

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

1. PURPOSE

Somindra is committed to protecting the confidentiality, integrity and availability of information and information-processing assets and to delivering reliable, secure and effective IT-enabled services to its customers.

This Integrated Information Security & IT Service Management Policy establishes the organization's overall direction and commitment towards:

- Information security and cybersecurity;
- Protection of customer, employee, supplier and business information;
- Effective management of IT-enabled services;
- Compliance with applicable legal, regulatory and contractual requirements;
- Management of information-security and IT service risks;
- Continual improvement of the Information Security Management System (ISMS) and IT Service Management System (ITSM).

2. SCOPE

This policy applies to all employees, management, contractual personnel, temporary personnel, third parties and other interested parties working for or on behalf of Somindra, and to information, technology, facilities and services within the approved certification scope.

The management-system scope covers:

“Storage, Supply, Installation, Commissioning, Technical Support and Solutions of IT, Networking, Audio/Video Solutions, Power & Energy Solutions, Imaging & Printing, Security Solutions; Storage, Supply & Installation of Telecommunication, Consumer Durables, Smart School Solution Software and Applications, Electronics and Electricals Consumables & Accessories, Automation Solution, Tools & Machinery.”

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

The policy applies to information handled through physical and electronic means, including organizational computers/laptops, network equipment, email, cloud storage, business applications, CCTV/NVR systems, customer information, project information and related records.

3. MANAGEMENT COMMITMENT

Top Management is committed to establishing, implementing, maintaining and continually improving the ISMS and ITSM system in accordance with **ISO/IEC 27001:2022** and **ISO/IEC 20000-1:2018**.

Management shall provide appropriate resources, responsibilities, infrastructure, competence and support required for effective operation of these systems.

Management shall ensure that information security and IT service requirements are considered in business decisions, customer projects, procurement, installation, commissioning, technical support and other relevant activities.

4. INFORMATION SECURITY & CYBERSECURITY COMMITMENT

Somindra shall protect information against unauthorized access, disclosure, modification, loss, misuse and destruction.

The organization shall adopt a risk-based approach to identify, assess and treat information-security risks arising from:

- Employees and third parties;
- IT assets and endpoints;
- Email and cloud services;
- Network infrastructure;
- Customer and project information;
- Cybersecurity threats;

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Physical and environmental conditions;
- Suppliers and third-party services; and
- Business and service disruptions.

Appropriate administrative, technical and physical controls shall be established based on identified risks and applicable requirements.

5. IT SERVICE MANAGEMENT COMMITMENT

Somindra is committed to delivering IT-enabled products, solutions and services in a controlled, consistent and customer-focused manner.

The organization shall establish appropriate arrangements for:

- Understanding customer and service requirements;
- Planning and delivering services;
- Installation, configuration and commissioning;
- Service requests and incidents;
- Service availability and continuity;
- Change and configuration management;
- Supplier and third-party management;
- Monitoring of service performance;
- Customer feedback and satisfaction; and
- Continual improvement of services.

Service performance shall be monitored against defined requirements, objectives and applicable service-level commitments.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

6. INFORMATION & DATA PROTECTION

Somindra shall ensure that information is appropriately classified, handled, stored, transferred, retained and disposed of according to its sensitivity and business requirements.

Personal information and other confidential information shall be protected against unauthorized access, use or disclosure.

Employees and relevant third parties shall maintain confidentiality of information obtained during their association with Somindra.

7. PEOPLE, AWARENESS & RESPONSIBILITY

All personnel shall understand their information-security and IT service responsibilities and shall comply with applicable policies, procedures and instructions.

Somindra shall provide appropriate induction, awareness and training relating to information security, cybersecurity, IT service management, acceptable use, incident reporting, remote working and other relevant requirements.

Roles and responsibilities shall be defined and communicated to ensure accountability for the operation and improvement of the ISMS and ITSM system.

8. INCIDENTS, DISASTERS & BUSINESS CONTINUITY

Somindra shall establish arrangements for reporting, assessing, responding to and learning from information-security incidents and IT service incidents.

The organization shall maintain appropriate backup, disaster recovery and business continuity arrangements based on business and service risks.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

Information and critical IT-enabled services shall be protected, restored and recovered within defined and practical requirements following disruption.

9. LEGAL, REGULATORY & CONTRACTUAL COMPLIANCE

Somindra shall identify and comply with applicable:

- Legal and statutory requirements;
- Regulatory requirements;
- Customer requirements;
- Contractual obligations;
- Confidentiality obligations;
- Intellectual property requirements; and
- Privacy and data-protection requirements.

Compliance shall be periodically reviewed and appropriate actions shall be taken for identified gaps.

10. SUPPLIERS & THIRD PARTIES

Information-security and IT service requirements shall be considered while selecting, engaging and monitoring suppliers, cloud-service providers, OEMs, contractors and other relevant third parties.

Where applicable, confidentiality, security, service quality, availability, incident reporting and contractual requirements shall be incorporated into supplier arrangements.

11. OBJECTIVES, PERFORMANCE & CONTINUAL IMPROVEMENT



SOMINDRA MARKETING

Integrated Information Security & IT Service Management Policy

FORMAT. No :SM/ISIT/POL/01

V.2.0, R.0.0

EFF DATE :21.08.2026

Somindra shall establish measurable information-security and IT service objectives appropriate to its business, risks and customer requirements.

Performance shall be monitored through appropriate indicators, audits, reviews, incidents, customer feedback, service performance and management review.

Nonconformities and identified improvement opportunities shall be addressed through appropriate corrective actions.

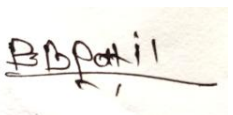
Somindra is committed to continually improving the suitability, adequacy and effectiveness of its ISMS and ITSM system.

12. POLICY REVIEW & APPROVAL

This policy shall be reviewed periodically and whenever significant changes occur in the organization's business, technology, services, risks, legal requirements or interested-party requirements.

The policy shall be communicated to relevant personnel and made available to applicable interested parties as appropriate.

All personnel working for or on behalf of Somindra are expected to comply with this policy and its applicable annexures.

Prepared By: Bhimagowda Patil	Reviewed By: Bhimagowda Patil & Mohan S. Desai	Approved By: Mohan S. Desai
Designation: CISO	Designation: CISO & MD	Designation: MD
Date: 01.08.2026	Date: 01.08.2026	Date: 01.08.2026
Signature:  _____	Signature:  _____	Signature:  _____

Prepared by: Bhimanagowda Patil(CISO)

Approved By: Mohan S Desai (MD)

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 01

INFORMATION SECURITY & CYBERSECURITY RULES

Reference: FTS/ISIT/POL/01 – Annexure 01

Somindra shall protect information and information-processing assets against unauthorized access, disclosure, alteration, loss, misuse and destruction.

Key Rules

1. Information shall only be accessed by authorized personnel having a legitimate business requirement.
2. Confidential/customer information shall not be disclosed to unauthorized persons.
3. Company information shall be stored only on approved systems, applications and storage locations.
4. Employees shall not knowingly introduce malware, unauthorized software or other malicious content into company systems.
5. Suspicious emails, phishing attempts, malware, unauthorized access, lost devices or suspected information leakage shall be reported immediately.
6. Security updates and controls implemented by Somindra shall not be deliberately disabled or bypassed.
7. Passwords and authentication information shall remain confidential.
8. Customer information and technical information shall be handled only for authorized business purposes.
9. Information-security requirements shall be considered during procurement, installation, configuration and commissioning of technology solutions.
10. Personnel shall cooperate with security investigations, audits and corrective actions.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 02

ACCEPTABLE USE OF IT & INFORMATION ASSETS

Reference: FTS/ISIT/POL/01 – Annexure 02

Company IT assets and information resources shall be used responsibly, securely and primarily for authorized business purposes.

Key Rules

- Company computers, laptops, email, Google Drive, Tally and other IT resources shall be used only for legitimate purposes.
 - Unauthorized access to systems, accounts, files or networks is prohibited.
 - Users shall not share passwords or authentication credentials.
 - Unauthorized software, applications, extensions or storage devices shall not be installed or connected.
 - Company devices shall not be used for activities that may create security, legal or reputational risks.
 - Employees shall exercise caution while opening email attachments, links or downloading files.
 - Confidential information shall not be copied to unauthorized personal storage or shared through unauthorized channels.
 - Users shall lock their computers/screens when unattended.
 - Internet resources shall be used responsibly and in accordance with organizational requirements.
 - Any suspected misuse, loss or compromise of an IT asset shall be reported immediately.
-

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 03

ACCESS CONTROL & AUTHENTICATION RULES

Reference: FTS/ISIT/POL/01 – Annexure 03

Access to information and systems shall be granted according to business need, role and authorization.

Key Rules

1. Each user shall use an individually assigned account wherever technically feasible.
2. Passwords shall be strong, confidential and shall not be shared.
3. Multi-factor authentication shall be enabled where supported and appropriate.
4. Access shall be granted only after appropriate authorization.
5. Privileged/administrative access shall be restricted to authorized personnel.
6. Access rights shall be reviewed periodically and whenever an employee changes role.
7. Access shall be promptly modified or withdrawn when employment or responsibilities change.
8. Users shall not attempt to bypass access restrictions.
9. Default passwords shall be changed where technically applicable.
10. Authentication information shall not be stored or communicated insecurely.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 04

INFORMATION CLASSIFICATION, PRIVACY & DATA PROTECTION RULES

Reference: FTS/ISIT/POL/01 – Annexure 04

Somindra shall protect information according to its sensitivity, business value, contractual obligations and privacy requirements.

Information Categories

Public: Information approved for public disclosure.

Internal: Routine business information intended for authorized organizational use.

Confidential: Customer, supplier, commercial, technical, financial, contractual or other sensitive information.

Restricted: Highly sensitive information requiring enhanced access restrictions.

Key Rules

- Information shall be accessed only for authorized purposes.
- Personal information shall be collected, used, stored and shared only for legitimate business purposes.
- Confidential information shall not be disclosed without authorization.
- Information shall be transferred through approved and reasonably secure channels.
- Information shall be retained only for the required period.
- Unnecessary copies shall be avoided.
- Information shall be securely disposed of when no longer required.
- Employees shall maintain confidentiality during and after employment.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 05

REMOTE WORKING & BYOD RULES

Reference: FTS/ISIT/POL/01 – Annexure 05

Somindra permits remote working where authorized and shall apply appropriate safeguards to protect organizational and customer information.

Remote Working Rules

- Employees shall work from reasonably secure locations.
- Company laptops/devices shall be protected against unauthorized access, theft and misuse.
- Screens shall be locked when unattended.
- Confidential information shall not be exposed to unauthorized persons in remote locations.
- Employees shall use approved accounts and applications for business work.
- Public or unsecured networks shall be avoided where reasonably possible.
- Lost or stolen devices shall be reported immediately.

BYOD Rules

Personal devices shall not be used for storing or processing confidential/customer information unless specifically authorized.

Where BYOD is permitted:

- The device shall have appropriate security protection.
- Access shall be limited to authorized business resources.
- Company information shall not be unnecessarily downloaded or retained.
- The organization may restrict or withdraw access where a security risk is identified.
- Business information shall be removed from personal devices when no longer authorized.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 06

PHYSICAL & ENVIRONMENTAL SECURITY RULES

Reference: FTS/ISIT/POL/01 – Annexure 06

Somindra shall protect its office, equipment, information and other physical assets against unauthorized access, theft, damage and environmental threats.

Key Rules

- Access to office premises shall be appropriately controlled.
 - Visitors shall be appropriately managed.
 - Visitors shall not be provided unrestricted access to sensitive areas or information.
 - Computers and other equipment shall be positioned to reduce unauthorized viewing or physical damage.
 - Employees shall follow clear-desk and clear-screen practices.
 - Company laptops and equipment taken outside the office shall be protected against loss and theft.
 - CCTV/security equipment shall be appropriately protected.
 - Fire, electrical, water, environmental and other physical risks shall be considered.
 - Equipment shall be maintained appropriately.
 - Storage media and equipment shall be securely disposed of or reused after appropriate data removal.
-

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 07

IT SERVICE MANAGEMENT & SERVICE QUALITY RULES

Reference: FTS/ISIT/POL/01 – Annexure 07

Somindra shall manage IT-enabled services in a structured and customer-focused manner throughout the service lifecycle.

Service Lifecycle

Customer Requirement → Planning → Procurement → Supply → Installation → Configuration → Commissioning → Handover → Technical Support → Service Closure / Improvement

Key Rules

- Customer and service requirements shall be clearly understood and recorded.
- Responsibilities for service delivery shall be defined.
- Installation and commissioning shall be performed in accordance with approved requirements.
- Service requests and incidents shall be recorded and tracked.
- Customer communication shall be timely and appropriate.
- Changes affecting services shall be appropriately assessed and authorized.
- Service performance shall be monitored against defined requirements.
- Customer feedback and complaints shall be recorded and addressed.
- Service records shall be maintained as evidence of delivery.
- Opportunities for improving service quality shall be identified and acted upon.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 08

IT CHANGE, CONFIGURATION & RELEASE RULES

Reference: FTS/ISIT/POL/01 – Annexure 08

Changes to IT systems, configurations, installations and customer solutions shall be controlled to minimize security and service risks.

Key Rules

1. Changes shall be identified and appropriately documented.
 2. Changes shall be reviewed for potential information-security and service impacts.
 3. Appropriate authorization shall be obtained before implementation.
 4. Critical configurations shall be recorded where necessary.
 5. Changes shall be tested or verified where practical.
 6. Customer-impacting changes shall be communicated appropriately.
 7. Emergency changes shall be controlled and reviewed after implementation.
 8. Failed changes shall be corrected or rolled back where practical.
 9. Configuration records shall be updated following relevant changes.
 10. Unauthorized changes shall be investigated.
-

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 09

INFORMATION SECURITY & CYBER INCIDENT RULES

Reference: FTS/ISIT/POL/01 – Annexure 09

All personnel shall promptly report actual or suspected information-security and cybersecurity incidents.

Examples

- Phishing, suspicious emails, malware, ransomware or other malicious activities;
- Unauthorized access, password/credential compromise or unauthorized system changes;
- Loss or theft of laptops, devices, equipment or information;
- Accidental or unauthorized disclosure, leakage or loss of confidential/personal information;
- Cybersecurity attacks, significant IT service disruptions or any other event that may compromise information security or service availability.

Incident Rules

- Report incidents immediately through the defined reporting channel.
- Do not delete or alter relevant evidence unnecessarily.
- Incidents shall be assessed and classified according to severity.
- Appropriate containment and corrective action shall be initiated.
- Relevant customers, suppliers or authorities shall be informed where required.
- Incident records shall be maintained.
- Lessons learned shall be considered for preventing recurrence.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 10

BACKUP, DISASTER RECOVERY & BUSINESS CONTINUITY RULES

Reference: FTS/ISIT/POL/01 – Annexure 10

Somindra shall maintain practical arrangements to protect critical information and continue or restore important business and IT-enabled services following disruption.

Key Rules

- Important business information shall be backed up using approved arrangements.
 - Backup arrangements shall consider confidentiality, integrity and availability.
 - Backup restoration shall be tested periodically where practical.
 - Critical IT dependencies shall be identified.
 - Business continuity and disaster recovery arrangements shall address reasonably foreseeable disruptions.
 - Employees shall understand their responsibilities during significant disruption.
 - Recovery priorities shall be based on business and service requirements.
 - Lessons from disruptions and recovery exercises shall be used for improvement.
-

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 11

SUPPLIER, CLOUD & THIRD-PARTY SECURITY RULES

Reference: FTS/ISIT/POL/01 – Annexure 11

Somindra shall consider information-security and IT service requirements when selecting and managing suppliers, OEMs, contractors, cloud-service providers and other third parties.

Key Rules

- Relevant suppliers shall be evaluated according to business and security risk.
 - Security and confidentiality requirements shall be included in agreements where appropriate.
 - Supplier access to Somindra/customer information shall be limited to authorized requirements.
 - Cloud services shall be used in accordance with approved business requirements.
 - Supplier performance and relevant security issues shall be monitored.
 - Supplier incidents affecting Somindra services or information shall be addressed.
 - Supplier changes that may affect services or security shall be reviewed.
 - Third-party access shall be withdrawn when no longer required.
-

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 12

SECURITY AWARENESS, TRAINING & CONTINUAL IMPROVEMENT RULES

Reference: FTS/ISIT/POL/01 – Annexure 12

Somindra shall ensure that personnel possess appropriate awareness and competence to perform their responsibilities securely and effectively.

Key Rules

- New personnel shall receive appropriate information-security and IT service awareness.
- Periodic training shall cover relevant cybersecurity and service-management topics.
- Training attendance shall be recorded.
- Training effectiveness shall be evaluated where appropriate.
- Personnel shall be informed about significant policy or procedure changes.
- Security incidents, audit findings, service failures and customer feedback shall be considered for improvement.
- Nonconformities shall be addressed through corrective action.
- Relevant KPIs and objectives shall be monitored.
- Management shall periodically review ISMS and ITSM performance.
- The organization shall continually improve the effectiveness of its management systems.

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ANNEXURE 13

SECURE WORKING, DATA LEAKAGE PREVENTION, CRYPTOGRAPHY & APPLICATION SECURITY RULES

Reference: SM/ISIT/POL/01 – Annexure 13

Somindra shall establish practical security requirements for work performed in secure areas, prevention of unauthorized information leakage, appropriate use of cryptography and security requirements for applications and technology solutions. These rules supplement the existing Physical & Environmental Security Rules, Remote Working & BYOD Rules, Information Classification, Privacy & Data Protection Rules, Access Control & Authentication Rules, IT Change, Configuration & Release Rules, Backup, Disaster Recovery & Business Continuity Rules, and Supplier, Cloud & Third-Party Security Rules.

A. SECURE WORKING IN CONTROLLED / SECURE AREAS

- Access to sensitive or critical areas shall be limited to authorized personnel based on business need.
- Visitors, vendors and third parties shall not enter controlled or restricted areas without authorization and appropriate supervision.
- Sensitive documents, screens, removable media and equipment shall not be left exposed or unattended.
- Photography, video/audio recording or use of personal recording/storage devices in restricted areas shall not be permitted unless specifically authorized.
- Portable computers, storage media and other devices used in controlled areas shall be subject to applicable security controls.
- Doors and access points to controlled areas shall not be bypassed or intentionally left unsecured.
- Unauthorized entry, loss, tampering or other physical-security concerns shall be reported promptly.

B. DATA LEAKAGE PREVENTION

- Information shall be accessed, copied, downloaded, transferred or shared only for authorized business purposes and in accordance with its classification.



Since 1994

SOMINDRA MARKETING

Integrated Information Security & IT Service Management Policy

FORMAT. No :SM/ISIT/POL/01

V.2.0, R.0.0

EFF DATE :21.08.2026

- Confidential or restricted information shall not be disclosed or transferred through unauthorized channels.
- Customer, supplier, commercial, technical, financial and contractual information shall be shared externally only with appropriate authorization and safeguards.
- Personal email, personal cloud storage, unauthorized file-sharing services and removable media shall not be used for Somindra or customer information unless specifically authorized.
- Unnecessary local copies, downloads and duplicate storage of sensitive information shall be avoided.
- Information shall be securely deleted or disposed of when no longer required, subject to applicable retention requirements.
- Suspected information leakage, accidental disclosure, loss or unauthorized transfer shall be reported immediately.
- Where technically feasible, available email, cloud, endpoint and access-control security features shall be used to reduce the risk of unauthorized disclosure.

C. USE OF CRYPTOGRAPHY

- Cryptographic protection shall be used where required by information sensitivity, risk, contractual requirements, applicable law or service requirements.
- Confidential or sensitive information shall be protected using appropriate encryption or other cryptographic safeguards when stored or transmitted, where applicable.
- Passwords, encryption keys, recovery codes, authentication secrets and other cryptographic credentials shall be protected from unauthorized access.
- Cryptographic keys and credentials shall not be shared insecurely or stored in openly accessible locations.
- Security and encryption requirements shall be considered when using cloud, SaaS, OEM and other third-party services.
- Access to credentials and cryptographic keys used to protect Somindra or customer information shall be restricted to authorized personnel.

D. APPLICATION & SOFTWARE SECURITY REQUIREMENTS

 SOMINDRA MARKETING	Integrated Information Security & IT Service Management Policy	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Information-security requirements shall be considered before acquiring, supplying, configuring, installing or materially changing applications and technology solutions.
- Only approved, licensed and authorized software and applications shall be used on organizational devices and systems.
- Third-party and OEM applications shall be assessed, as appropriate, for security, access, support, licensing, update, compatibility and contractual requirements.
- Application access shall be restricted according to business need and assigned responsibilities.
- Security updates, patches and configuration changes shall be implemented or coordinated based on risk, OEM guidance and service requirements.
- Applications and configurations shall be tested or verified before deployment where practical, particularly where customer information, security or service availability may be affected.
- For software and solutions supplied, installed, configured or commissioned by Somindra, applicable security requirements shall be considered during procurement, installation, configuration, testing and handover.
- Security weaknesses, unauthorized software, unsupported applications or significant application-security concerns shall be addressed through the applicable risk, incident, supplier or change-management process.

E. RESPONSIBILITY & AWARENESS

- Personnel shall comply with these rules and protect Somindra and customer information, systems, devices and other assets.
- The CISO and Management shall ensure awareness of these requirements through the existing ISMS/ITSM training and awareness programme.
- Violations or repeated non-compliance shall be addressed through the applicable incident, disciplinary, corrective-action or contractual process.



Since 1994

SOMINDRA MARKETING

Integrated Information Security & IT Service Management Policy

FORMAT. No :SM/ISIT/POL/01

V.2.0, R.0.0

EFF DATE :21.08.2026

DOCUMENT CHANGE NOTE

Version No.	Rev. No.	Effective Date	Summary of changes
01	00	01.08.2026	First Release
02	00	21.08.2026	New Annexure 13 introduced following Stage 1 AOCs to define secure working, data leakage prevention, cryptography and application/software security requirements.

Prepared by: Bhimanagowda Patil(CISO)

Approved By: Mohan S Desai (MD)