identified, assessed, and controlled.

2. SCOPE - This policy applies to all employees, contractors, systems, devices, and information assets of Telema Electricals Private Limited including physical, digital, and verbal information.

This policy covers access control, password management, data protection, system usage, monitoring, and risk management.

3. DEFINITIONS - For the purpose of this policy, the following definitions shall apply:

3.1 Information asset means any data, document, system, or resource containing company information.
3.2 Confidentiality means protection of information from unauthorized access.
3.3 Integrity means accuracy and completeness of information.
3.4 Availability means accessibility of information when required.

4. OVERALL RESPONSIBILITY

4.1 The Director shall ensure enforcement of this policy and overall ISMS effectiveness.
4.2 The HR Department shall manage access control, maintain records, and monitor compliance.
4.3 The IT/System responsible person shall ensure system security, implementation of controls, and monitoring.
4.4 Department Heads shall ensure secure use of information within their teams.
4.5 Employees shall protect information and comply with all security requirements.

5. ABBREVIATIONS

- HR – Human Resources

6. ACTIVITY DESCRIPTION

6.1 The company shall ensure protection of all information assets by maintaining confidentiality, integrity, and availability at all times.
6.2 All information including digital, physical, and verbal communication shall be protected against unauthorized access, disclosure, alteration, or destruction.
6.3 The company shall identify, assess, and manage risks to information assets and shall implement appropriate controls to mitigate identified risks.
6.4 The company shall comply with all applicable legal, regulatory, and contractual requirements related to information security.
6.5 User access to systems, applications, and data shall be granted only after approval and records shall be maintained in the personal file of the employee.
6.6 Access shall be granted based on job role and minimum required access shall be provided.
6.7 The company shall establish internal controls to restrict physical or digital access to customer or client data by unauthorized employees or third parties.
6.8 The company shall establish internal controls to restrict physical or digital access to customer or client data by unauthorized employees or third parties.

PREPARED BY	REVIEWED & APPROVED BY
Management Representative	Director

6.9 All user access shall be reviewed at least once every 30 days.
6.10 All users shall be provided with unique user IDs and passwords and sharing of credentials shall not be permitted.
6.11 Passwords shall be communicated securely and initial passwords shall be valid for a maximum period of 3 hours and shall be changed immediately after first login.
6.12 Passwords shall meet defined strength requirements and shall be changed periodically.
6.13 Systems shall be locked when not in use and unauthorized physical access shall not be permitted.
6.14 The company shall implement measures for obtaining stakeholder consent regarding the processing, sharing, and retention of confidential information. Retention time shall be decided based on the discussions with external stakeholders.
6.15 The company shall establish an operational process to consult and inform customers or clients regarding the collection, use, sharing, and storage of their personal data.
6.16 The company shall implement measures for obtaining stakeholder consent regarding the processing, sharing, and retention of confidential information.
6.17 The company shall establish an operational process to consult and inform customers or clients regarding the collection, use, sharing, and storage of their personal data.
6.18 Confidential information shall not be shared with unauthorized persons and shall be protected during storage, processing, and transmission.
6.19 The company shall implement measures to protect third-party data from unauthorized access or disclosure.
6.20 Information shall not be copied, transferred, or stored on unauthorized devices or locations.
6.21 All systems shall be protected through appropriate security measures including antivirus, access control, and monitoring.
6.22 The company shall implement measures to protect third-party data from unauthorized access or disclosure.
6.23 Any information security incident, breach, or unauthorized access shall be reported on the same working day.
6.24 All incidents shall be recorded in the **Incident, Investigation, Action & Closure Record - (TEPL/EV/F/01).**
6.25 The HR Department shall acknowledge the incident within 1 working day and initiate review.
6.26 The IT/System responsible person shall investigate the incident within 5 working days including review of logs and access records.
6.27 The company shall establish a method to detect, respond to, and limit the impact of information security breaches to prevent further damage and reassure affected parties.
6.28 The company shall establish, implement, and maintain a structured Incident Response Plan (IRP) for effective identification, reporting, assessment, containment, investigation, response, recovery, and closure of information security incidents, confidential information breaches, unauthorized access events, cybersecurity threats, system compromise incidents, or any event that may negatively affect confidentiality, integrity, or availability of company or third-party information assets.
6.29 The Incident Response Plan shall define responsibilities, authority levels, reporting channels, escalation procedures, communication requirements, containment measures, investigation activities, recovery actions, and corrective and preventive actions necessary for effective and timely management of information security incidents and reduction of operational, legal, financial, and reputational risks.
6.30 The company shall ensure that all employees, contractors, and authorized users immediately report any suspected or actual information security incident including unauthorized access, phishing attempts, malware attacks, password compromise, suspicious system behavior,

accidental disclosure of information, loss of devices, data leakage, or misuse of confidential information through designated reporting channels without delay.

6.31 The company shall ensure that reported incidents are assessed based on severity, type of information affected, operational impact, legal implications, stakeholder impact, and potential risks to determine appropriate response actions and escalation requirements.

6.32 The company shall implement immediate containment measures wherever required in order to prevent further unauthorized access, data loss, operational disruption, malware spread, or compromise of information systems and confidential information.

6.33 The company shall conduct investigation of information security incidents through review of access records, system logs, communication records, device activity, user actions, and other relevant information necessary to determine root cause, extent of impact, affected systems, and corrective actions required.

6.34 The company shall ensure that recovery and restoration activities are implemented in a controlled manner to restore affected systems, applications, devices, or operations while ensuring continued protection of confidentiality, integrity, and availability of information assets.
The company shall ensure that customers, stakeholders, regulatory authorities, or affected parties are informed wherever required based on contractual obligations, severity of incident, applicable legal requirements, or impact on third-party information.

6.35 The company shall maintain confidentiality during incident handling activities and shall ensure that incident-related information is accessed only by authorized personnel involved in investigation, management, or recovery activities.

6.36 The company shall maintain records of information security incidents, reporting details, investigations, containment measures, recovery actions, corrective actions, stakeholder communication, and closure activities for monitoring, review, audit, and continual improvement purposes.

6.37 The company shall periodically review, test, and improve the Incident Response Plan based on incident trends, technological changes, identified vulnerabilities, operational requirements, risk assessments, and effectiveness of implemented controls in order to strengthen organizational preparedness and resilience against information security threats.

6.38 The company shall establish a method to detect, respond to, and limit the impact of information security breaches to prevent further damage and reassure affected parties.

6.39 The company shall ensure confidentiality of incident handling and shall protect individuals reporting concerns from retaliation.

6.40 Where violation is confirmed, corrective action shall be taken and system access shall be modified or revoked.

6.41 Where misconduct is identified, the case shall be recorded in the **Incident, Investigation, Action & Closure Record – (TEPL/EV/F/01)**.

6.42 Access rights shall be removed immediately upon employee exit or role change and shall be completed within 1 working day.

6.43 The company shall establish a method to detect, respond to, and limit the impact of information security breaches to prevent further damage and reassure affected parties.

6.44 The company shall establish a method to detect, respond to, and limit the impact of information security breaches to prevent further damage and reassure affected parties.

6.45 All information security records shall be maintained and reviewed at least once every 30 days.

6.46 The company shall promote security awareness and ensure that all employees understand their responsibilities.

6.47 Training on information security shall be conducted at the time of joining and refresher training shall be conducted at least once every 12 months.

PREPARED BY	REVIEWED & APPROVED BY
Management Representative	Director

6.48 The company shall ensure continual improvement of the ISMS through regular monitoring, review, and corrective actions.

6.49 No exception to this policy shall be allowed under any condition.

7. DOCUMENTED INFORMATION

7.1 **Incident, Investigation, Action & Closure Record – (TEPL/EV/F/01)**

8. KPI (KEY PERFORMANCE INDICATORS)

8.1 Quantitative KPIs

- Access approval before grant – Target: 100%
- Access reviews every 30 days – Target: 100%
- Access removal within 1 working day of exit – Target: 100%

8.2 Qualitative KPIs

- Secure information systems
- No unauthorized access
- Strong data protection
- Employee awareness

9. REVISION HISTORY

Version	Date	Description of Change	Prepared By	Approved By
1.0	01.01.25	Initial Release	HR	Director

PREPARED BY	REVIEWED & APPROVED BY
Management Representative	Director