edifecs®

Vulnerability Disclosure Policy

INTRDUCTION

Edifecs, Inc. values feedback from security experts, external researchers and the general public to enhance our security measures. If you believe you have identified a vulnerability, privacy issue, exposed data, or any other security concern involving Edifecs and our IT assets, networks, systems, or processes, then we encourage you to report it. This policy details the steps for reporting vulnerabilities, our expectations from you, and what you can expect from us.

SCOPE

This policy applies to all IT assets, networks, systems, or processes owned, operated, or maintained by Edifecs, Inc. It addresses the potential misuse of, or unauthorized access to, Edifecs' assets in ways that violate our terms of use and/or our privacy policy(ies) and may cause harm.

OUR COMMITMENTS

When working with us under this policy, you can expect the following:

- We will respond to your report promptly and collaborate with you to understand and validate it, aiming to complete this process within thirty (30) days.
- We will keep you informed about the progress of the vulnerability as it is being addressed.
- We will work to remediate discovered vulnerabilities in a timely manner, within our operational constraints.
- We will extend safe harbor for vulnerability research related to this policy.

OUR EXPECTATIONS

When participating in our vulnerability disclosure program in good faith, we ask that you:

- Follow this policy and any other relevant agreements. If there is any inconsistency between this policy and other applicable terms, this policy will prevail.
- Report any discovered vulnerabilities promptly.
- Avoid violating others' privacy, disrupting our systems, destroying data, or harming user experience.
- Use only the designated email address (<EMAIL ADDRESS>) to discuss vulnerability information with us.
- Keep the details of any discovered vulnerabilities confidential until authorized for release by the Edifecs, Inc. security team, which aims to provide authorization within 90 days of receiving each report.
- Allow us a reasonable amount of time to resolve the issue.
- Perform testing only on in-scope systems and respect out-of-scope systems and activities.
- If a vulnerability provides unintended access to data, limit the amount of data accessed to the minimum required for demonstrating a Proof of Concept. Cease testing and submit a report immediately if you encounter any user data, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data (PCI), or other non-public confidential or proprietary information.
- Only interact with accounts you own.
- Do not engage in extortion.
- Note that Edifecs, Inc. does not offer compensation for vulnerability information.

At Edifecs Inc., we welcome vulnerability disclosure without conditions attached. While we do not offer monetary compensation for vulnerability information, we appreciate your efforts to help us maintain the highest standards of security. We strictly prohibit any form of extortion, threats, or coercion. Please note that Edifecs, Inc. will not provide safe harbor for vulnerabilities shared under threat of public disclosure, data exposure, or non-disclosure.

OUT OF SCOPE

The following items are non-exhaustively out-of-scope:

- Assets or equipment not owned by parties participating in this policy. (Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or authority).
- Any attacks intended to degrade, deny, or negatively impact services or user experience—such as brute force, denial of service, spamming, and fuzzing—are strictly prohibited unless specifically permitted by Edifecs, Inc.
- Attacks intended to destroy, corrupt, or render data unreadable are strictly prohibited if the data does not belong to you.
- Attacks that exploit stolen or reused credentials, account takeovers, hijacking, and other forms of credential-based activities.
- Deliberately accessing data or information that is not rightfully yours, beyond the minimum access necessary to demonstrate a vulnerability.
- Physically or electronically gaining access to Edifecs, Inc. personnel, offices, wireless networks, or property through social engineering, phishing, or any other means is strictly prohibited.
- Attacks linked to email servers, including those associated with email protocols, security measures like SPF, DMARC, and DKIM, as well as email-based spam.
- Reports of insecure SSL/TLS ciphers, unless accompanied by a working proof-of-concept.
- Reports of missing HTTP headers (e.g., lack of HSTS), unless accompanied by a working proof-of-concept.
- Reports of iFraming on pages where no sensitive/user action is required.

OFFICIAL CHANNELS

Please report security issues via <EMAIL ADDRESS>, including all relevant information. The more details you provide, the easier it will be for us to triage and resolve the issue

SAFE HARBOR

When conducting vulnerability research under this policy, we consider your actions to be:

- Authorized under applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy.
- Authorized under relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls.
- Exempt from restrictions in our Terms of Service (TOS) and/or Acceptable Usage Policy (AUP) that would interfere with conducting security research, and we waive those restrictions on a limited basis.
- Lawful, beneficial to the overall security of the Internet, and conducted in good faith.

You are expected to comply with all applicable laws. If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to disclose that your actions complied with this policy.

If you have concerns or are uncertain whether your security research aligns with this policy, then please submit a report through one of our Official Channels before proceeding.

Please note that Safe Harbor applies only to legal claims under the control of the organization participating in this policy and does not bind independent third parties.

REPORTING

To report a security issue or vulnerability, please follow this process:

1. Gather as much technical information as possible, including steps to reproduce and validate the issue.
2. Email your report to the Edifecs security team via <EMAIL ADDRESS> within 24 hours of discovery.
3. Allow up to 5 business days for confirmation of the reported issue.

ENFORCEMENT AND PERIODIC REVIEW
Compliance with this policy will be monitored through regular audits. Non-compliance will result in corrective actions to ensure adherence to the policy.

This policy will be reviewed annually or following significant changes in the organization or technology. Updates will be made to address new threats and ensure alignment with industry best practices.