A practical, fill-in-the-blanks **Information Security Policy** for an Indian SME (10–500 people). Replace every **[bracketed placeholder]**, delete the italic guidance notes, have management approve it, and circulate it. One policy that staff actually read beats a 14-document suite nobody opens. Each section maps to CERT-In's 15 MSME controls, ISO/IEC 27001:2022 Annex A, and DPDP-readiness — the mapping annex is at the end, so the same document serves your audit trail.

Before you start — three rules for using this template

1. Adapt, don't adopt. A policy signed unread is an audit finding waiting to happen — strike every clause that doesn't match how you actually work, and add what's missing.
2. Name real owners. Every bracket that asks for a role needs a person who knows they own it.
3. Review on a schedule. Annually at minimum, and after any major incident, system change, or regulatory update.

Document control

Field	Value
Organisation	**[Company legal name]**
Policy owner	**[Role — e.g., InfoSec Owner / IT Head / vCISO]**
Approved by	**[MD / CEO / Partners]** on **[date]**
Version	**[1.0]** Effective: **[date]** Next review: **[date + 12 months]**
Applies to	All employees, contractors, interns and third parties accessing **[Company]** systems or data

1. Purpose & scope

This policy protects the confidentiality, integrity and availability of **[Company]**'s information — customer data, employee data, business records and systems — against misuse, loss and attack, and supports our obligations under Indian law, including the IT Act 2000, CERT-In directions, and the DPDP Act 2023. It covers all information assets owned or operated by **[Company]**, wherever they run — on-premises, cloud, or personal devices used for work.

2. Roles & responsibilities

2.1 Management ([MD/CEO/Partners]**)** — approves this policy, funds its implementation, reviews security posture **[quarterly/half-yearly]**, and owns risk acceptance decisions. ☐

2.2 InfoSec Owner ([name the role — IT Head, vCISO, or designated manager]**)** — maintains this policy, runs the controls, leads incident response, reports to management, and is the single point of contact for security questions. ☐

2.3 All staff — follow this policy, complete security training, and report suspected incidents immediately to **[incident contact]**. Security is a condition of employment, not an IT department service. ☐

2.4 Vendors & third parties — bound to equivalent security obligations through contracts before receiving access or data (see §9). ☐

3. Asset management

3.1 We maintain a central inventory of hardware, software and information assets, owned by **[role]**, updated on every purchase, move, or disposal. ☐

3.2 Information is classified as Public / Internal / Confidential — and handled per its class. **[Adjust classes to your reality; three is plenty for most SMEs]**. ☐

3.3 Equipment is disposed of securely: storage wiped or destroyed, asset register updated, certificate kept for **[retention period]**. ☐

4. Access control, identity & passwords

4.1 Access follows least privilege and is role-based; privileged (admin) access is restricted to **[named roles]** and logged. ☐

4.2 Multi-factor authentication is mandatory on email, cloud consoles, finance systems, VPN and any internet-facing administration. ☐

4.3 Passwords: minimum **[12]** characters, unique per system, no sharing, managed via **[password manager]**. Default passwords are changed before any system goes live. ☐

4.4 Joiner-mover-leaver: access is provisioned on role start, adjusted on role change, and **revoked within [24 hours] of exit** — with the §12 asset-return checklist. ☐

4.5 Access rights are reviewed **[quarterly]** by **[role]**; the review is documented. ☐

5. Acceptable use

5.1 Company systems are for business use; limited personal use is acceptable where it creates no security, legal, or productivity risk. ☐

5.2 Prohibited: pirated or unauthorised software, disabling security tools, sharing credentials, forwarding business data to personal accounts, and connecting unapproved devices to internal networks. ☐

5.3 Email & messaging: treat unexpected attachments, payment-change requests and urgent "act now" messages as suspect — verify out-of-band before acting; report phishing to **[incident contact]**. ☐

6. Endpoints, mobile & remote work

6.1 All company devices run licensed, current OS and endpoint protection; OS security features stay enabled; disk encryption is on by default. ☐

6.2 Software installation is restricted to authorised personnel; USB/removable media use is **[restricted/controlled — state your rule]**; autorun is disabled. ☐

6.3 Remote work: company data is accessed via **[VPN / zero-trust gateway]** with MFA; public Wi-Fi requires the VPN; screens lock at **[5]** minutes. ☐

6.4 Personal devices (BYOD) **[are/are not]** permitted for work; where permitted, they meet the same protection baseline and accept remote-wipe of company data. ☐

7. Network & secure configuration

7.1 Perimeter and host firewalls are enabled and configured; guest Wi-Fi is segregated; Wi-Fi uses WPA2/WPA3 with strong credentials. ☐

7.2 Systems are deployed against approved baseline configurations; unnecessary ports, services and default applications are disabled. ☐

7.3 Changes to production systems follow a documented change process with approval by **[role]** and rollback steps. ☐

8. Patch & vulnerability management

8.1 Security patches are applied on a schedule: critical within **[7]** days, high within **[30]** days, others within **[90]** days. **[Role]** monitors vendor and CERT-In advisories. ☐

8.2 An independent vulnerability assessment of business-critical assets runs at least annually, with findings remediated on a tracked plan. ☐

9. Vendors, cloud & third parties

9.1 A vendor register lists every third party with access to systems or data, its owner, and the data it touches. ☐

9.2 Security obligations — confidentiality, breach notification within **[24/48]** hours, data-handling limits, audit rights, exit/return-of-data terms — are contractual before access is granted. ☐

9.3 Where vendors process personal data on our behalf, a Data Processing Agreement aligned to the DPDP Act is in place (see §11). ☐

9.4 Cloud services are approved by **[role]** before use; shadow IT — signing up to tools without approval — is prohibited. ☐

10. Backup & recovery

10.1 Backups run on a schedule (**[daily incremental / weekly full — state yours]**), encrypted, with at least one copy stored separately from production. ☐

10.2 Restoration is **tested every [quarter]** and the result documented — an untested backup is a hope, not a control. ☐

10.3 Recovery objectives: critical systems restored within **[RTO — e.g., 8 hours]** with maximum data loss of **[RPO — e.g., 24 hours]**. ☐

11. Data protection & privacy (DPDP-readiness)

11.1 We maintain an inventory of personal data: what we hold, whose, why, where, retention, and which vendors touch it. ☐

11.2 Personal data is collected with notice and valid consent (or a documented legitimate use), used only for stated purposes, and erased when no longer needed unless law requires retention. ☐

11.3 **[Role/email]** is the published contact for data-principal requests (access, correction, erasure, withdrawal); requests are logged and answered within our published timeline of **[X — must not exceed 90]** days. ☐

11.4 Personal data breaches trigger §12 immediately — DPDP requires intimating affected individuals and the Data Protection Board without delay, with a detailed report within 72 hours. ☐

12. Incident management & reporting

12.1 Suspected incidents are reported immediately to **[incident contact / phone / email]** — staff are never penalised for good-faith reporting. ☐

12.2 **[Role]** classifies the incident, leads containment, and decides external notifications using the incident response plan at **[location of IRP]**. ☐

12.3 CERT-In reporting: listed cyber incidents are reported within **6 hours** of noticing (incident@cert-in.org.in / 1800-11-4949), per the April 2022 Directions. ☐

12.4 System clocks sync to NIC/NPL NTP servers; **ICT logs are retained 180 days** (CERT-In) and breach-relevant logs **at least one year** (DPDP Rules) within Indian jurisdiction. ☐

12.5 Every significant incident gets a root-cause review and at least one preventive change; lessons update this policy and the IRP. ☐

13. Physical security

13.1 Server/network equipment sits in access-controlled space (**[locked room / badge / biometric — state yours]**); visitor access is logged and escorted. ☐

13.2 Every employee exit completes an asset-return checklist: ID, laptop, storage media, keys/badges — alongside §4.4 access revocation. ☐

13.3 Clear desk & screen: confidential material locked away; screens locked when unattended; printing of confidential data minimised and collected immediately. ☐

14. Training, exceptions, enforcement & review

14.1 Security awareness training at onboarding and at least annually; phishing simulations **[frequency — optional but recommended]**; completion is tracked. ☐

14.2 Exceptions to this policy require written approval by **[Management role]** with a stated reason, compensating control, and expiry date — kept in an exceptions register. ☐

14.3 Violations may lead to disciplinary action up to termination and, where applicable, legal action. Suspected criminal activity is reported to authorities. ☐

14.4 This policy is reviewed **[annually]** by the InfoSec Owner, re-approved by management, and version-logged in the document control table. ☐

Annex — control mapping (audit crosswalk)

Policy §	CERT-In 15 controls (MSME v1.0)	ISO/IEC 27001:2022 Annex A
§3 Assets	1. EAM	A.5 asset mgmt; A.5.9–5.13
§4 Access & passwords	12. RPP · 13. ACIM	A.5.15–5.18; A.8.2–8.5
§5 Acceptable use	2. NES (email) · 8. AT	A.5.10; A.6.3
§6 Endpoints & remote	3. EMS	A.6.7; A.8.1
§7 Network & config	2. NES · 4. SC	A.8.9; A.8.20–8.22
§8 Patching & vulns	5. PM · 15. VAA	A.8.8
§9 Vendors & cloud	9. TPRM	A.5.19–5.23
§10 Backup	10. DPBP	A.8.13–8.14
§11 Data protection	10. DPBP · 11. GC	A.5.33–5.34 · DPDP Act s.8
§12 Incidents & logs	6. IM · 7. LM	A.5.24–5.28; A.8.15–8.16
§13 Physical	14. PS	A.7.1–7.14
§14 Training & review	8. AT · 11. GC	A.6.3; A.5.1; A.5.35–5.36

Approval

Approved and adopted on behalf of **[Company legal name]**:

Name: **[approver name or designation — anonymous-brand note: use designations on public copies]** Designation: **[MD / CEO / Partner]** Date: **[date]** Signature: _____

Template current as of 5 June 2026. Pair it with the CERT-In 15-controls checklist and the DPDP compliance guide from the same resource library — vcisodesk.com/grc-radar/ — free, like everything on GRC RADAR.