VULNERABILITY DISCLOSURE POLICY			
Document Reference	VULNERABILITY DISCLOSURE POLICY	*Effective Date*	1 July 2026
Document Approval	Chief Digital and Technology Officer	*Review Date*	20 April 2026
Document Ownership	CISO	*Version*	V 1.0

Contents

VULNERABILITY DISCLOSURE POLICY			
Document Reference	VULNERABILITY DISCLOSURE POLICY	*Effective Date*	1 July 2026
Document Approval	Chief Digital and Technology Officer	*Review Date*	20 April 2026
Document Ownership	CISO	*Version*	V 1.0

RESPONSIBLE DISCLOSURE POLICY

PURPOSE –

This policy outlines how Aramex engages with external security researchers to identify and report potential vulnerabilities in our digital infrastructure. We welcome responsible security research and are committed to working with the security community to protect our customers and improve our security posture.

SCOPE

This policy applies to the Aramex Group systems and services mentioned in Annex – 1

SAFE HARBOUR

Aramex supports responsible security research and will not pursue legal action against researchers who:

- Act in good faith and comply with this policy
- Report vulnerabilities through the designated channel
- Do not access, modify, or delete customer or company data or violate privacy
- Do not disrupt our services or degrade system performance
- Do not publicly disclose vulnerabilities before we have addressed them

We consider activities conducted under this policy to constitute "authorized" conduct under applicable anti-hacking laws, and we will not initiate legal action against you for such activities, provided you do not act maliciously or with malicious intent. If legal action is initiated by a third party against you based on your participation in this program, we will take steps to make it known that your actions were conducted in compliance with this policy. This protection applies only to good-faith security research conducted within the defined scope and rules.

HOW TO REPORT:

If you believe you've found a security vulnerability, please send it to us on reportcyber@aramex.com.

Include in your report:

In addition to your contact details, include the following in your report:

- Clear description of the vulnerability and its location
- Step-by-step reproduction instructions
- Screenshots or proof-of-concept (when it is safe to do so)
- Potential impact assessment
- Your contact information

- **We are interested in vulnerabilities such as:**

- Authentication and authorization flaws
- Injection Attacks (SQL, XML, Json, etc)
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Server-Side request forgery (SSRF)
- Server-side code execution (RCE)
- Privilege escalations
- Business logic flaws
- Insecure direct object references

TESTING GUIDELINES

Permitted activities:

- Testing only on systems within our defined scope
- Using automated scanner with rate limiting to avoid service disruption
- Creating test accounts with obviously fake information
- Testing authentication and session management
- Analyzing client-side code and APIs.

- **Prohibited activities**

Do not:

- Access, modify or delete data belonging to other users
- Perform denial or service (DoS) or distributed denial of service (DDoS)
- Conduct social engineering attacks against our employees or customers.
- Perform physical security testing
- Install any back doors or malicious software.
- Spam or send unsolicited communications
- Violate privacy or users or employees
- Continue testing after discovering a vulnerability.
- Share access credentials or vulnerability details with others.

Out of scope

We do not accept reports for:

Out-dated software without proof of exploitability

- Missing security headers without demonstrated impact
- SSL/TLS configuration issues without proof of exploitability
- Click-jacking on pages without sensitive actions
- CSRF on forms available to anonymous users
- Logout Cross-Site Request Forgery (CSRF)

- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Social engineering attacks
- Physical security issues
- Third party applications or services
- UI/UX bugs and spelling mistakes
- Public information disclosure (robots.txt, etc)
- SSL Attacks such as BEAST, BREACH, Renegotiation attack
- SSL Forward secrecy not enabled
- SSL Insecure cipher suites
- The Anti-MIME-Sniffing header X-Content-Type-Options

VULNERABILITY DISCLOSURE POLICY		aramex	
Document Reference	VULNERABILITY DISCLOSURE POLICY	*Effective Date*	1 July 2026
Document Approval	Chief Digital and Technology Officer	*Review Date*	20 April 2026
Document Ownership	CISO	*Version*	V 1.0

OUR COMMITMENT

When you report a valid vulnerability we will –

- Acknowledge receipt within 2 business days
- Provide regular updates on our investigation progress
- Work with you to understand and validate the issue
- Address confirmed vulnerabilities based on risk and impact
- Credit you for the discovery (unless you prefer to remain anonymous)
- Not pursue legal action for good-faith research conducted under this policy.

Response timeline:

- Initial acknowledgment: 2 business days
- Vulnerability assessment: 10 business days
- Resolution timeline: Varies by severity (communicated during assessment)

BOUNTY PROGRAM

We offer monetary rewards for qualifying vulnerability reports as a token of appreciation for responsible disclosure.

Eligibility Requirements

- First to report the vulnerability
- Follows all policy guidelines
- Provides clear reproductive steps
- Demonstrates real security impact
- Does not publicly disclose before resolution

VULNERABILITY DISCLOSURE POLICY		aramex	
Document Reference	VULNERABILITY DISCLOSURE POLICY	*Effective Date*	1 July 2026
Document Approval	Chief Digital and Technology Officer	*Review Date*	20 April 2026
Document Ownership	CISO	*Version*	V 1.0

Eligibility Matrix for Bounty Rewards

Severity Level	Description	Examples	Reward Range
Critical	SSystem compromise, sensitive data access, RCE	- Remote code execution, database access, admin privilege escalation	$500 - $5000
High	Significant data exposure, privilege escalation.	- SQL injection with data access, stored XSS affecting multiple users	$200 - $500
Medium	Limited data exposure user account compromise.	Reflected XSS, CSRF with impact, information disclosure	$50 - $200
Low	Minimal impact, theoretical vulnerabilities.	-Minor information leakage, low-impact configuration issues	$10 - $50

Note: Final reward amounts are determined based on vulnerability severity, impact, exploitability, and report quality. Decisions are at Aramex's sole discretion.

VULNERABILITY DISCLOSURE POLICY			
Document Reference	VULNERABILITY DISCLOSURE POLICY	*Effective Date*	1 July 2026
Document Approval	Chief Digital and Technology Officer	*Review Date*	20 April 2026
Document Ownership	CISO	*Version*	V 1.0

DISCLOSURE TIMELINE

Coordinated Disclosure Process:

1. Report submitted and acknowledged
2. Vulnerability validated and assessed
3. Fix developed and deployed
4. Public disclosure (if applicable) after 90 days or upon fix deployment, whichever comes first

Public Disclosure:

- We may publicly acknowledge the researcher (with permission)
- Technical details may be shared in security advisories
- Researchers should not publicly disclose without written consent

LEGAL CONSIDERATIONS

- This policy applies only to Aramex's systems within the defined scope
- Testing must comply with applicable laws in your jurisdiction
- We reserve the right to modify this policy at any time
- Violation of this policy may result in suspension from the program and potential legal action
- This policy does not create any employment relationship

QUESTIONS

For questions about this policy, contact: reportcyber@aramex.com

VULNERABILITY DISCLOSURE POLICY			
Document Reference	VULNERABILITY DISCLOSURE POLICY	*Effective Date*	1 July 2026
Document Approval	Chief Digital and Technology Officer	*Review Date*	20 April 2026
Document Ownership	CISO	*Version*	V 1.0

Annex – 1

In-Scope Domain List
*.shopandship.com
*.aramex.com
*.aramex.net
*.aramex.co.nz
*.aramex.com.au
*.aramex.au
*.aramex.net
*.aramex.co.za
*.myus.com
*.aramexgo.com
myus.com
aramex.co.nz
aramex.com.au
aramexgo.com
aramex-china.cn
returnsunlimited.com
aramex.cn
aramexconnect.com.au
aramexconnect.co.nz
fastwayenquiries.com
fastwayifms.com
fastway.org
myaramex.me
boundr.com
doorstep.global
Mybermudapost.bm
Goshop.mv
Ugotbox.com
Marketsz.com
myaccount.wa9il.me
Redboxshipping.com
myaccount.ws1.com
www.shop8home.com
fastwaycustomer.com
fastwaycustomer.com
fastway.com.au

END OF THE DOCUMENT