Achieva Credit Union Vulnerability Disclosure Policy

Introduction

Achieva Credit Union ("Achieva") welcomes feedback from security researchers and the general public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you. This policy outlines steps for reporting vulnerabilities to us, what we expect, and what you can expect from us.

Systems in Scope

This policy applies to the following website(s) and system(s) owned, operated, or maintained by Achieva: https://www.achievacu.com.

Out of Scope

Websites, assets, or other systems or equipment not owned by Achieva are excluded from this policy and are not authorized by Achieva for security research.

Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority. If you're unsure whether a system is in-scope or out-of-scope, contact us at the Official Channel (stated below) before starting your research.

Our Commitments

If you comply with this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints; and
- Extend Safe Harbor (discussed below) for your vulnerability research that is related to this policy.

Notwithstanding the foregoing, Achieva may be unable to share certain information with you for security, legal, or other reasons, and Achieva reserves all rights, and has complete discretion, to determine what information to share, if any, with you or any third parties.

Achieva does not agree to provide any "bug bounty," financial payment, or other compensation, rewards, or recognition for any research or reports, and you understand and agree that Achieva will not pay or otherwise compensate you.

Our Expectations

In participating in our vulnerability disclosure program, you agree to:

- Play by the rules, including complying with this policy and all applicable laws and regulations;

- Promptly report to Achieva (and no one else) any vulnerability you've discovered as to the above-described in-scope website or system;
- Avoid violating the privacy or safety of others, disrupting our websites and systems, conducting a network denial-of-service (Dos or DDos) test or other actions that impair access to or damage a website, system or data, conducting social engineering or spear phishing of Achieva personnel, members, or contractors, destroying data, and/or harming user experience;
- Avoid compromising or infringing the intellectual property or other commercial or financial interests of Achieva or its personnel, members, or contractors;
- Avoid exfiltrating, copying, or deleting data;
- Avoid establishing command line access and/or persistence, pivoting to out-of-scope systems, escalating privileges, disrupting access to Achieva's websites or systems, or introducing any malware;
- Use only the Official Channel to discuss vulnerability information with us;
- Keep your research confidential and not disclose any details about your research, report, or any vulnerability to the public, or any other third party, until and unless Achieva remediates the vulnerability and provides you with specific explicit written authorization to disclose information about the vulnerability, and you agree any disclosure shall be limited to the extent of Achieva's written authorization;
- Limit your actions to confirm whether a vulnerability exists and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Protected Health Information (PHI), credit card data, bank account or other financial information, or proprietary information or trade secrets;
- Interact only with test accounts you own or with explicit permission from the account holder; and
- Not engage in extortion.

If you engage in unlawful conduct or violate this policy, Achieva reserves all claims and remedies.

Official Channel

Please report security issues via **https://www.achievacu.com/Home/VulnerabilityDisclosure**, providing all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.

Safe Harbor

If you comply with this policy and applicable law, and act in good faith in conducting your research, we will consider your research to be authorized and exempt from restrictions in our Terms of Service and Acceptable Usage Policy that would interfere with conducting security research, and we will waive those restrictions on a limited basis.

If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

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

Note that the Safe Harbor applies only to legal claims under the control of Achieva and that the policy does not bind independent third parties.

Achieva reserves the right to share any of your research or report with any third parties in Achieva's discretion.

Modification or Termination of This Policy

Achieva reserves the right to change or terminate this policy at any time for any reason in Achieva's discretion and without prior notice.