ResolvX

Data Classification Policy

Topic-Specific Policy — Information Asset Handling

POL-004 · v1.0 · 2026 · Internal

Document Information

Policy ID	POL-004
Version	1.0
Status	Active
Classification	Internal
Owner	GRC Lead — Derick G. Dmello
Approver	CISO
Review Cycle	Annual
Next Review	Q1 2027
Frameworks	ISO 27001:2022 A5.12–A5.14 · NIST 800-53B RA-2, MP-3, SI-12 · SOC 2 CC6.1, CC6.7, P1–P8

ResolvX — Data Classification Policy

1. Purpose

This Data Classification Policy establishes a consistent framework for classifying, labelling, and handling ResolvX's information assets based on their sensitivity, business value, and regulatory obligations. Proper classification ensures that information receives an appropriate level of protection throughout its lifecycle from creation or receipt through to secure disposal.

ResolvX processes highly sensitive financial and personal data on behalf of regulated financial institutions. The stakes of misclassification or improper handling are significant, regulatory penalties, contractual breach, reputational damage, and harm to individuals whose data is entrusted to ResolvX's care.

2. Scope

This policy applies to all information created, received, stored, processed, or transmitted by ResolvX, in any format, digital, physical, or verbal, regardless of the system or medium used.

3. Classification Framework

ResolvX uses a four-tier classification scheme aligned to the sensitivity of the information and the potential impact of unauthorised disclosure.

Tier 1 — RESTRICTED

Definition: The most sensitive category. Unauthorised disclosure would cause severe harm to ResolvX, its clients, or individuals including regulatory penalties, significant financial loss, or irreversible reputational damage.

Examples:

- Client PII (names, addresses, financial account numbers, identity documents)
- Financial dispute records and case file contents
- Authentication credentials, API keys, encryption keys, certificates
- ResolvX's own financial records and board-level strategic documents
- Security vulnerability reports, penetration test results, risk assessments
- Personal health information (PHI) if ever processed
- Any data subject to a specific legal confidentiality obligation

Handling Requirements:

Requirement	Standard
Storage	Encrypted at rest using AES-256; AWS KMS or equivalent
Transmission	TLS 1.3 minimum; no unencrypted channels
Access	Strictly need-to-know; quarterly access reviews
Sharing (external)	Prohibited without DPA, NDA, and GRC Lead approval
Physical handling	Printed copies must be shredded; locked storage required
Labelling	Marked "RESTRICTED" on all documents and communications
Logging	All access events logged; anomalies reviewed
Retention	Per retention schedule; reviewed before any retention extension
Disposal	Secure erasure (NIST 800-88 compliant) or physical destruction

Tier 2 — CONFIDENTIAL

Definition: Sensitive business information that, if disclosed without authorisation, could cause material harm to ResolvX's competitive position, client relationships, or business operations.

Examples:

- Internal strategic plans, product roadmaps, and merger/acquisition discussions
- Vendor contracts, pricing agreements, and commercial terms
- Audit reports, gap analyses, and internal control assessments
- Employee personal data and HR records
- Client-specific configurations and integration details (excluding PII)
- Unpatched vulnerability details and security architecture diagrams

Handling Requirements:

Requirement	Standard
Storage	Encrypted at rest; access-controlled
Transmission	Encrypted (TLS); corporate email only
Access	Role-based; manager approval for external sharing
Sharing (external)	Requires NDA; GRC Lead notification for non-standard recipients
Physical handling	Not left unattended; disposed via shredding
Labelling	Marked "CONFIDENTIAL" on documents
Retention	Per retention schedule
Disposal	Secure deletion; no recovery-grade disposal required

Tier 3 — INTERNAL

Definition: Information intended for internal use within ResolvX. Disclosure outside ResolvX without authorisation would be inappropriate but is unlikely to cause significant harm.

Examples:

- Internal policies, procedures, and operating guidelines
- Internal project documentation and meeting notes
- Employee directories and internal contact lists
- General IT operational information
- Internal performance metrics and reporting

Handling Requirements:

Requirement	Standard
Storage	Standard access controls; no special encryption requirement
Transmission	Corporate systems preferred; encryption encouraged
Access	All ResolvX personnel
Sharing (external)	Not for external distribution without manager approval
Physical handling	Do not leave in public view
Labelling	No mandatory label; "INTERNAL" label recommended for clarity
Disposal	Standard deletion is acceptable

Tier 4 — PUBLIC

Definition: Information explicitly approved for public release or that is already in the public domain.

Examples:

- Published marketing materials, website content, press releases
- Published product documentation and API specifications
- Job postings and publicly disclosed company information

Handling Requirements:

Requirement	Standard
Storage	Standard; no special controls
Transmission	No restrictions
Access	No restrictions
Sharing	No restrictions
Labelling	Not required
Disposal	Standard deletion

4. Classification Responsibilities

4.1 Information Owner

Every piece of information has an **Information Owner**, typically the person or team that creates or receives it. Information owners are responsible for:

- Assigning the correct classification at the time of creation or receipt
- Reviewing classification when information is shared, modified, or aged
- Ensuring appropriate handling by all recipients

4.2 All Personnel

All personnel are responsible for:

- Applying the correct classification label to documents and communications they create
- Handling information received from others in accordance with its classification
- Escalating to the GRC Lead when uncertain about how to classify or handle specific information

4.3 GRC Lead

The GRC Lead is responsible for:

- Maintaining and updating this policy
- Providing guidance on classification decisions
- Conducting periodic audits of data classification practices
- Maintaining the data asset inventory with classification metadata

5. Labelling

5.1 Digital Documents

Documents should include a classification label in the header or footer:

- Microsoft 365 / Google Workspace: Use sensitivity labels (configured by IT Admin)
- PDF documents: Classification label in document header
- Email: Classification label in the subject line prefix e.g., `[RESTRICTED]`, `[CONFIDENTIAL]`

5.2 Physical Documents

Physical documents containing Restricted or Confidential information must be:

- Marked "RESTRICTED" or "CONFIDENTIAL" on the cover page
- Stored in locked storage when not in active use
- Disposed of via cross-cut shredding

5.3 Verbal Communication

When communicating Restricted or Confidential information verbally:

- Confirm that only authorised parties are present or on the call
- Do not discuss in public spaces
- Do not leave voicemails containing Restricted information

6. Data Retention

ResolvX retains information in accordance with the following schedule, unless legal or contractual obligations require longer retention:

Data Category	Classification	Retention Period	Basis
Client dispute case files	Restricted	7 years from case close	Contractual / regulatory
Client PII (active)	Restricted	Duration of client relationship + 2 years	GDPR Art. 5(1)(e) / contractual
Client PII (terminated client)	Restricted	2 years from termination	GDPR minimum / contract
Employee records	Confidential	Duration of employment + 7 years	Legal (tax / employment law)
Financial records	Confidential	7 years	Legal (tax)
Security logs	Internal	12 months	SOC 2 / operational
Audit evidence	Confidential	5 years	SOC 2 / ISO 27001
Email and communications	Internal	3 years	Operational
Marketing materials	Public	Until superseded	Operational

Data that has reached the end of its retention period must be disposed of securely and promptly. Data must not be retained beyond its retention period without documented justification and GRC Lead approval.

7. Special Categories of Data

The following categories of data require additional handling controls beyond their classification tier:

7.1 Personal Data (GDPR / CCPA)

All personal data is subject to the requirements of the Privacy Policy (POL-006). Personal data must:

- Only be processed for documented, lawful purposes
- Not be transferred to third countries without adequate safeguards
- Be subject to individual rights requests (access, rectification, erasure, portability)

7.2 Payment Card Data (PCI DSS)

If ResolvX processes, stores, or transmits cardholder data, it must comply with PCI DSS v4.0 requirements. The Head of Cloud Ops is responsible for assessing and maintaining PCI DSS scope.

7.3 Authentication and Cryptographic Material

Credentials, API keys, certificates, and encryption keys are classified as **Restricted** and are subject to additional controls:

- Stored exclusively in authorised secret management tools (1Password, AWS Secrets Manager)
- Never hardcoded in source code, configuration files, or documentation
- Rotated on a defined schedule and immediately upon suspected compromise

8. Cross-Border Data Transfers

Restricted and Confidential data must not be transferred to third countries (outside the EEA or without adequate safeguards) without:

- Legal approval confirming the transfer mechanism (e.g., Standard Contractual Clauses)
- GRC Lead notification and documentation
- A Data Processing Agreement in place with the recipient

9. Compliance and Enforcement

Incorrect classification, mislabelling, or mishandling of data, whether deliberate or negligent, may result in disciplinary action and, where applicable, regulatory notification. Personnel who are uncertain about classification must consult the GRC Lead before proceeding.

10. Document Control

Field	Detail
Policy ID	POL-004
Version	1.0
Status	Active
Classification	Internal
Owner	GRC Lead — Derick G. Dmello
Approver	CISO
Review Cycle	Annual
Next Review	Q1 2027
Framework References	ISO/IEC 27001:2022 A5.12, A5.13, A5.14 · NIST SP 800-53B RA-2, MP-3, SI-12 · NIST CSF 2.0 PR.DS-01 through PR.DS-10 · SOC 2 TSC CC6.1, CC6.7, P1–P8
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	