[COMPANY NAME]
[Add your company logo / letterhead and registered address here]

Vendor and Third-Party Risk Management Policy

HOW TO USE THIS TEMPLATE
This template is mostly complete and pre-filled with standard Indian practice. You should not have to fill many blanks.
Text in blue is a default that companies commonly change. Skim the blue text and edit only what differs for you.
Add your company name and letterhead once, in the header above. The body refers to "the Company".
Tier every new vendor at intake, run due diligence proportionate to the tier, and sign a Data Processing Agreement before any personal data is shared. Reassess all vendors at least [[annually]].
Have it reviewed by a qualified HR or legal professional before you adopt it, and delete this box.
Provided by CFOmatrix (cfomatrix.in). General template, not legal advice.

Policy owner	**[Human Resources / IT / Compliance]**
Effective date	**[DD MMM YYYY]**
Version	1.0
Approved by	**[Name, Title]**

1. Purpose

The Company relies on external vendors, suppliers, contractors, consultants, agencies, cloud platforms, payment partners and other third parties (collectively, "Vendors") to deliver its products and services. Each Vendor relationship introduces risk: operational, financial, legal, regulatory, reputational, information security and data privacy risk. This Policy establishes a consistent, risk-based framework to identify, assess, contract, monitor and offboard Vendors so that the Company can use third parties confidently while protecting its data, its customers, its systems and its compliance obligations.

This Policy supports the Company's commitments under the Digital Personal Data Protection Act, 2023 (DPDP Act), the CERT-In Directions, 2022, and the Company's information security control framework (mapped to SOC 2 and ISO/IEC 27001). Where the Company processes personal data through Vendors, the Company remains accountable as the Data Fiduciary and Vendors typically act as Data Processors on the Company's behalf.

2. Scope

This Policy applies to:

- All Vendors and prospective Vendors engaged by the Company, regardless of contract value, engagement length or business unit.

- All employees, officers, directors, contractors and authorised representatives of the Company who initiate, approve, manage, pay or end a Vendor relationship ("Vendor Owners" and "Approvers").
- All forms of engagement: master service agreements, statements of work, purchase orders, subscriptions (including self-service SaaS and free tools), professional services, staffing, outsourcing, and any arrangement under which a Vendor accesses, processes, stores or transmits Company data, systems, networks or facilities.
- Sub-processors and fourth parties engaged by a Vendor to the extent they touch Company or customer data.

Exclusions: routine, low-value, non-data, non-system purchases below Rs **25,000** (for example, office supplies or local catering) may follow a simplified intake at the discretion of the Vendor Owner, provided no personal data, confidential information or system access is involved.

3. Definitions

- Vendor / Third Party: any external organisation or individual providing goods or services to the Company.
- Vendor Owner: the Company employee accountable for the day-to-day relationship, performance and risk of a specific Vendor.
- Data Fiduciary / Data Processor: as defined under the DPDP Act, 2023. The Company is generally the Data Fiduciary; a Vendor that processes personal data on the Company's instructions is a Data Processor.
- Sub-processor: a third party engaged by a Vendor to assist in processing Company or customer data.
- DPA: Data Processing Agreement or Addendum governing the processing of personal data by a Vendor.
- Critical Vendor: a Vendor whose failure, breach or non-performance would materially disrupt operations, breach a legal obligation, or expose sensitive data.
- Inherent Risk: risk before controls. Residual Risk: risk after the Vendor's and the Company's controls are applied.

4. Roles and Responsibilities

Role	Responsibility
Vendor Owner	Initiates intake, justifies the business need, manages performance and SLAs, drives reassessment and offboarding.
Procurement / Finance	Runs commercial due diligence, verifies legal/tax registrations, manages POs, payments and the Vendor master.
Information Security	Owns the security assessment, sets risk tiering criteria, reviews certifications, signs off on Critical Vendors.

Data Protection Officer (DPO) / Privacy	Reviews privacy impact, approves DPAs, validates cross-border transfer and data-deletion terms.
Legal	Reviews and negotiates contracts, DPAs, liability, indemnity and termination clauses.
Vendor Risk Committee	Governs the programme, approves the highest-tier and exception cases, reviews the Vendor risk register.
Approving Authority	Authorises onboarding per the financial and risk approval matrix.

The Company's Vendor Risk programme is owned by **the Chief Information Security Officer / Head of Procurement**. Privacy matters escalate to **dpo@company.com**.

5. Vendor Risk Tiering

Every Vendor must be assigned a risk tier at intake. Tiering drives the depth of due diligence, the contract terms required, and the frequency of reassessment. Tier is based on data sensitivity, system access, business criticality, spend, and regulatory exposure.

Tier	Typical profile	Examples	Due diligence	Reassessment
Tier 1 (Critical)	Processes sensitive/large-volume personal data, deep system access, or business-critical	Cloud/hosting, payroll, payment processor, core SaaS	Full assessment, security questionnaire, evidence review, DPA, on-site/virtual review	**Annually**
Tier 2 (Moderate)	Limited personal data or moderate system/network access	CRM add-ons, analytics, marketing tools, recruiting platforms	Standard questionnaire, certification review, DPA	Every **18 months**
Tier 3 (Low)	No personal/confidential data, no system access	Office supplies, facilities, event vendors	Simplified intake, basic checks	Every **3 years** or on change

A Vendor is automatically treated as Tier 1 if it processes special-category or large volumes of personal data, holds privileged/admin access, or supports a regulated process (financial reporting, KYC, payroll, customer payments).

6. Onboarding and Due Diligence

No Vendor may be engaged, and no data or system access may be granted, until intake and tier-appropriate due diligence are complete and the engagement is approved.

Intake (all Vendors): the Vendor Owner submits a request capturing business need, data and systems involved, expected spend, and proposed tier via **the Vendor Intake form / procurement tool**.

Commercial and legal due diligence (Tier 1 and 2):

- Legal entity verification: registered name, CIN/LLPIN, GSTIN, PAN, registered address.
- Financial stability check proportionate to spend and criticality (financials, credit signals, going-concern indicators).
- Confirmation the Vendor is not on any applicable sanctions or debarment list.
- Conflict-of-interest and beneficial-ownership check; confirmation of no undisclosed relationship with Company personnel.
- Anti-bribery and anti-corruption screening; the Vendor must confirm compliance with the Prevention of Corruption Act, 1988, and, for cross-border dealings, the FCPA and UK Bribery Act.
- References or proof of capability for material engagements.

Security and privacy due diligence is covered in Sections 7 and 8.

Approval: the completed assessment, risk tier and residual risk are routed to the Approving Authority. Any control gap must be documented with a remediation plan or a formal, time-bound risk acceptance signed by **the Vendor Risk Committee**.

7. Security Assessment

Information Security conducts a security assessment scaled to the Vendor's tier. Tier 1 and Tier 2 Vendors must complete the Company's security questionnaire (aligned to SOC 2 Trust Services Criteria and ISO/IEC 27001 Annex A controls) before onboarding.

The assessment evaluates, at minimum:

- Independent attestations: a current SOC 2 Type II report or ISO/IEC 27001 certificate, reviewed for scope and exceptions. Where unavailable, the Vendor must evidence equivalent controls.
- Access control: least privilege, role-based access, multi-factor authentication, and joiner/mover/leaver processes.
- Encryption of data in transit (TLS 1.2 or higher) and at rest.
- Network and endpoint security, vulnerability management, and patching cadence.
- Secure software development practices and change management (for software/SaaS Vendors).
- Logging, monitoring and incident detection capability.
- Business continuity and disaster recovery, including tested RTO/RPO commitments.
- Sub-processor inventory and the Vendor's own third-party risk practices.
- Personnel security: background checks and security/privacy training.

Findings are scored, gaps are tracked to closure, and Critical Vendor sign-off rests with **Information Security**. High-risk findings without acceptable remediation block onboarding.

8. Privacy and Data Protection Assessment

Where a Vendor will access, process, store or transmit personal data, a privacy assessment is mandatory and the DPO must approve before data sharing begins. The Company remains the Data Fiduciary and is accountable under the DPDP Act, 2023.

The assessment confirms:

- Lawful basis and consent: data is shared only for the specified, lawful purpose with a valid basis under the DPDP Act, and Vendor processing stays within that purpose (purpose limitation).
- Data minimisation: only the personal data necessary for the service is shared.
- Data principal rights: the Vendor can support access, correction, completion, updating, erasure and grievance redressal requests the Company must honour as Data Fiduciary.
- Retention limits: the Vendor retains personal data only as long as necessary and deletes or returns it on instruction or contract end.
- Breach notification: the Vendor must notify the Company without undue delay so the Company can meet its own obligations to notify the Data Protection Board of India and affected data principals. Note: the DPDP Rules are still being finalised and notification timelines may evolve; the contract should require notification within **24 hours** of the Vendor becoming aware.
- Cross-border transfer: any transfer of personal data outside India complies with the DPDP Act and any government restrictions; transfer locations are documented.
- Cyber incident reporting: Vendors handling Company systems or data must support the Company's compliance with the CERT-In Directions, 2022, which require reporting specified cyber incidents within 6 hours of detection.

A Data Protection Impact Assessment is conducted for Vendors processing significant volumes of, or sensitive, personal data.

9. Contracts and Data Processing Agreements

No Tier 1 or Tier 2 Vendor may be engaged without a signed written contract reviewed by Legal. Where personal data is processed, a Data Processing Agreement (DPA) must be executed before any data is shared.

Every Vendor contract should address, as applicable:

- Clear scope of work, deliverables, acceptance criteria and pricing.
- Confidentiality and protection of Company and customer information.
- Service levels and remedies (see Section 10).

- Security obligations consistent with the Company's control framework and the Vendor's attestations.
- Audit rights: the right to audit, or to receive independent attestation reports, at least **annually**.
- Liability, indemnity, and insurance appropriate to the risk (including cyber liability for Tier 1 Vendors).
- Compliance with applicable law, including anti-bribery, the DPDP Act and CERT-In Directions.
- Term, renewal, termination for cause and convenience, and exit assistance.

The DPA must, at minimum, specify:

- The subject matter, nature, purpose and duration of processing, and the categories of personal data and data principals.
- That the Vendor processes personal data only on the Company's documented instructions, as a Data Processor.
- Sub-processing only with the Company's prior written authorisation, with flow-down of equivalent obligations and the Company's right to object.
- Technical and organisational security measures.
- Assistance with data principal rights requests and with breach handling.
- Breach notification timelines (see Section 8).
- Return or deletion of all personal data at the end of the engagement, with written certification of deletion (see Section 12).
- Records of processing and audit/inspection support.

10. Service Levels (SLAs)

Tier 1 and material Tier 2 Vendors must operate against documented, measurable SLAs with reporting and remedies. Targets below are standard defaults to be tailored per engagement.

Metric	Target	Measurement	Remedy on breach
Service availability / uptime	**99.9%** monthly	Vendor + Company monitoring	Service credit per contract
Critical (P1) incident response	Within **30 minutes**	Ticket timestamps	Escalation + credit
Critical (P1) resolution	Within **4 hours**	Ticket timestamps	Escalation + credit
Standard support response	Within **1 business day**	Ticketing system	Tracked in review
Security patch (critical CVE)	Within **7 days** of release	Patch reports	Remediation plan
Breach / incident notification	Within **24 hours** of awareness	Notification log	Material breach
SLA / performance reporting	**Monthly**	Vendor report	Tracked in review

Persistent SLA failure is escalated to the Vendor Owner and, for Critical Vendors, to the Vendor Risk Committee, and may constitute grounds for termination.

11. Ongoing Monitoring and Reassessment

Vendor risk is managed continuously, not only at onboarding. The Vendor Owner is accountable for ongoing oversight, supported by Information Security and the DPO.

Ongoing activities:

- Performance and SLA reviews at the cadence set per tier (**quarterly** business reviews for Tier 1).
- Periodic reassessment: refresh due diligence and re-score risk per the tier schedule in Section 5 (at least **annually** for Tier 1).
- Annual collection of refreshed attestations (SOC 2 / ISO 27001 reports, DPA confirmations, insurance certificates).
- Continuous monitoring of adverse signals: financial distress, ownership changes, sanctions listing, public breach disclosures, regulatory action and material news.
- Sub-processor change review: any new or changed sub-processor for a Tier 1 Vendor is assessed before it takes effect.
- Maintenance of a central Vendor risk register recording tier, residual risk, attestations, contract dates, DPA status and next review date.

Trigger-based reassessment occurs regardless of schedule when there is a security incident, a material change in services or data scope, a change of control, a regulatory change, or a significant SLA failure.

12. Offboarding, Data Return and Deletion

When a Vendor relationship ends (expiry, termination or non-renewal), a controlled offboarding must be completed to remove access and recover or destroy Company data.

Offboarding checklist:

- Revoke all Vendor access to Company systems, networks, applications, accounts, badges and premises.
- Disable API keys, integrations, service accounts and federated logins.
- Recover all Company assets, devices, documentation and credentials.
- Require return or secure deletion of all Company and personal data held by the Vendor and its sub-processors, including backups, within **30 days** of termination.
- Obtain written certification of deletion from the Vendor, confirming the data, formats and locations destroyed.
- Confirm cessation of any further processing of personal data, consistent with the DPA and the DPDP Act.

- Settle final invoices, close the PO, and update the Vendor master to "offboarded".
- Conduct an exit/lessons-learned review for Tier 1 Vendors and document any transition or knowledge transfer.

The Vendor Owner is responsible for completing offboarding; Information Security verifies access revocation and the DPO verifies data deletion for Vendors that processed personal data.

13. Exceptions and Enforcement

Any deviation from this Policy (for example, engaging a Vendor before due diligence completes, accepting a known control gap, or onboarding without a DPA) requires a documented, time-bound exception approved by **the Vendor Risk Committee** with a remediation plan and an accountable owner.

Engaging Vendors outside this Policy ("shadow IT" or unapproved tools), bypassing required assessments, or sharing personal data without a DPA is a serious matter. Violations may result in disciplinary action up to and including termination of employment or contract, and may expose individuals and the Company to legal and regulatory liability. Vendors that breach their obligations are subject to remediation, suspension or termination.

14. Review and Governance

This Policy is owned by **the Vendor Risk Committee / CISO** and reviewed at least **annually**, or sooner upon a material change in law (including finalisation of the DPDP Rules), the Company's control framework, or the Vendor risk landscape. The Vendor risk register and programme metrics are reported to **senior management** on a **quarterly** basis. All employees engaging Vendors are responsible for compliance with this Policy.

Effective date: **01 April 2026**. Version: **1.0**.