Vulnerability Disclosure Policy

EFFECTIVE AS OF JUNE 3, 2025

Introduction

Firmex, the cloud-based SaaS platform, is committed to securing our products, services and maintaining the trust of our customers. This policy prescribes how security researchers must conduct vulnerability discovery activities and submit those discovered vulnerabilities responsibly to Firmex. With our SaaS based platform, no patching is required to apply remediations to vulnerabilities, thus we will work directly with the researchers to confirm and validate that fixes have been applied and no longer exist. For our mobile application, we will publicly mention any security fix in the application release notes.

You Should

- Respect the rules. Operate within the rules set forth herein or please contact us.
- Respect privacy. Do not access or destroy another user's data.
- Be patient. Make a good faith effort to clarify and support your reports upon request.
- Do no harm. Act prudently and for the common good. Promptly report of all found vulnerabilities. Never willfully exploit others without their permission.

We encourage you to contact us to report potential vulnerabilities in our systems. Thank you in advance for your submission and discretion, we appreciate researchers assisting us in our security efforts.

Authorization

In consideration for complying with this policy, Firmex authorizes you to conduct security research. We will work with you to understand and resolve the issue quickly, and will not recommend or pursue legal action related to your research nor support any third-party legal action brought against, unless required by law, for activities that were conducted in accordance with this policy.

Guidelines

Under this policy, “research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent strictly necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Do not submit a high volume of low-quality findings.
- Use only the Official Channels to communicate vulnerability information with us.
- You attest you are not a resident of, or will not make your Submission from, an embargoed country or region of the Canada or United States or that you are not, nor do you represent a legal entity, that is currently under Canada/U.S.sanction (e.g., Cuba, Iran, North Korea, Sudan, Syria and Crimea);

Once you’ve established that a vulnerability exists or if you’ve encountered any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must cease your test, notify us immediately, and not disclose this data to anyone else**.

You agree that you will keep information related to the vulnerability confidential and will not disclose the vulnerability to any third-party unless Firmex has provided you with written authorization to do so even if you decide not to report it. By submitting your vulnerability, you hereby grant Firmex the right to use, create derivatives of, disclose, or modify any information that you have provided.

Scope

This policy applies to the following systems and services:

Firmex.com, and the following hostnames:

firmex.com

login.firmex.com

api.firmex.com

Any other subdomain of Firmex.com and all customer applications are excluded from this policy.

Mobile applications for iOS

Any service not expressly listed above, such as any connected services or third-party systems, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us using the form below before starting your research.

While we encourage you to discover and report to us any vulnerabilities you find in a responsible manner, the following conduct is expressly prohibited:

- Performing actions that may negatively impact Firmex or its users (e.g. Spam, Brute Force, Denial of Service…) or other tests that impair access to or damage a system or data.
- Accessing, or attempting to access, data or information that does not belong to you.
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.
- Social engineering any Firmex service desk, employee, or contractor.
- Violating any laws or breaching any agreements in order to discover vulnerabilities.
- Use of leaked credentials is strictly prohibited. If customer or staff credentials are found, you must not test with them and should report them to Firmex immediately.

The following issues are considered out of scope please confirm your submission is not one of:

- Clickjacking on pages with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration.
- Any activity that could lead to the disruption of our service (DoS).
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS

- Rate limiting or bruteforce issues on non-authentication endpoints
- Missing best practices in Content Security Policy.
- Missing HttpOnly or Secure flags on cookies
- Missing email best practices (Invalid, incomplete or missing SPF/DKIM/DMARC records, etc.)
- Vulnerabilities only affecting users of outdated or unpatched browsers [Less than 2 stable versions behind the latest released stable version]
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Tabnabbing Vulnerability
- Open redirect – unless an additional security impact can be demonstrated
- Issues that require unlikely user interaction
- Results from automated tooling
- Internal IP address disclosure
- Issues related to robots.txt
- Verbose error messages with no significant impact

Reporting a Vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. We will not share your name or contact information without your express permission.

Submitting your vulnerability constitutes acceptance of this Vulnerability Disclosure Policy. Therefore, first, you should review this Vulnerability Disclosure Policy. Then submit the vulnerability using the Official Communication Channels. If you share contact information, we will acknowledge receipt of your report within a timely manner.

Upon receipt of the report, we will review and investigate the vulnerability without undue delay. We shall make every effort to notify you when this investigation starts. We will internally assess the finding using a variety of methods to calculate severity. If we determine that vulnerability requires remediation, we will start remediating the vulnerability as soon as practicable.

Official Communication Channels

Vulnerability reports should be submitted by contacting our team at security-alert@Firmex.com.

We do not support PGP-encrypted emails. For particularly sensitive information, reach out directly via the email address provided and ask for a meeting to be setup to discuss.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports contain the following information:

- Summary Title
- Researcher Name
- Researcher Email
- Describe the location (URL) in which the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability.
- It is recommended to include a video or screenshot as Proof-of-Concept in your submissions. These files should not be shared publicly. This includes uploading to any publicly accessible websites (e.g. YouTube, Imgur).
- Well written reports in English will have a higher chance of being accepted.
- Reports that include proof of concept code will be more likely to be accepted.
- Reports that include only crash dumps or other automated tools output will most likely not be accepted.
- Reports that are outside of the scope listed above will most likely be ignored.

What you can expect from us

When you choose to share your contact information with us, we shall make every effort to coordinate with you quickly and openly.

- Extend **Safe Harbor** (see below) for your vulnerability research that complies with this policy.
- Within a timely manner, we will acknowledge that your report has been received, assuming proper contact information has been included.

- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.
- Firmex does not operate a public bug bounty program.

Safe Harbor

When conducting vulnerability research in compliance this policy and applicable laws, we consider this research to be:

- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws), and we will not initiate or support legal action against you for accidental, good faith violations of this policy.
- Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technology controls.
- Exempt from restrictions in our Terms of Use that would interfere with conducting security research, and we waive those restrictions on a limited basis for work done under this policy.
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

If at any time you have questions or concerns or you are uncertain whether your security research is consistent with this policy, please submit a report through our Official Channels before going any further.

By reporting a vulnerability, you hereby acknowledge the foregoing and that you have carefully read, fully understand and knowingly and voluntarily agree to Firmex's Vulnerability Disclosure Policy.