RESPONSIBLE DISCLOSURE

Responsible disclosure — how to report security issues

Version	1.1
Effective date	April 18, 2026
Last updated	April 18, 2026

Introduction

We take the security of our systems and those of our clients seriously. Despite our best efforts, vulnerabilities may exist. If you discover a security issue in our systems, websites or client environments that we manage, we would greatly appreciate you letting us know. This allows us to act quickly and protect our clients.

This policy applies to all systems, websites and online environments that fall under the responsibility of xYnta Hosting B.V. — including our own websites, our client portal and client environments hosted on our infrastructure.

Our responsible disclosure policy is based on the guidelines of the Dutch National Cyber Security Centre (NCSC) and the standard from responsibledisclosure.nl by Floor Terra, published under the Creative Commons Attribution 3.0 licence.

What falls within scope?

We welcome reports about vulnerabilities in:

- Our own websites and online environments (such as xynta.com, mijn.xynta.com, orbit.xynta.com, help.xynta.com and xyntastatus.com)
- Our internal systems and infrastructure, to the extent that these are accessible from the outside
- Client environments that we manage on our infrastructure

Vulnerabilities in third-party systems that we do not manage fall outside the scope of this policy. In those cases, please contact the relevant party directly.

What do we ask of you?

To allow us to handle your report safely and responsibly, we ask that you:

- **Report your finding as soon as possible** by emailing security@xynta.nl. Please encrypt your message using our PGP key to prevent sensitive information from falling into the wrong hands.
- **Do not exploit the vulnerability.** Do not download more data than is strictly necessary to demonstrate the issue. Do not view, modify or delete data belonging to third parties.
- **Do not share the vulnerability with others** until we have resolved the issue. Delete any confidential data obtained through the vulnerability as soon as the issue has been fixed.
- **Do not use attack techniques** that could compromise the availability or integrity of our systems, such as denial-of-service attacks, brute force, spam or social engineering.
- **Provide sufficient information** for us to reproduce and resolve the issue. In most cases, the IP address or URL of the affected system and a clear description of the vulnerability are sufficient. For more complex vulnerabilities, additional information may be required.
- **Act in good faith** and follow this procedure. Reporting under a pseudonym is permitted.

What can you expect from us?

- **We will respond within one business day** with an acknowledgement of receipt and an initial assessment.
- **We will resolve the issue as quickly as possible** and aim to do so within 90 days. If more time is needed, we will discuss this with you. We will keep you informed of progress throughout the process.
- **We will not take any legal or other action against you** if you act in good faith and follow the procedure set out in this policy. This also applies if you have inadvertently crossed a boundary that you could not reasonably have foreseen.
- **We will treat your report confidentially.** Your personal data will not be shared with third parties without your consent, unless we are legally required to do so.
- **We will credit you as the discoverer** in our hall of fame if you wish. If you prefer to remain anonymous, we will respect that.
- **We will involve you in any publication** about the vulnerability after it has been resolved, if you would like to be involved.

What falls outside this policy?

We do not process reports relating to:

- Already known vulnerabilities or issues that have previously been reported to us
- Vulnerabilities where the vulnerability has been actively exploited or where data belonging to third parties has been accessed, modified or copied beyond what was necessary for the report
- Theoretical vulnerabilities without a demonstrable practical risk
- Findings from automated scanning tools without manual verification
- Attacks on physical security, social engineering or xYnta employees

We reserve the right not to process reports that fall outside the scope of this policy or that do not meet its conditions.

How to report a vulnerability

Send your report to security@xynta.nl. Please encrypt your message using our PGP key. Include the following in your report:

- A clear description of the vulnerability
- The IP address, URL or system on which the vulnerability was found
- Steps to reproduce the issue
- Your contact details or pseudonym, so that we can reach you with any follow-up questions

We will confirm receipt of your report within one business day.

Contact

- **xYnta Hosting B.V.**
- Kapitein Luidingaflat 26
- 3333 CM Zwijndrecht
- The Netherlands
- Security email: security@xynta.nl
- General email: info@xynta.nl
- Phone: +31 85 400 6666
- Chamber of Commerce: 64691675

The current version of this document is always available at:
https://www.xynta.com/en/legal/responsible-disclosure
This PDF is a snapshot of version 1.1. Always verify you are reading the latest version.