ResolvX

Acceptable Use Policy

Topic-Specific Policy — Personnel Obligations

POL-002 · v1.0 · 2026 · Internal

Document Information

Policy ID	POL-002
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 A5.10, A6.7 · NIST 800-53B AC-8, PL-4, PS-6 · SOC 2 CC1.2, CC1.4

ResolvX — Acceptable Use Policy

1. Purpose

This Acceptable Use Policy (AUP) defines the rules governing acceptable use of ResolvX's information assets, systems, devices, and networks. It establishes minimum standards of behaviour expected of all personnel when using these assets, whether for business or incidental personal purposes.

This policy exists to protect ResolvX's information assets from misuse, accidental loss, legal exposure, and reputational harm and to protect personnel from inadvertently causing a security incident through unclear expectations.

2. Scope

This policy applies to:

- All employees, contractors, consultants, interns, and temporary staff of ResolvX
- All information assets including corporate devices, cloud systems, SaaS applications, networks, data, and communications infrastructure
- All locations including ResolvX offices, home offices, client sites, and any other location from which ResolvX assets are accessed
- All devices both ResolvX-owned assets and personally-owned devices used to access ResolvX systems (BYOD)

3. General Acceptable Use Requirements

3.1 Business Purpose

ResolvX information assets are provided for legitimate business purposes. Incidental personal use is permitted provided it does not:

- Consume excessive resources or impair system performance
- Violate any provision of this or any other ResolvX policy
- Create legal, regulatory, or reputational risk for ResolvX
- Occur during working hours in a manner that detracts from job performance

3.2 No Expectation of Privacy

Personnel should be aware that ResolvX may monitor use of its systems, networks, and assets for security, operational, and compliance purposes. Use of ResolvX assets constitutes consent to such monitoring. Personnel have no expectation of privacy when using ResolvX-owned systems or when accessing ResolvX systems from personal devices.

3.3 Lawful Use Only

All use of ResolvX assets must comply with applicable laws and regulations. Illegal use of ResolvX assets is strictly prohibited and may result in immediate termination and referral to law enforcement.

4. Device Use

4.1 Corporate Devices

All ResolvX-issued devices are managed via Jamf MDM and are subject to:

- Full-disk encryption (FileVault for macOS, BitLocker for Windows)
- Automatic screen lock after 5 minutes of inactivity
- Mandatory operating system and security updates
- Endpoint Detection and Response (EDR) agent
- Remote wipe capability

Personnel must not:

- Disable or tamper with MDM management, encryption, or EDR agents
- Install unauthorised software outside the approved software catalogue
- Physically modify corporate devices

Personnel must:

- Immediately report lost or stolen devices to IT Admin
- Not leave devices unattended in public places without locking the screen
- Return all corporate devices upon termination or upon request

4.2 Personal Devices (BYOD)

Personal devices may be used to access ResolvX systems only if:

- The device is enrolled in Jamf MDM or meets the minimum security baseline defined by IT Admin
- The device has full-disk encryption enabled
- MFA is enabled for all ResolvX accounts accessed from the device
- The device runs a supported, patched operating system

Personal devices used for ResolvX access may be subject to security monitoring of ResolvX-related activity. ResolvX data stored on personal devices must be removed upon termination.

4.3 Removable Media

Use of removable media (USB drives, external hard drives, SD cards) with ResolvX data is prohibited unless specifically authorised by the IT Admin for a documented business purpose. Authorised removable media must be encrypted.

5. Network and Internet Use

5.1 Corporate Network

The corporate network is provided for business use. All traffic on ResolvX networks may be monitored. Personnel must not:

- Attempt to bypass network security controls, firewalls, or filters
- Connect unauthorised devices to the corporate network
- Enable network bridging or routing that could expose ResolvX systems

5.2 Public and Untrusted Networks

When working remotely from public or untrusted networks (cafes, hotels, airports):

- VPN must be active before accessing any ResolvX system or data
- Personnel must ensure screens are not visible to bystanders when handling sensitive information

5.3 Internet Use

Internet access is provided for business purposes. Acceptable internet use includes research, accessing business tools, and communication with clients and vendors. The following activities are explicitly prohibited:

- Downloading unlicensed software, media, or copyrighted content
- Accessing or distributing content that is illegal, offensive, or harassing
- Using ResolvX systems to conduct personal commercial activities
- Using anonymising tools (Tor, VPNs not provided by ResolvX) to conceal activity

6. Email and Communications

6.1 Email

Corporate email (Google Workspace / M365) is the authorised platform for business communications. Personnel must:

- Not use personal email accounts for ResolvX business communications involving non-public information
- Exercise caution before clicking links or opening attachments — when in doubt, verify with the sender via a separate channel
- Report suspected phishing emails to the GRC Lead before clicking anything
- Not auto-forward corporate email to personal accounts

6.2 Messaging and Collaboration Tools

Authorised communication platforms include Slack, Google Meet, and Zoom. Personnel must not:

- Share Restricted or Confidential information via unauthorised messaging applications
- Enable automatic cloud backup of business conversations to personal cloud accounts

6.3 Social Media

Personnel must not:

- Share non-public ResolvX information, client information, or product roadmap details on social media
- Represent personal opinions as ResolvX's position
- Use ResolvX's name or logo in personal social media profiles in a manner that implies official endorsement

Authorised social media activity (e.g., LinkedIn posts about ResolvX achievements) is permitted and encouraged but must not disclose confidential or client-identifiable information.

7. Data Handling

7.1 Data Classification

All ResolvX information must be handled in accordance with its classification level as defined in the Data Classification Policy (POL-004). Personnel are responsible for correctly identifying and handling data per its classification.

7.2 Client Data

Client data including PII, financial records, and dispute case files is among ResolvX's most sensitive assets. Personnel must:

- Access client data only for documented business purposes
- Never download, export, or copy client data to personal devices or unauthorised locations
- Never share client data with third parties without a valid legal basis and appropriate agreements in place
- Report any suspected unauthorised access to or disclosure of client data immediately

7.3 Data at Rest and in Transit

- All sensitive data stored locally must be encrypted
- All data transmitted externally must use TLS 1.2 or higher
- Unencrypted transmission of Restricted or Confidential data is prohibited

7.4 Data Disposal

Data must be disposed of in accordance with the Data Classification Policy. Electronic data must be securely deleted or device-wiped. Physical documents containing sensitive information must be shredded.

8. Password and Authentication Requirements

All personnel must comply with the following minimum requirements, enforced by the Okta identity platform:

Requirement	Standard
Minimum password length	14 characters
Password complexity	Mixed case, numbers, and special characters
Password reuse	Last 12 passwords may not be reused
MFA	Required for all ResolvX systems ; no exceptions
Password manager	1Password is the authorised password manager
Shared credentials	Strictly prohibited ; all accounts must be individual

Personnel must:

- Never share passwords with anyone including colleagues or IT staff
- Never write down passwords in plaintext
- Immediately report suspected credential compromise to IT Admin

Privileged accounts (admin access, cloud console) have additional requirements defined in the Access Control Policy (POL-003).

9. Software and Application Use

9.1 Approved Software

Only software approved by IT Admin or included in the Jamf-managed catalogue may be installed on corporate devices. Requests to use new software must be submitted to IT Admin for evaluation.

9.2 AI and Generative AI Tools

Use of AI tools (including ChatGPT, Claude, Gemini, Copilot, and similar) is permitted for productivity purposes subject to the following restrictions:

- Prohibited: Inputting client PII, financial data, credentials, source code, or any Restricted or Confidential data into any AI tool whether a consumer product or API.
- Permitted: Using AI tools with Internal or Public information for drafting, summarisation, and research.
- Outputs from AI tools must be reviewed for accuracy before being used in client-facing or regulatory contexts.

9.3 Open Source and Third-Party Libraries

Use of open-source software in ResolvX products must comply with the secure development lifecycle (POL-SDLC). Developers must not introduce open-source components without reviewing licence obligations and conducting a vulnerability check.

10. Physical Security

Personnel are responsible for physical security of information assets in their custody. This includes:

- Locking workstations when leaving a desk even briefly.
- Not allowing tailgating through secure areas.
- Not leaving sensitive documents visible or accessible to unauthorised persons.
- Following clean desk practices, clearing desks of sensitive materials when unattended.

11. Reporting Obligations

All personnel must promptly report the following to the GRC Lead:

- Lost or stolen devices
- Suspected phishing attempts or social engineering
- Accidental disclosure of client or confidential data
- Suspected policy violations by colleagues
- Any unusual system behaviour or suspected security incident

Reports can be made via the #security-alerts Slack channel, by email to the GRC Lead, or by direct message. Anonymous reporting is available via the GRC Lead.

Early reporting reduces harm and is always treated in a manner that protects the reporter who acts in good faith.

12. Compliance and Enforcement

Violations of this policy will be addressed through ResolvX's disciplinary process, which may include:

- Formal warning
- Suspension of system access
- Termination of employment or contract
- Legal action in cases of wilful misconduct or criminal activity

Severity of consequences will be proportionate to the nature and impact of the violation, whether the violation was deliberate or negligent, and whether the violation resulted in actual harm.

13. Exceptions

Exceptions to this policy require written approval from the GRC Lead. Approved exceptions are time-limited (maximum 90 days unless renewed) and are logged in the Policy Exception Register.

14. Acknowledgement

All personnel must acknowledge receipt and understanding of this policy at onboarding and annually thereafter. Acknowledgement records are maintained by HR.

15. Document Control

Field	Detail
Policy ID	POL-002
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 A5.10, A6.7 · NIST SP 800-53B AC-8, PL-4, PS-6 · NIST CSF 2.0 GV.PO, PR.AT · SOC 2 TSC CC1.2, CC1.4
Supersedes	N/A — Initial Issue
Related Policies	POL-001 (IS Policy), POL-003 (Access Control), POL-004 (Data Classification)

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

Authorisation

Role	Name	Date
CEO		
CISO		
GRC Lead	Derick G. Dmello	