ResolvX

Vendor Management Policy & TPRM Framework

Topic-Specific Policy — Third-Party Risk

POL-005 · v1.0 · 2026 · Internal — Confidential

Document Information

Policy ID	POL-005
Version	1.0
Status	Active
Classification	Internal — Confidential
Owner	GRC Lead — Derick G. Dmello
Approver	CISO
Review Cycle	Annual
Next Review	Q1 2027
Frameworks	ISO 27001:2022 A5.19–A5.23 · NIST 800-53B SR-1–SR-12 · NIST CSF GV.SC-01–10 · SOC 2 CC9.1, CC9.2

ResolvX — Vendor Management Policy & Third-Party Risk Management Framework

1. Purpose

This policy establishes ResolvX's framework for managing information security risks introduced by third-party vendors, suppliers, cloud service providers, and other external parties that access, process, store, or transmit ResolvX information assets or that provide critical services upon which ResolvX depends.

Third parties represent one of the most significant and least directly controllable risk surfaces in any organisation's security posture. This policy ensures that third-party relationships are established, maintained, and terminated with appropriate security controls and that ResolvX does not inadvertently extend trust to parties that have not earned it.

2. Scope

This policy applies to all third parties that:

- Access ResolvX systems, networks, or data (including cloud environments and SaaS platforms)
- Process, store, or transmit ResolvX or client data on ResolvX's behalf
- Provide technology infrastructure, software, or professional services upon which ResolvX's operations depend
- Have contractual, commercial, or operational relationships with ResolvX involving exchange of Confidential or Restricted information

This includes but is not limited to: SaaS vendors, cloud infrastructure providers (IaaS/PaaS), professional services firms, managed service providers, and subcontractors.

3. Vendor Risk Tiers

Not all vendors represent equal risk. ResolvX uses a tiered classification to direct assessment effort proportionally:

Tier	Risk Level	Criteria	Review Frequency
Tier 1 — Critical	Very High	Access to Restricted data (client PII, financial records); core infrastructure provider; single point of failure risk	Annual assessment + event-triggered review
Tier 2 — High	High	Access to Confidential data; significant business continuity dependency; material sub-processors	Annual assessment
Tier 3 — Medium	Medium	Access to Internal data only; limited dependency; replaceable within 30 days	Biennial assessment or on contract renewal

Tier 4 — Low	Low	No data access; no system integration; off-the-shelf commodity services	Lightweight onboarding check only

Tier assignment is made by the GRC Lead at onboarding and reviewed annually.

4. Vendor Lifecycle Management

4.1 Pre-Engagement Due Diligence

Before any contract is executed with a Tier 1, 2, or 3 vendor, the following must be completed:

Security Assessment (Tier 1 & 2):
- Complete ResolvX's Vendor Security Questionnaire (VSQ)
- Review vendor's most recent SOC 2 Type II report, ISO 27001 certificate, or equivalent third-party audit
- Assess vendor's incident history and breach disclosure record
- Evaluate vendor's sub-processor chain and any fourth-party risks
- Review vendor's business continuity and disaster recovery capabilities
- Assess vendor's regulatory and legal compliance posture

Lightweight Check (Tier 3):
- Abbreviated VSQ (governance, access control, data handling sections only)
- Confirm existence of basic security programme (policy, incident response, patching)

Legal Review (all Tier 1 & 2, and any vendor with data access):
- NDA executed before any information sharing
- DPA executed before any personal data processing
- Review and negotiate security-specific contract clauses (see Section 6)
- Legal review of contractual indemnification and liability provisions

The GRC Lead maintains the Vendor Register with current tier, assessment status, and contract dates.

4.2 Onboarding

Upon completion of due diligence and contract execution:

- GRC Lead records vendor in Vendor Register with tier, data types accessed, primary contact, and contract expiry
- IT Admin provisions vendor access per the Access Control Policy (POL-003): minimum necessary permissions, time-limited where possible, MFA required
- Head of Cloud Ops reviews any AWS-level integration or API access scope
- Legal confirms DPA is filed and sub-processor register is updated if applicable

4.3 Ongoing Monitoring

Vendor relationships do not end at onboarding. Active monitoring requirements by tier:

Tier 1 — Critical:

- Annual reassessment including refreshed VSQ and updated SOC 2 / audit report
- Review of vendor security advisories and incident notifications
- Quarterly review of vendor's access logs to ResolvX systems
- Annual contractual right-to-audit clause exercise (or review of independent audit report)
- Notification obligations: vendor must notify ResolvX within 72 hours of any security incident that may affect ResolvX data or services

Tier 2 — High:

- Annual reassessment
- Review updated SOC 2 / audit report on renewal or annually, whichever is sooner
- Incident notification requirement: 72 hours

Tier 3 — Medium:

- Reassessment at contract renewal or biannually
- Passive monitoring (review public breach reports, security advisories)

All Tiers:

- Immediate review triggered by: vendor data breach, change in vendor ownership, significant service disruption, material change in vendor's security posture or regulatory standing

4.4 Offboarding

When a vendor relationship ends by contract expiry, termination, or mutual agreement:

- IT Admin revokes all vendor access within 24 hours of relationship end date (coordinate with account manager to confirm access end date in advance)
- GRC Lead confirms all ResolvX data in vendor custody has been returned, deleted, or destroyed per contractual and legal requirements like obtaining written confirmation
- Vendor access is documented as terminated in the Vendor Register
- DPA is reviewed for any surviving obligations (e.g., audit rights, data retention)
- API keys and integration credentials are rotated if shared with the vendor

5. Vendor Security Questionnaire (VSQ)

The VSQ is the primary tool for assessing a vendor's security posture. It is completed by the vendor at onboarding and at each reassessment. The full VSQ covers:

Domain	Key Questions
Governance	Does the vendor have a formal information security programme? Is it assigned to a named owner? Do they conduct annual risk assessments?
Access Control	How is access to ResolvX data or systems controlled? Is MFA enforced? Are access rights reviewed periodically?
Data Protection	Is data encrypted at rest and in transit? Where is data stored (geography)? Who are their sub-processors? What are their retention and disposal practices?
Vulnerability Management	How frequently is patching performed? Are annual penetration tests conducted? Is there a vulnerability disclosure programme?
Incident Response	Does the vendor have a documented IR plan? What is the breach notification timeline? Have they experienced incidents in the past 24 months?
Business Continuity	What is the target RTO/RPO? When was DR last tested? What is the uptime SLA?
Compliance	What certifications does the vendor hold (SOC 2, ISO 27001, PCI DSS)? Are they subject to relevant regulations?
Sub-processors	Who are the vendor's key sub-processors? What security requirements flow down to them?
Personnel Security	Are background checks conducted for staff with access to client data? Is security awareness training mandatory?

Vendor responses are scored and documented in the Vendor Register. Material gaps require a documented risk treatment decision before contract execution.

6. Contractual Security Requirements

All contracts with Tier 1 and Tier 2 vendors, and any vendor that accesses personal data, must include the following minimum security provisions:

Clause	Requirement
Security obligations	Vendor must maintain an information security programme appropriate to the risk of the engagement
Incident notification	Vendor must notify ResolvX within 72 hours of any confirmed or suspected security incident affecting ResolvX data or services
Data handling	Vendor may process ResolvX data only for the purposes defined in the contract; no secondary use without explicit authorisation
Sub-processors	Vendor must disclose sub-processors processing ResolvX data and obtain ResolvX consent before adding material new sub-processors
Audit rights	ResolvX retains the right to audit vendor's security controls, or to require the vendor to provide an independent audit report (e.g., SOC 2 Type II) on request
Data return / deletion	Upon termination, vendor must return, delete, or destroy all ResolvX data within 30 days and provide written confirmation
Compliance obligations	Vendor must comply with applicable laws and regulations relevant to the data processed
Change notification	Vendor must notify ResolvX of material changes to its security posture, ownership, or relevant certifications

For vendors processing personal data on ResolvX's behalf, a **Data Processing Agreement (DPA)** compliant with GDPR Article 28 is mandatory before processing commences.

7. Cloud Service Providers

ResolvX's primary infrastructure is hosted on AWS. Cloud services present distinct risk considerations addressed by ISO A5.23 and NIST GV.SC. The following apply to all cloud service usage:

- New cloud services used to process Restricted or Confidential data must be approved by the GRC Lead and IT Admin before use
- Shadow IT (use of cloud services not approved by IT Admin) is prohibited
- All cloud services must be accessed via Okta SSO where technically supported
- Data residency must be assessed for all cloud services processing personal data; EU/EEA storage required for EU personal data unless adequacy decision or SCCs are in place
- Exit strategy must be documented for all Tier 1 cloud providers at onboarding ; what is the data recovery and migration path if the service is discontinued?
- AWS Shared Responsibility Model is acknowledged: ResolvX is responsible for securing its workloads, configurations, data, and access management; AWS is responsible for infrastructure security

8. Vendor Risk Register

The GRC Lead maintains a Vendor Risk Register as a sub-component of the main Risk Register. It records:

- Vendor name, tier, services provided, data types accessed
- Assessment date and outcome summary
- Residual risk rating
- Outstanding risk treatment actions
- Contract expiry and next review date
- DPA status and sub-processor register reference

The Vendor Risk Register is reviewed quarterly by the GRC Lead and presented to the CISO at each management review.

9. Current Critical Vendors (Tier 1)

Vendor	Service	Data Accessed	SOC 2 Status	DPA
Amazon Web Services (AWS)	Cloud infrastructure (IaaS)	All system data	SOC 2 Type II ✓	AWS Data Processing Addendum ✓
Okta	Identity Provider (SSO + MFA)	Employee identity data	SOC 2 Type II ✓	DPA ✓
GitHub (Microsoft)	Source code management	Source code, secrets risk	SOC 2 Type II ✓	DPA ✓
Google Workspace	Email, documents, collaboration	Internal + some client comms	SOC 2 Type II ✓	DPA ✓
Jamf	MDM — device management	Device inventory, compliance data	SOC 2 Type II ✓	DPA ✓
1Password	Credential management	Credential metadata	SOC 2 Type II ✓	DPA ✓

This table is maintained live in the Vendor Register and is reviewed and updated quarterly.

10. Roles and Responsibilities

Role	Responsibility
GRC Lead	Maintains Vendor Register and Vendor Risk Register; owns the TPRM framework; conducts or coordinates all vendor assessments; approves new vendor onboarding; manages DPA compliance
Legal	Reviews and negotiates contracts and DPAs; provides legal sign-off on cross-border data transfers; maintains sub-processor register
IT Admin	Provisions and revokes vendor access; manages API credentials and integration security; reviews vendor access logs
Head of Cloud Ops	Reviews cloud service configurations and data residency; assesses AWS-level integration risks; owns shared responsibility model alignment
Business Owners	Identify vendor need; participate in assessment; own the ongoing business relationship; escalate vendor security concerns to GRC Lead

11. Compliance and Enforcement

Engaging a vendor that has not completed the required due diligence or sharing ResolvX data with a vendor without an executed DPA (where required), is a policy violation. This includes the use of free-tier or consumer cloud services to process Restricted data. Violations are subject to disciplinary action.

12. Document Control

Field	Detail
Policy ID	POL-005
Version	1.0
Status	Active
Classification	Internal — Confidential
Owner	GRC Lead — Derick G. Dmello
Approver	CISO
Review Cycle	Annual
Next Review	Q1 2027
Framework References	ISO/IEC 27001:2022 A5.19, A5.20, A5.21, A5.22, A5.23 · NIST SP 800-53B SR-1 to SR-12, SA-5 · NIST CSF 2.0 GV.SC-01 through GV.SC-10 · SOC 2 TSC CC9.1, CC9.2
Related Policies	POL-001 (IS Policy), POL-003 (Access Control), POL-006 (Privacy Policy)

ResolvX GRC Program — Internal Use Only — v1.0 — 2026

Authorisation

Role	Name	Date
CEO		
CISO		
GRC Lead	Derick G. Dmello	