



Responsible Disclosure Guidelines

Introduction

At Priva, we take the security of our applications, products, and services seriously, and we value the work of security researchers who help us protect our customers. This policy explains how to report a suspected security vulnerability to Priva, what you can expect from us in return, and the conditions under which we ask you to conduct your research. We are committed to working with researchers who report issues in good faith.

How to Report a Vulnerability

If you believe you have found a security vulnerability in a Priva-owned application, product, or service, please report it to us using the contact details published in our security.txt file, available at <https://www.priva.com/.well-known/security.txt>. Our security.txt lists the current security contact address, our PGP/encryption key for sending sensitive information securely, and our preferred language(s) for reports.

You can also reach our security team directly at isdg@priva.com. For sensitive details, please encrypt your report using the PGP key referenced in our security.txt.

Please allow us to investigate and remediate the issue (see *Coordinated Disclosure and Confidentiality*) by not disclosing the issue publicly until we have had the opportunity to do so.

What to Include in Your Report

To help us reproduce and investigate the issue quickly, please include:

- A description of the vulnerability and the affected application, product, URL, or component.
- The steps required to reproduce the issue, including any accounts, inputs, or preconditions.
- A proof of concept where possible (for example, a request/response, script, or screenshots).
- The potential impact of the vulnerability, as you understand it.
- The date, time, and time zone of your testing, and the IP address(es) you tested from.
- Your name or handle, and how you would like to be contacted and credited.



When Conducting Security Research

When conducting security research, please:

- Act in good faith.
- Avoid privacy violations.
- Do not access, modify, or delete customer data.
- Avoid actions that could impact the availability of production services.
- Limit testing to the minimum necessary to validate the issue.
- Provide sufficient information for us to reproduce and investigate the finding.
- Allow Priva a reasonable period to assess and remediate confirmed vulnerabilities before public disclosure.

Prohibited Activities

To keep testing safe for our customers, the following activities are **not** permitted under this policy:

- Accessing, modifying, deleting, or exfiltrating (personal) data that does not belong to you.
- Denial-of-service (DoS/DDoS), volumetric, or load testing, or any activity that degrades or interrupts our services.
- Social engineering, phishing, or physical attacks against Priva staff, customers, contractors, or facilities.
- Testing systems, products, or services that are not owned or operated by Priva.
- Automated scanning that generates excessive traffic or using a finding to pivot further into our environment.
- Publicly disclosing a vulnerability before Priva has confirmed it is resolved, unless otherwise agreed with us in writing.



What Happens After Submission?

- Our security team reviews every report.
- We may contact you for additional information.
- Valid vulnerabilities are assessed and prioritized based on risk.
- Confirmed vulnerabilities are addressed through our vulnerability management process.

Our Commitment and Response Targets

When you report a vulnerability in good faith and in line with this policy, you can expect the following from us:

- We will acknowledge receipt of your report within 2 business days.
- We will provide an initial assessment, including whether the report is in scope, within 5 business days.
- We will keep you informed of our progress at reasonable intervals and let you know when the issue is resolved.
- We will handle your report confidentially and share it only on a need-to-know basis.
- Remediation is prioritized based on risk; where relevant, we will agree on a coordinated disclosure date with you.

Coordinated Disclosure and Confidentiality

Priva follows a coordinated vulnerability disclosure (CVD) approach. Any vulnerability identified in or affecting Priva's systems, products, or services, including related technical details, evidence, or proof-of-concept material, must be treated as confidential.

You must not disclose, publish, communicate, or otherwise make any vulnerability or related information available to any third party or the public without Priva's prior written consent. This includes disclosure through websites, social media, security advisories, conferences, reports, or other channels.

Any disclosure must be coordinated with and expressly agreed upon by Priva in advance.

Legal Safe Harbor

Priva considers security research and vulnerability disclosure conducted in good faith and in accordance with this policy to be authorized activity. We will not pursue or support legal action against researchers who act in good faith, comply with this policy, avoid privacy violations, data destruction, and service disruption, and give us a reasonable opportunity to remediate before any disclosure. This policy does not authorize actions that violate applicable law, and it does not extend to the systems or data of Priva customers or third parties. If you are unsure whether a specific action is permitted, contact us first.



Recognition

Recognition and Compensation

We greatly appreciate the time, expertise, and effort that security researchers invest in identifying and responsibly reporting potential vulnerabilities in our systems.

Please note that we do not offer financial rewards, monetary compensation, or other forms of remuneration for vulnerability reports submitted under this Coordinated Vulnerability Disclosure (CVD) policy.

Nevertheless, we recognize the value and contribution it makes to improving the security and resilience of our assets and we appreciate your effort in helping us keep our customers safe.

Systems and Assets in Scope

This policy applies to Priva-owned applications and is not limited to products, and services. Systems, domains, and products not listed here, or operated by third parties on Priva's behalf, are out of scope unless we confirm otherwise in writing.

To provide transparency, the systems and applications that are End Of Life are identified and made visible through the applicable Priva customer and partner portals. This enables customers and partners to clearly distinguish between systems and applications that are covered by this policy and those that are explicitly excluded from its scope.

In Scope

We welcome reports of security vulnerabilities affecting Priva-owned applications, products, and services, including:

- Authentication and authorization vulnerabilities
- Privilege escalation vulnerabilities
- Injection vulnerabilities (e.g., SQL injection)
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Security misconfigurations within Priva applications
- Sensitive data exposure caused by application vulnerabilities
- Business logic vulnerabilities that create a security risk
- Other vulnerabilities that significantly compromise the confidentiality, integrity, or availability of our applications or customer data



Out of Scope

The following are generally not considered valid vulnerability reports under this process:

- TLS/SSL observations without a demonstrable security impact
- Publicly exposed security parameters, HTTP headers, certificates, or service banners
- Security characteristics, limitations, or findings that are inherent to Microsoft Azure or other third-party cloud providers
- Functional defects, usability issues, feature requests, or product enhancements
- Configuration recommendations, hardening suggestions, or tweaks that do not introduce a security risk
- Reports generated solely by automated vulnerability scanners without evidence of an exploitable issue
- Vulnerabilities affecting third-party products or services not owned or operated by Priva
- Clickjacking findings on pages that do not process sensitive information or authenticated actions.
- Missing SPF, DKIM, or DMARC records where email security is managed through approved third-party services.
- Search engine indexing of publicly available content.
- Self-XSS that cannot be used to attack another user (*added*)
- Missing security headers or cookie flags without a demonstrated, exploitable impact (*added*)
- Rate-limiting or brute-force concerns on endpoints without a proven security impact (*added*)
- Content spoofing or text injection without a demonstrated attack vector (*added*)
- Reports of outdated software versions without a demonstrated, exploitable vulnerability (*added*)

For functional issues, product feedback, or enhancement requests, please use the appropriate support or feedback channels.



Eligibility

To participate in responsible disclosure with Priva, please note:

- You must be legally permitted to conduct security research in your jurisdiction and in the Netherlands.
- Priva employees, contractors, partners, and their immediate family members, are not eligible for recognition under this policy.
- You must always comply with all applicable laws and with this policy.

Policy Governance

- **Version:** 1.0
- **Effective date:** September 2026
- **Last updated:** September 2026
- **Owner:** Information Security & Data Governance
- **Review cycle:** upon significant change
- **Contact:** as published in our security.txt (<https://www.priva.com/.well-known/security.txt>)

Priva may update this policy at any time. The current version always takes precedence.