ResolvX

Information Security Policy

Master Policy — ISMS Apex Document

POL-001 · v1.0 · 2026 · Internal — Restricted

Document Information

Policy ID	POL-001
Version	1.0
Status	Active
Classification	Internal — Restricted
Owner	GRC Lead — Derick G. Dmello
Approver	CEO / CISO
Review Cycle	Annual
Next Review	Q1 2027
Frameworks	ISO 27001:2022 Cl.5.2, A5.1, A5.4 · NIST CSF GV.PO-01/02 · SOC 2 CC1.1–CC1.3

ResolvX — Information Security Policy

1. Purpose

This Information Security Policy establishes ResolvX's commitment to protecting the confidentiality, integrity, and availability of all information assets including customer data, financial records, system infrastructure, and intellectual property in support of its business objectives and its obligations to clients, regulators, and interested parties.

This policy is the apex document of ResolvX's Information Security Management System (ISMS). All topic-specific policies, procedures, and controls derive their authority from this document and must be consistent with it.

ResolvX operates as a cloud-native fintech service organisation processing dispute resolution workflow on behalf of regulated financial institutions. This creates heightened obligations under applicable privacy and financial services regulations, and a corresponding duty to maintain a security posture that enterprise clients can rely upon.

2. Scope

This policy applies to:

- All personnel ; employees, contractors, consultants, interns, and any third party granted access to ResolvX systems or data.
- All information assets, digital, physical, or otherwise, owned, leased, or processed by ResolvX.
- All systems and infrastructure including AWS cloud environments, corporate endpoints, SaaS applications, APIs, and third-party integrations.
- All locations including ResolvX offices, remote work environments, and any location from which ResolvX systems are accessed.

This policy applies globally. Where local laws impose stricter requirements, the stricter requirement prevails.

3. Management Commitment

ResolvX's leadership is committed to:

- Establishing, implementing, maintaining, and continuously improving an effective ISMS aligned to ISO/IEC 27001:2022.
- Ensuring information security objectives are established, communicated, and integrated into business planning.
- Providing sufficient resources, budget, personnel, tooling, and time to implement and maintain this policy.
- Requiring all personnel to comply with this policy and its subordinate policies, procedures, and standards.
- Ensuring information security considerations are embedded in all material business decisions, projects, and changes.
- Conducting periodic management reviews of the ISMS to verify continued suitability, adequacy, and effectiveness.
- Supporting a culture in which security is viewed as an enabler of business rather than a barrier.

This commitment is communicated to all personnel at onboarding and reinforced through mandatory annual security awareness training.

4. Information Security Objectives

ResolvX's information security objectives for the current programme cycle are:

Objective	Target	Measurement	Timeline
Achieve SOC 2 Type II certification	Pass with zero critical findings	Auditor report	Q4 2026
Reduce Critical and High residual risks to zero	0 Critical, ≤3 High residual risks	Risk register review	Q3 2026
Achieve NIST CSF 2.0 Tier 2 (Risk-Informed)	Tier 2 across all functions	CSF maturity assessment	Q3 2026
Implement SIEM and achieve ≥90% log coverage	≥90% of critical systems covered	SIEM coverage report	Q2 2026
Complete Phase 3 policy suite and obtain staff acknowledgement	100% staff acknowledgement	Acknowledgement log	Q2 2026
Establish quarterly access review cycle	100% on-time completion	Access review records	Q1 2026

These objectives are reviewed quarterly by the GRC Lead and updated annually as part of the management review process.

5. Policy Principles

ResolvX's approach to information security is governed by the following principles:

5.1 Confidentiality

Information is accessible only to those with an authorised business need. Access is granted on the basis of least privilege and need-to-know. All personnel have a duty of confidentiality that survives their employment or engagement.

5.2 Integrity

Information is accurate, complete, and protected against unauthorised modification. Controls are in place to detect and respond to integrity failures across all critical systems.

5.3 Availability

Information and systems are available when required to support business operations and client commitments. Resilience, redundancy, and recovery capabilities are maintained and tested.

5.4 Risk-Based Decision Making

Security controls are selected and prioritised based on assessed risk. ResolvX uses the FAIR (Factor Analysis of Information Risk) quantitative model alongside NIST SP 800-30 qualitative assessments to make risk-informed decisions.

5.5 Defence in Depth

No single control is treated as sufficient. Layered controls, technical, procedural, and physical, are implemented such that the failure of any single control does not result in a security breach.

5.6 Continuous Improvement

The ISMS is subject to ongoing monitoring, measurement, and improvement. Lessons learned from incidents, audits, and near misses are used to strengthen the control environment.

5.7 Shared Responsibility

Security is everyone's responsibility. Technical controls are supplemented by a culture of security awareness in which all personnel understand their obligations and act accordingly.

6. Legal, Regulatory, and Contractual Obligations

ResolvX's information security programme must satisfy the following obligations:

Framework / Regulation	Applicability	Primary Owner
SOC 2 Type II (AICPA TSC)	Contractually required by enterprise clients	GRC Lead
ISO/IEC 27001:2022	Certification target — audit readiness programme	GRC Lead / CISO
GDPR (EU 2016/679)	Processing EU personal data of dispute parties	GRC Lead / Legal
CCPA (California Civil Code §1798)	Processing California resident data	GRC Lead / Legal
GLBA (15 U.S.C. §6801)	Serving regulated US financial institutions	Legal
NYDFS Cybersecurity Regulation (23 NYCRR 500)	Downstream obligation via financial institution clients	GRC Lead / Legal
PCI DSS v4.0	Scoped where payment card data is processed	Head of Cloud Ops

Legal and regulatory requirements are documented in the Compliance Obligations Register, which is maintained by the GRC Lead and reviewed quarterly.

7. Roles and Responsibilities

7.1 Chief Executive Officer (CEO)

- Ultimate accountability for the organisation's security posture
- Approves this Information Security Policy
- Ensures adequate resources are allocated to the ISMS

7.2 Chief Information Security Officer (CISO)

- Oversees implementation and operation of the ISMS
- Escalates material risks and incidents to the CEO
- Approves topic-specific policies
- Conducts quarterly ISMS management reviews

7.3 GRC Lead

- Authors and maintains this policy and all topic-specific policies
- Owns the risk register, control framework, and compliance obligations register
- Coordinates the internal audit programme
- Reports on ISMS performance to the CISO and leadership team

7.4 Control Owners (All Roles)

- Implement controls assigned in the Controls Owners Register
- Maintain evidence of control operation
- Report control gaps, failures, or incidents to the GRC Lead
- Participate in periodic control reviews

7.5 All Personnel

- Read, understand, and comply with this policy and all applicable topic-specific policies
- Complete mandatory security awareness training annually
- Report suspected security incidents, policy violations, or unusual activity immediately via the designated reporting channel
- Protect information assets to which they have access

8. Topic-Specific Policies

This master policy is supported by the following topic-specific policies, each of which provides detailed requirements for its subject area:

Policy ID	Policy Title	Owner	Framework Alignment
POL-002	Acceptable Use Policy	GRC Lead	ISO A5.10, NIST PL-4, SOC 2 CC1.2
POL-003	Access Control Policy	IT Admin	ISO A5.15–A5.18, NIST AC-1 to AC-17
POL-004	Data Classification Policy	GRC Lead	ISO A5.12–A5.13, NIST RA-2
POL-005	Vendor Management Policy	GRC Lead	ISO A5.19–A5.23, NIST SR-1 to SR-12
POL-006	Privacy Policy (ROPA + DSR)	GRC Lead / Legal	ISO A5.34, GDPR Art. 30, SOC 2 P1–P8
POL-007	Incident Response Plan	GRC Lead	ISO A5.24–A5.26, NIST SP 800-61
POL-008	Business Continuity Plan	VP Engineering	ISO A5.29–A5.30, NIST CP-1 to CP-13

All topic-specific policies are reviewed annually and upon material change to the business, technology, or regulatory environment.

9. Risk Management

ResolvX manages information security risks in accordance with the Risk Assessment Methodology (POL-RM-001), which is aligned to ISO/IEC 27005:2022 and NIST SP 800-30 Rev. 1.

The key principles are:

- Risk identification: Risks are identified through formal annual assessments, continuous monitoring, threat intelligence, and incident review.
- Risk assessment: Risks are assessed using both qualitative (likelihood × impact) and quantitative (FAIR ALE) methods.
- Risk treatment: For each identified risk, a treatment decision is made; Mitigate, Accept, Transfer, or Avoid, with documented rationale
- Risk acceptance: Residual risks accepted above the defined risk appetite threshold require explicit sign-off by the CISO.
- Risk monitoring: The risk register is reviewed quarterly; high and critical residual risks are reviewed monthly.

The current risk appetite is: **zero tolerance for Critical residual risks; High residual risks require active treatment plans with defined timelines.**

10. Asset Management

All information assets including data, systems, software, and infrastructure must be inventoried, classified, and owned. The asset inventory is maintained in the Company Profile and updated quarterly.

All assets are classified per the Data Classification Policy (POL-004). Handling requirements vary by classification level:

Classification	Examples	Handling Requirement
Restricted	Client PII, financial records, credentials	Encrypted at rest and in transit; strict need-to-know access
Confidential	Internal strategy, contracts, audit materials	Access limited to authorised personnel; not shared externally
Internal	Internal communications, operational data	Not for external distribution without authorisation
Public	Marketing materials, published documentation	No special handling required

11. Incident Management

All information security incidents or suspected incidents must be reported immediately to the GRC Lead via the designated security reporting channel. Personnel must not investigate, remediate, or disclose incidents independently without GRC Lead direction.

Incident management is governed by the Incident Response Plan (POL-007), which defines classification criteria, response procedures, escalation paths, and communication requirements.

12. Compliance and Enforcement

All personnel are required to comply with this policy. Non-compliance may result in:

- Formal warnings or disciplinary action, up to and including termination of employment or contract
- Legal action in cases of wilful misconduct, data theft, or regulatory breach
- Notification to relevant regulatory authorities where required by law

Compliance is monitored through access reviews, security awareness training records, internal audits, and continuous monitoring controls.

13. Exceptions

Requests for exceptions to this policy must be submitted to the GRC Lead in writing. Each exception request must document:

- The specific requirement from which an exception is sought
- The business justification
- The proposed compensating controls
- The requested duration

Exceptions are approved by the GRC Lead and CISO. All approved exceptions are logged in the Policy Exception Register and reviewed at each quarterly management review.

14. Policy Review

This policy is reviewed:

- Annually as part of the ISMS management review cycle
- Upon material change including significant changes to the business model, technology infrastructure, regulatory landscape, or security threat environment
- Following a material security incident to assess whether policy updates are required

Policy updates require CISO approval before publication.

15. Related Documents

- Risk Assessment Methodology (POL-RM-001)
- Controls Owners Register
- Company Profile and Asset Inventory
- Compliance Obligations Register
- All topic-specific policies (POL-002 through POL-008)

16. Definitions

Term	Definition
ISMS	Information Security Management System is the set of policies, procedures, controls, and processes used to manage information security
CIA Triad	Confidentiality, Integrity, and Availability are the three core properties of information security
Risk Appetite	The level of risk ResolvX is willing to accept in pursuit of its objectives
Control Owner	The individual accountable for implementing and maintaining a specific security control
Residual Risk	The risk that remains after controls have been applied
ALE	Annualised Loss Expectancy is a quantitative measure of risk expressed as annual financial exposure

17. Document Control

Field	Detail
Policy ID	POL-001
Version	1.0
Status	Active
Classification	Internal — Restricted
Owner	GRC Lead — Derick G. Dmello
Approver	CEO / CISO
Review Cycle	Annual
Next Review	Q1 2027
Framework References	ISO/IEC 27001:2022 Clause 5.2; Annex A 5.1, 5.4 · NIST SP 800-53B PL-1, PM-1 · NIST CSF 2.0 GV.PO-01/02 · SOC 2 TSC CC1.1, CC1.2, CC1.3
Supersedes	N/A — Initial Issue

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

This policy has been approved by ResolvX leadership and is effective immediately upon publication.

Role	Name	Signature	Date
CEO		_____	_____
CISO		_____	_____
GRC Lead	Derick G. Dmello	_____	_____

Authorisation

Role	Name	Date
CEO		
CISO		
GRC Lead	Derick G. Dmello	