GRC+

Responsible Disclosure Policy

CLASSIFICATION	VERSION	IN EFFECT FROM
PUBLIC	3.0	12 November 2026

LATEST VERSION
grc.plus/security

Check this address before you rely on a printed or saved copy.

© 2026 GRC+

Document Control

FIELD	VALUE
Classification	PUBLIC: may be shared with anyone
Version	3.0
In effect from	12 November 2026
Latest version	grc.plus/security

© 2026 GRC+

Contents

1	We do not run a bug bounty	4
2	What we want to hear about	4
3	Systems in scope	5
4	Findings that do not need a report	5
5	How to report	6
6	Encrypting your report	7
7	Testing with care	7
8	What you can expect from us	7
9	Change history	8

© 2026 GRC+

Thank you for taking the time to look at our security. We work in security ourselves, so we take every real vulnerabilityA weakness, susceptibility or flaw that a threat can exploit. NIS2 applies it to ICT products and services, the CRA to products with digital elements and DORA to any asset, system, process or control. Coordinated vulnerability disclosure and handling duties build on this definition. in our systems seriously and fix it quickly. This page explains what we need from you, what you can expect from us, and which findings do not need a report. It follows the Dutch National Cyber Security Centre's guideline for coordinated vulnerability disclosureA process in which someone who discovers a security weakness reports it to the system owner or product supplier and works with them to address it. The parties coordinate investigation, a fix and the timing and content of any public disclosure, reducing the chance of exposing users before protection is available. A national cybersecurity centre may help coordinate when several parties are involved or contact fails.. Our contact details are also in security.txt.

1 We do not run a bug bounty

GRC+ does not pay for vulnerabilityA weakness, susceptibility or flaw that a threat can exploit. NIS2 applies it to ICT products and services, the CRA to products with digital elements and DORA to any asset, system, process or control. Coordinated vulnerability disclosure and handling duties build on this definition. reports, whatever the severity. That means no reward, no gift and no paid "hall of fame" entry. We say this up front so you can decide how to spend your time before you start.

A report that asks for payment, or that makes disclosure depend on payment, is not something we can take forward. If you are looking for paid research work, a bug bounty platform is a better place for it.

We are glad to say thank you in public: with your permission, we name you on this page once a serious issue you reported has been fixed.

2 What we want to hear about

VulnerabilitiesA weakness, susceptibility or flaw that a threat can exploit. NIS2 applies it to ICT products and services, the CRA to products with digital elements and DORA to any asset, system, process or control. Coordinated vulnerability disclosure and handling duties build on this definition. that you can show have a real impact on the confidentialityThe information-security property of keeping information from being disclosed to people, organisations or systems that are not authorised to receive it. Access restrictions and encryption help preserve confidentiality when information is stored, sent or processed. It concerns who can see information; it does not by itself ensure that the information is accurate or that a service remains available., integrity or availabilityThe information-security property that authorised people and systems can access and

© 2026 GRC+

use information or services when needed, reliably and within an acceptable time. An outage or an attack that overwhelms a service can reduce availability even if no information is stolen or changed. In product security, this includes keeping essential functions accessible and usable. of GRC+ systems or of the data we hold. For example:

- remote code execution, SQL injection or other injection that reaches data or the server;
- a way around login or permissions, including access to another user's data (IDOR);
- cross-site scripting that works against other users without unusual interaction;
- exposure of personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity., credentials, keys or confidential documents;
- server-side request forgery or path traversal that reaches internal resources;
- payment or subscription logic that gives access to paid services without paying.

3 Systems in scope

Systems run by GRC+: grc.plus and its subdomains, and GRC+ apps and integrations. Systems of our clients and of our providers, such as HubSpot, Microsoft, Stripe, Google or our hosting company, are not ours to fix: please report those to the provider. A third-party service on one of our subdomains stays the provider's responsibility.

4 Findings that do not need a report

Automated scanners flag many things that are not a risk for a site like ours, or that we have already decided to accept. To save you the effort, these findings do not qualify on their own. We do read every report, but we do not reply individually when a report only contains one of them:

- scanner or tool output without manual checking and a working proof of concept;
- missing or "weak" HTTP security headers, cookieA small text file that a website saves on a computer or mobile device. It lets the site remember information between pages or visits, such as a login, language choice or other preference. Cookies can support a site's functions or provide information about its use. The term identifies the storage technology; whether a particular cookie needs consent depends on its purpose and the law that applies. flags, CSP or HSTS settings;
- SPF, DKIM, DMARC, BIMI or other e-mail configuration advice;
- clickjacking on pages without a sensitive action, and tabnabbing;
- software or version disclosure, banner grabbing, directory listings without sensitive content,

© 2026 GRC+

descriptive error messages;
- CSRF on forms without a sensitive action, such as login, logout, contact or newsletter forms;
- self-XSS, and content or text injection without script execution;
- missing rate limits on public forms, or being able to send many form submissions;
- user enumeration through the login or password reset pages;
- public files and pages such as robots.txt, sitemap.xml, llms.txt, wp-json routes that list public content, or the reachable WordPress login page;
- SSL or TLSTransport Layer Security settings such as cipher suite order, without a practical attack;
- broken links, typos, and social media accounts or domains we do not own;
- attacks that need physical access, a compromised device or an outdated browser;
- denial of service, load testing, social engineeringAn attack approach that manipulates people into revealing sensitive information, granting unauthorised access or helping commit fraud. The attacker may build trust or pretend to be a legitimate contact so that a person shares a password or takes another harmful action. The weakness being exploited is human trust and behaviour, which can give the attacker access to systems or data., phishingAn attack that impersonates a trusted person or organisation through electronic communications, often an email or a fake website, to trick someone into revealing information such as passwords or bank details. The attacker uses apparent familiarity or credibility to persuade the person to respond. Training simulations practise recognising these deceptive requests. and spam.

If you believe one of these does have a real impact in our case, you are welcome to report it: show the impact with a working proof of concept and we will look at it properly.

5 How to report

The quickest way is the security report form on this page. It asks for what we need to reproduce the problem: the affected address or system, the type of vulnerabilityA weakness, susceptibility or flaw that a threat can exploit. NIS2 applies it to ICT products and services, the CRA to products with digital elements and DORA to any asset, system, process or control. Coordinated vulnerability disclosure and handling duties build on this definition., the impact, the steps and a proof of concept. You can also e-mail security@grc.plus; those reports go through the same review.

Please leave out any personal dataAny information relating to an identified or identifiable natural person, the data subject. A person is identifiable if they can be identified directly or indirectly, for example by a name, an identification number, location data, an online identifier or factors specific to their identity. you came across. You can write in English or Dutch, and you may report anonymously.

© 2026 GRC+

6 Encrypting your report

The report form on this page is sent over an encrypted connection, so most reports need nothing more. If you prefer to e-mail us, or your report contains sensitive details, you can encrypt it with our PGP key:

Key
: GRC+ Security <security@grc.plus>

Fingerprint
: B516 C076 76A0 4F3B 9487 D5FE 5746 A8DB 9AE6 BDAC

Valid until
: 12 November 2029

Download
: /.well-known/pgp-key.asc · keys.openpgp.org

Please send your own public key with an encrypted report, so we can reply in the same way.

7 Testing with care

- Do only what is needed to show the vulnerabilityA weakness, susceptibility or flaw that a threat can exploit. NIS2 applies it to ICT products and services, the CRA to products with digital elements and DORA to any asset, system, process or control. Coordinated vulnerability disclosure and handling duties build on this definition.. Please do not copy, change or delete data; if you reach personal or confidential data, stop and let us know.
- Keep automated tools at a gentle pace that does not affect the site, and do not run denial-of-service tests.
- Do not install anything, keep access open, or move on to other systems.
- Keep the details confidential until the issue is fixed, and agree the timing of any publication with us. We aim to fix serious issues within 90 days.
- Stay within the law: this policy cannot authorise anything that is illegal.

8 What you can expect from us

- We confirm receipt of an in-scope report within 3 business days and give a first assessment within 10 business days.
- We keep you informed until the issue is fixed, and tell you when it is.
- If you act in good faith and follow this policy, we will not take legal action against you or report

© 2026 GRC+

you to the police for your report.

- We treat your report and your personal details confidentially and do not share them without your permission, unless the law requires it.

9 Change history

VERSION	DATE	CHANGE
3.0	12 November 2026	Text revised; section on encrypting your report with our PGP key added.
2.2	5 May 2026	Security report form added.

Is this the latest version?
Scan the code or open grc.plus/security. Version 3.0 was in effect from 12 November 2026.

This PDF is saved as PDF/A-1b for archiving. © 2026 GRC+

END OF DOCUMENT