

CHANGELOG

VERSION	LAST UPDATED	CHANGES
1.0	07/05/2026	Document creation.

VULNERABILITY DISCLOSURE POLICY



To work collaboratively with the security community to improve our cyber resilience and protect user data,

Embrace-IT ApS

CVR no. 36942320

Kildehøjvej 12

3460 Birkerød

Denmark

encourages you to contact us to report potential security issues in our systems by following this policy.

1. INTRODUCTION

Embrace-IT ApS, CVR no. 36942320 (hereinafter "embrace-it") is committed to ensuring the security of our communication and information systems and protecting information. The policy represents our collective commitment to safeguarding the privacy and rights of individuals whose data we process.

This policy describes what systems and types of research that are covered and how to send us vulnerability reports. We encourage you to contact us to report on potential vulnerabilities in our systems.

2. AUTHORIZATION

If you are acting in good faith to identify and report vulnerabilities on embrace-it systems, while complying with this policy, we will work with you to understand and resolve the issues quickly. embrace-it will not recommend or pursue legal action related to your activities of identifying vulnerabilities on our systems as long as you follow the guidelines in this policy. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

3. SCOPE

This policy applies to the following systems and services, namely all internet-facing systems operated by embrace-it:

- the entire web presence of embrace-it
- public IPs
- any other software published by embrace-it

Any services not expressly listed above are excluded from the scope and are not authorized for testing. Additionally, vulnerabilities found in systems from vendors are also excluded from the scope and should be reported directly to the vendor according to their own disclosure policy (if any). If you aren't sure whether a system is in scope, please contact us at security@embrace-it.com.

4. GUIDELINES

While carrying out your activities in accordance with this policy, it's imperative that you:

- notify us as soon as possible after you discover a real or potential security issue
- do not take advantage of the vulnerability or problem you have discovered
- only use harmless exploits to confirm that a vulnerability is present
- make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data
- do not reveal any data downloaded during the discovery of the vulnerability or problem to the public or any other parties
- do not submit a high volume of low-quality reports
- stop your tests when you discover sensitive information, notify us immediately, and do not disclose any obtained data to anyone else

5. TEST METHODS

The following test methods are not authorized:

- place malware (virus, worm, Trojan horse, etc.) on any system
- compromise any systems using exploits to gain full or partial control
- copy, modify or delete data from the system
- make changes to the system
- repeatedly access the system or share access with the public or other parties
- use any access obtained to attempt to access other systems
- change access rights of other users
- use automated scanning tools
- use a so-called "brute force" attack to access any systems
- use denial-of-service or social engineering (phishing, vishing, spam, etc.)
- use attacks on physical security

6. REPORTING

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If you have identified a vulnerability or security issue on embrace-it's systems, please:

- email your findings as soon as possible to security@embrace-it.com (reports may be submitted anonymously)
- do not attach particularly sensitive information without encryption
- provide us with sufficient information to reproduce the problem so that we can resolve it as quickly as possible. Typically, this includes the location of the vulnerability, the potential impact of exploitation, and a detailed description of the steps needed to reproduce the it (proof-of-concept scripts or screenshots are helpful)
- preferably provide your report in English, or in any other official language of the European Union

When you choose to share information with us, we commit to coordinating with you as openly and as quickly as possible. We will handle your report with strict confidentiality and be as transparent as possible about what steps we are taking during the remediation process.

We will acknowledge that your report has been received within 3 business days, and we aim to resolve reported vulnerabilities within 90 days. For critical vulnerabilities, we will provide an initial assessment within 5 business days. We will keep you informed of our progress and agree on a disclosure timeline before any public disclosure is made.

7. QUESTIONS

Questions regarding this policy may be sent to our legal compliance department at compliance@embrace-it.com. We also invite you to contact us with suggestions for improving this policy.