Vulnerability Disclosure

Table of Contents

Introduction.......... 3

Scope.......... 3

Contact Information & Vulnerability Reporting.......... 3

Bug Bounty.......... 3

Triage and Remediation.......... 3

Confidentiality.......... 3

Policy Updates.......... 3

Introduction

Groupe Atlantic UK, ROI & North America (GA UK) and its associated companies are committed to maintaining the security of our systems and protecting sensitive information, this policy outlines the process for reporting vulnerabilities in our systems and services.

Scope

This policy applies to any security vulnerabilities found within any digital service or system operated by GA UK.

Contact Information & Vulnerability Reporting

For further inquiries or to report a vulnerability, send an email to: security@groupe-atlantic.co.uk

The report should include four key items:

1. A description of the vulnerability
2. The potential impact
3. Any steps to identify or exploit the vulnerability
4. Your contact information for follow-up

Bug Bounty

A bug bounty program is a deal offered by websites, organizations, and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. GA UK does not offer a bug bounty program. All vulnerability reports are voluntary, and we do not compensate reporters for identifying potential or confirmed vulnerabilities.

Triage and Remediation

Upon receiving a report, GA UK will:

- Acknowledge receipt within five working days
- Triage the reported vulnerability to assess the severity and impact
- Work to remediate verified vulnerabilities within 90 days of the report

Confidentiality

All reports will be treated as confidential. Reporters are also requested to keep vulnerabilities confidential until a resolution is found.

Policy Updates

This policy will be updated to reflect changes in regulations or security best practices.