Reponsible Disclosure Policy

1. Purpose & Scope

This policy defines how security researchers, partners, and any other parties may responsibly disclose security-related findings that affect the public website **https://dataown.nl**. It outlines the expectations for both the reporter and DataOwn, ensuring that vulnerabilities are handled safely, transparently, and in compliance with applicable law.

---

2. What We Accept

Category	Description
Web-application flaws	XSS, CSRF, SQL/NoSQL injection, authentication bypass, insecure direct object references, broken access control, information leakage, misconfigurations, etc.
Infrastructure issues	Open ports, exposed services, insecure TLS/SSL configurations, server-side request forgery (SSRF), DNS hijacking, etc.
Third-party component problems	Vulnerabilities in libraries, frameworks, or services that are part of the public site.
Other security-relevant observations	Any finding that could realistically be leveraged to compromise confidentiality, integrity, or availability of the site or its users.

We **do not accept**:

- Requests for voluntary penetration testing or security assessments that are not tied to a specific, reproducible vulnerability.
- Reports that contain malicious code, exploit scripts, or instructions intended for weaponisation.

---

3. How to Submit a Report

1. **Email** – Send a concise, plain-text description to **security@dataown.nl**.
2. **Subject line** – Use the format: Vulnerability Disclosure – <Brief Title> (e.g., “Vulnerability Disclosure – Reflected XSS on login page”).
3. **Content** – Include the following sections:
    - **Summary** – One-sentence overview of the issue.
    - **Affected URL(s) / endpoint(s)** – Exact location(s) where the problem occurs.
    - **Impact** – What an attacker could achieve (e.g., steal session cookies, execute arbitrary code).
    - **Steps to Reproduce** – Clear, numbered steps that allow us to verify the flaw.
    - **Proof-of-Concept (PoC)** – Minimal, non-malicious example (e.g., a curl command or a sanitized HTML snippet).
    - **Suggested Mitigation** (optional) – Your recommendation for fixing the issue.
4. **Attachments** – If you need to provide screenshots or logs, compress them into a password-protected ZIP file. Send the password in a separate email or via a secure messaging channel (e.g., Signal).
5. **Confidentiality** – Do **not** disclose the vulnerability publicly, on social media, or to third parties before DataOwn has had a reasonable chance to remediate it.

4. What Happens After Submission

Phase	Timeline	Details
Acknowledgement	≤ 2 business days	We confirm receipt of your email and assign a reference number.
Initial Triage	≤ 5 business days	Security team evaluates severity, reproducibility, and scope.
Investigation & Fix	Variable (typically 7–30 days)	Depending on complexity, we develop and test a fix. We will keep you informed of progress (no more than one update per week unless a critical change occurs).
Resolution Notification	Within 5 business days after fix deployment	You receive a summary of the remediation and, if applicable, a reference to the public advisory.
Public Disclosure	At DataOwn's discretion (usually after fix is live)	We may publish a security advisory on our website. If you wish to be credited, let us know; anonymity is respected.

All timelines are best-effort estimates; exceptionally complex issues may require longer periods.

5. Safe Harbor

By submitting a report in accordance with this policy, you agree to:

- Act in good faith and refrain from any activity that exceeds the scope of the disclosed vulnerability.
- Not exploit, sell, or otherwise misuse the information.
- Comply with all applicable laws and regulations.

In return, DataOwn commits to:

- Not initiate legal action against you for good-faith disclosures made under this policy.
- Protect any personally identifying information you provide, handling it in line with our privacy policy.

6. What We Do **Not** Offer

- **Bug bounty payments** – We do not operate a monetary reward program.
- **Acceptance of unsolicited penetration testing** – We will not authorize or engage in ad-hoc testing that is not linked to a specific vulnerability report.

If you are interested in a formal engagement (e.g., a penetration test), please contact our sales team to discuss a scoped, paid assessment.

7. Contact Information

Primary point of contact: Gert Jan – Security OfficerE-mail: security@dataown.nl

8. Policy Updates

We may revise this policy as needed. Changes will be posted on the **DataOwn Security** page (https://dataown.nl/security) with a revised effective date. Continued use of the disclosure channel after modifications constitutes acceptance of the updated terms.

Thank you for helping us keep DataOwn secure. — *The DataOwn Security Team*