Responsible Disclosure Beleid NOS

Versie 2.0 | Bijgewerkt: mei 2026

ENGLISH VERSION ON PAGE 10

Inhoud

Introductie

Bij de NOS vinden wij de veiligheid van onze systemen en de bescherming van onze journalistieke informatiebronnen van het hoogste belang. Als publieke omroep en primaire informatiebron voor Nederland dragen wij een bijzondere verantwoordelijkheid voor de digitale veiligheid van onze platforms en de bescherming van persvrijheid.
Ondanks onze uitgebreide beveiligingsmaatregelen kan het voorkomen dat er een kwetsbaarheid in onze systemen aanwezig is. Wij waarderen het enorm wanneer beveiligingsonderzoekers ons helpen om deze te identificeren en op te lossen. Dit beleid beschrijft hoe wij samenwerken met de security research community volgens de principes van Coordinated Vulnerability Disclosure (CVD).

Scope: Wat mag en mag niet

In scope

De volgende systemen en diensten vallen binnen de scope van dit beleid:

- Alle publiek toegankelijke webapplicaties en API's op *.nos.nl domeinen
- Mobiele applicaties van de NOS (iOS en Android)
- Publiek toegankelijke netwerk services van de NOS
- AI-gedreven systemen en functionaliteiten die door de NOS aangeboden worden, inclusief:
    - Prompt injection kwetsbaarheden in AI-assistenten
    - Content moderatie en aanbevelingssystemen
    - Geautomatiseerde nieuws aggregatie tools

Expliciet buiten scope

De volgende activiteiten en systemen zijn **niet toegestaan** en vallen buiten de bescherming van dit beleid:
Verboden testmethoden:

- Denial of Service (DoS/DDoS) aanvallen
- Fysieke security testing van gebouwen of apparatuur
- Social engineering (phishing, vishing, pretexting) richting medewerkers en/of leveranciers
- Brute force aanvallen op authenticatie
- Grootschalig geautomatiseerd scannen zonder voorafgaande coördinatie
- Het uitvoeren van acties die de beschikbaarheid beïnvloeden
- Het plaatsen van malware, virussen, ransomware of andere schadelijke code
- Het kopiëren, wijzigen of van productiedata
- Het delen van toegang met andere partijen

- Het verkopen van kwetsbaarheden aan derden
- Het openbaar maken van kwetsbaarheden voor coördinatie met ons
- Chantagepogingen of eisen stellen aan de NOS

Systemen buiten scope:

- Persoonlijke apparaten van medewerkers
- Interne netwerken zonder expliciete toestemming
- Systemen van derde partijen of leveranciers
- Test- en development omgevingen (tenzij expliciet aangegeven)

Overtredingen van deze regels kunnen leiden tot:

- Uitsluiting van het programma
- Inhouden van rewards
- Intrekking van juridische bescherming
- Mogelijke juridische vervolgstappen

Kwetsbaarheden in systemen van leveranciers

Ontdek je een kwetsbaarheid in een systeem van één van onze leveranciers of software partners? Meld deze dan rechtstreeks bij de betreffende partij volgens hun eigen disclosure beleid. Wij kunnen je helpen het juiste contactpunt te vinden. Stuur hiervoor een e-mail naar informatiebeveiliging@nos.nl met het onderwerp “Leverancier kwetsbaarheid”.

Juridische bescherming

De NOS biedt volledige bescherming aan beveiligingsonderzoekers die te goeder trouw handelen volgens dit beleid.

Wat wij beloven

Juridische immuniteit:

- Indien je voldoet aan dit beleid, beschouwen wij jouw onderzoek als geautoriseerde activiteit onder het Nederlandse strafrecht (Artikel 138ab Sr)
- De NOS onderneemt geen civiele of strafrechtelijke stappen tegen jou
- De NOS doet geen aangifte bij justitie of andere autoriteiten

Bescherming van jouw identiteit:

- Jouw persoonlijke gegevens worden vertrouwelijk behandeld
- Wij delen geen identificerende informatie met derden zonder uw uitdrukkelijke schriftelijke toestemming
- Dit geldt ook voor leveranciers, partners, of andere betrokken partijen
- Je hebt het recht om anoniem te blijven in alle communicatie en eventuele publicaties

Derde partijen notificatie:

- Als jouw melding betrekking heeft op systemen van derden, informeren wij deze partijen dat jouw onderzoek geautoriseerd was door de NOS
- Wij delen relevante technische informatie met betrokken partijen, maar nooit jouw identificerende gegevens zonder toestemming

Te goeder trouw handelen

Je handelt te goeder trouw wanneer je:

- Dit beleid in al zijn onderdelen naleeft
- Toegang tot systemen direct beëindigt na het aantonen van een kwetsbaarheid
- Geen gegevens kopieert, wijzigt of verwijdert (tenzij strikt noodzakelijk voor het aantonen van de kwetsbaarheid)
- Geen kwetsbaarheden exploiteert voor persoonlijk gewin of om anderen schade toe te brengen
- De kwetsbaarheid vertrouwelijk houdt totdat wij gezamenlijk tot publicatie overgaan
- Ons voldoende tijd geeft om het probleem op te lossen (zie termijnen)

Hoe te melden

Je kunt een beveiligingskwetsbaarheid op de volgende manieren melden:

Primaire kanalen:

- E-mail: informatiebeveiliging@nos.nl
- Security.txt: https://nos.nl/.well-known/security.txt

Versleutelde communicatie:

Voor gevoelige informatie kun je onze PGP-sleutel gebruiken

- PGP public key: te vinden op https://pgp.surfnet.nl

Talen:

- Meldingen kunnen in het Nederlands of Engels worden ingediend
- Onze communicatie gebeurt standaard in het Nederlands, maar Engels is mogelijk op verzoek

Vereiste informatie

Voor een effectieve behandeling van jouw melding hebben wij de volgende informatie nodig:
Minimaal vereist:

- Beschrijving van de kwetsbaarheid en het potentiële impact
- Stappen om de kwetsbaarheid te reproduceren
- URL, IP-adres, of systeemidentificatie waar de kwetsbaarheid zich bevindt

Optioneel maar waardevol:

- Proof of Concept (PoC) code of screenshots
- Suggesties voor een oplossing
- CVSS score inschatting (wij gebruiken CVSS v4.0)
- Informatie over mogelijke exploitatie in het wild

Jouw contactgegevens (optioneel):

- Voor reward programma: naam, email- en postadres
- Anonieme meldingen zijn mogelijk, je hoeft geen identificerende informatie te verstrekken

Wat gebeurt er na jouw melding?

Zodra wij jouw melding ontvangen:

1. Ontvangstbevestiging binnen 5 werkdagen
2. Initiële beoordeling binnen 10 werkdagen
3. Volledige triage en severity classificatie binnen 14 dagen
4. Reguliere updates over de voortgang van oplossing
5. Gezamenlijke beslissing over publicatie timing

Onze commitments: Tijdlijnen en transparantie

Responstijden

De NOS committeert zich aan de volgende Service Level Agreements:

- Ontvangstbevestiging: 5 werkdagen
- Initiële beoordeling: 10 werkdagen
- Triage en severity bepaling: 14 dagen
- Status updates: Minimaal elke 30 dagen

Oplostermijnen per klasse

Wij hanteren de volgende termijnen voor het oplossen van kwetsbaarheden:

- Kritiek: 7 dagen, bijvoorbeeld actieve exploitatie, RCE zonder authenticatie, complete systeemcompromise
- Hoog: 30 dagen, bijvoorbeeld privilege escalation, SQL injection met data toegang, XSS in admin panel
- Midden: 60 dagen, bijvoorbeeld XSS in publieke pagina's, information disclosure, CSRF
- Laag: 90 dagen, bijvoorbeeld minor information leakage, best practice verbeteringen

Actief geëxploiteerde kwetsbaarheden worden binnen 24-48 uur geadresseerd, conform NIS2 incidentmeldingsplicht.

Gecoördineerde Disclosure

Wij volgen het 90+30 disclosure model voor gecoördineerde publicatie:

- 90 dagen voor de ontwikkeling en uitrol van patches
- +30 dagen na patch release voor volledige technische details
- 7 dagen na melding: publieke aankondiging dat een kwetsbaarheid is gemeld (zonder technische details)

Versnelde disclosure

- Bij actieve exploitatie: 7 dagen (tenzij er nog geen patch beschikbaar is)
- Bij meerdere getroffen organisaties: coördinatie via NCSC

Melding bij het NCSC

Indien van toepassing melden wij nog niet bekende kwetsbaarheden bij het NCSC. Met jouw toestemming delen we jouw contactgevens met het NCSC.

Rewards en Erkenning

Collector's Item T-Shirt

Als dank voor jouw bijdrage aan de veiligheid van de NOS bieden wij een exclusief t-shirt aan. Deze t-shirts zijn speciaal ontworpen voor security researchers en zijn niet publiekelijk verkrijgbaar. Ze zijn bedoeld als collector's items die je met trots kunt dragen op cybersecurity conferenties.

Voorwaarden:

- Het moet gaan om een door ons geverifieerde kwetsbaarheid
- De kwetsbaarheid moet onbekend zijn bij de NOS (geen duplicaat)
- Minimaal severity rating: Medium (CVSS ≥ 4.0)
- Jouw contactgegevens (minimaal naam en postadres) moeten bekend zijn voor verzending

Limited Edition:

- Unieke designs per jaar

Privacy en Gegevensbescherming

AVG Compliance

De NOS verwerkt jouw persoonsgegevens conform de Algemene Verordening Gegevensbescherming.
Welke gegevens verwerken wij:

- Contactgegevens die je verstrekt (naam, e-mail, adres)

- Technische gegevens over de melding (IP-adressen, logs, PoC code)
- Communicatie geschiedenis tussen jou en de NOS

Rechtsgrond verwerking:
- Gerechtvaardigd belang voor het onderzoeken en verhelpen van kwetsbaarheden

Bewaartermijn:
- Meldingsgegevens: 2 jaar na oplossing van de kwetsbaarheid
- Communicatie: 1 jaar

Jouw rechten:
- Inzage in uw gegevens
- Rectificatie van onjuiste gegevens
- Verwijdering (recht op vergetelheid)
- Beperking van verwerking
- Bezwaar tegen verwerking
- Dataportabiliteit

Neem contact op met onze Functionaris Gegevensbescherming via privacy@nos.nl voor uitoefening van deze rechten.

Gegevens tijdens security testing

Wat je niet mag doen:
- Persoonlijke gegevens van gebruikers bekijken, kopiëren of verwerken
- Toegang krijgen tot communicatie of content van derden
- Persoonsgegevens bewaren na het aantonen van de kwetsbaarheid

Wat te doen bij onbedoelde toegang tot data:
- Stop onmiddellijk met verdere acties
- Documenteer alleen de methode, niet de inhoud
- Meld de situatie direct aan ons
- Verwijder alle lokale kopieën van gegevens

Speciale Scenario's

AI en Machine Learning Kwetsbaarheden

Voor kwetsbaarheden in AI-systemen hanteren wij dezelfde principes, maar met additionele overwegingen:
Prompt injection en jailbreaks:
- Documenteer de prompt die tot ongewenst gedrag leidt
- Beschrijf de potentiële impact (data extractie, instructie override, etc.)
- Test niet verder dan nodig voor demonstratie

Model manipulation:

- Poisoning attacks, adversarial inputs, en model extraction vallen binnen scope
- Grootschalige aanvallen op training data zijn niet toegestaan

Supply Chain en Third Party Components

Kwetsbaarheden in open-source libraries:

- Controleer eerst of de kwetsbaarheid al bekend is (CVE, GitHub Security Advisories)
- Als deze al upstream gemeld is, meld dan alleen de aanwezigheid bij NOS
- Nieuwe zero-days in dependencies: meld eerst bij maintainer, dan bij ons

SaaS Platform van derden:

- Configuratiefouten in onze implementatie: binnen scope
- Kwetsbaarheden in het SaaS platform zelf: meld bij de leverancier

Gevoelige Kwetsbaarheden

Voor kwetsbaarheden die bijzonder gevoelig zijn (journalistieke bronnen, intern communicatiesystemen):

- Gebruik verplicht PGP encryptie
- Neem telefonisch contact op voor escalatie: +31 (0)35 677 9222 (Front Office)
- Verstrek minimale details in initiële melding
- Wacht op een beveiligd communicatie kanaal voor volledige details

Vragen en Contact

Voor vragen over dit Responsible Disclosure beleid:
E-mail: informatiebeveiliging@nos.nl
Voor urgente security incidenten:

- 24/7 Hotline: +31 (0)35 677 9222 (Front Office)

Functionaris Gegevensbescherming:

- E-mail: privacy@nos.nl

Feedback op dit beleid

Heeft u suggesties voor verbetering van dit beleid? Wij staan open voor feedback van de security research community. Stuur uw suggesties naar informatiebeveiliging@nos.nl

Responsible Disclosure Policy

Nederlandse Omroep Stichting (NOS)

1. Introduction

At the NOS, the security of our systems and the protection of our journalistic sources are of the highest priority. As the Netherlands' primary public broadcaster and principal source of news, we have a special responsibility for the digital security of our platforms and the protection of press freedom.

Despite our extensive security measures, vulnerabilities may still arise. We greatly value the work of security researchers who help us identify and remediate these issues. This policy describes how we work with the security research community in accordance with the principles of Coordinated Vulnerability Disclosure (CVD).

2. Scope

In scope

The following systems and services are covered by this policy:

- All publicly accessible web applications and APIs on *.nos.nl domains
- NOS mobile applications (iOS and Android)
- Publicly accessible network services operated by NOS
- AI-driven systems and features offered by NOS, including:
  - Prompt injection vulnerabilities in AI assistants
  - Content moderation and recommendation systems
  - Automated news aggregation tools

Out of scope

The following activities and systems are not permitted and fall outside the protections of this policy:

Prohibited testing methods

- Denial of Service (DoS/DDoS) attacks
- Physical security testing of buildings or equipment
- Social engineering (phishing, vishing, pretexting) targeting employees or suppliers

- Brute force attacks against authentication mechanisms
- Large-scale automated scanning without prior coordination
- Actions that affect system availability
- Deploying malware, viruses, ransomware, or other harmful code
- Copying, modifying, or deleting production data
- Sharing access with third parties
- Selling vulnerabilities to third parties
- Publicly disclosing vulnerabilities before coordinating with us
- Any form of extortion or making demands of NOS

Systems out of scope

- Personal devices of employees
- Internal networks without explicit permission
- Systems belonging to third parties or suppliers
- Test and development environments (unless explicitly stated otherwise)

> *Violations of these rules may result in exclusion from the programme, withholding of rewards, revocation of legal protections, and potential legal action.*

Vulnerabilities in supplier systems

If you discover a vulnerability in a system belonging to one of our suppliers or software partners, please report it directly to that party according to their own disclosure policy. We can help you find the appropriate contact. Send an email to informatiebeveiliging@nos.nl with the subject line "Supplier vulnerability".

3. Legal Protection

NOS provides full protection to security researchers who act in good faith in accordance with this policy.

Our commitments

Legal immunity

- If you comply with this policy, we consider your research to be an authorised activity under Dutch criminal law (Article 138ab Sr)
- NOS will not take civil or criminal action against you
- NOS will not file a complaint with law enforcement or other authorities

Protection of your identity

- Your personal data will be treated in strict confidence
- We will not share identifying information with third parties without your explicit written consent
- This applies to suppliers, partners, and all other involved parties
- You have the right to remain anonymous in all communications and any publications

Third-party notification

- If your report relates to third-party systems, we will inform those parties that your research was authorised by NOS
- We will share relevant technical information with involved parties, but never your identifying details without your consent

Acting in good faith

You are acting in good faith when you:

- Comply with all provisions of this policy
- Terminate access to systems immediately after demonstrating a vulnerability
- Do not copy, modify, or delete data (unless strictly necessary to demonstrate the vulnerability)
- Do not exploit vulnerabilities for personal gain or to harm others
- Keep the vulnerability confidential until we jointly agree on publication
- Allow us sufficient time to remediate the issue (see timelines)

4. How to Report

Reporting channels

Primary channels

- **Email:** informatiebeveiliging@nos.nl
- **Security.txt:** https://nos.nl/.well-known/security.txt

Encrypted communication

For sensitive information, you may use our PGP key. The PGP public key is available at https://pgp.surfnet.nl.

Languages

- Reports may be submitted in Dutch or English
- Our default response language is Dutch; English is available on request

Required information

Minimum required

- Description of the vulnerability and its potential impact
- Steps to reproduce the vulnerability
- URL, IP address, or system identifier where the vulnerability exists

Optional but valuable

- Proof of Concept (PoC) code or screenshots
- Suggested remediation
- CVSS score estimate (we use CVSS v4.0)
- Information on known active exploitation

Your contact details (optional)

- For the reward program: name, email address, and postal address
- Anonymous reports are accepted — you are not required to provide identifying information

What happens after your report?

Once we receive your report, you can expect:

- Acknowledgement of receipt: within 5 business days
- Initial assessment: within 10 business days
- Full triage and severity classification: within 14 days
- Regular progress updates throughout remediation
- A joint decision on publication timing

5. Response Timelines & Transparency

Service Level Agreements

Metric	Commitment
Acknowledgement	Within 5 business days
Initial assessment	Within 10 business days
Triage & severity	Within 14 calendar days
Status updates	At minimum every 30 days

Remediation deadlines by severity class

Severity	Deadline	Examples
Critical	7 days	Active exploitation, unauthenticated RCE, complete system compromise
High	30 days	Privilege escalation, SQL injection with data access, admin panel XSS
Medium	60 days	XSS on public pages, information disclosure, CSRF
Low	90 days	Minor information leakage, best-practice improvements

Coordinated Disclosure

NOS follows the 90+30 disclosure model for coordinated publication:

- 90 days for the development and rollout of patches
- +30 days after patch release before full technical details are disclosed
- 7 days after initial report: public announcement that a vulnerability has been reported (without technical details)

Accelerated disclosure

- In case of active exploitation: 7 days (unless no patch is yet available)
- Where multiple organizations are affected: coordination via NCSC-NL

NCSC notification

Where applicable, NOS will report previously unknown vulnerabilities to the NCSC-NL. With your consent, we may share your contact details with the NCSC-NL.

6. Rewards & Recognition

Collector's Item T-Shirt

As a token of appreciation for your contribution to the NOS security, we offer an exclusive t-shirt. These shirts are specially designed for security researchers and are not available to the general public — they are intended as collector's items to wear proudly at cybersecurity conferences.

Eligibility criteria

- The vulnerability must be verified by the NOS
- The vulnerability must be previously unknown to the NOS (no duplicates)
- Minimum severity rating: Medium (CVSS ≥ 4.0)
- Your contact details (at minimum name and postal address) must be provided for shipping

Limited editions

- Unique designs released annually

7. Privacy & Data Protection

GDPR compliance

The NOS processes your personal data in accordance with the General Data Protection Regulation (GDPR).

Data we process

- Contact details you provide (name, email, address)
- Technical details related to the report (IP addresses, logs, PoC code)
- Communication history between you and NOS

Legal basis for processing

- Legitimate interest in investigating and remediating security vulnerabilities

Retention periods

- Report data: 2 years after the vulnerability is resolved
- Communications: 1 year

Your rights

Under the GDPR, you have the right to:

- Access your personal data
- Rectification of inaccurate data
- Erasure (right to be forgotten)
- Restriction of processing
- Object to processing
- Data portability

To exercise these rights, contact our Data Protection Officer at privacy@nos.nl.

Data during security testing

What you must not do

- View, copy, or process personal data of users
- Access communications or content belonging to third parties
- Retain personal data after demonstrating the vulnerability

If you inadvertently access data

- Stop all further actions immediately
- Document only the method, not the content
- Report the situation to us without delay
- Delete all local copies of the data

8. Special Scenarios

AI and Machine Learning vulnerabilities

For vulnerabilities in AI systems, we apply the same principles with the following additional considerations:

Prompt injection and jailbreaks

- Document the prompt that produces unintended behaviour
- Describe the potential impact (data extraction, instruction override, etc.)
- Do not test beyond what is necessary for demonstration purposes

Model manipulation

- Poisoning attacks, adversarial inputs, and model extraction fall within scope
- Large-scale attacks on training data are not permitted

Supply chain and third-party components

Open-source library vulnerabilities

- First check whether the vulnerability is already known (CVE, GitHub Security Advisories)

- If it has already been reported upstream, only notify the NOS of its presence in our systems
- New zero-days in dependencies: report to the maintainer first, then notify us

Third-party SaaS platforms

- Configuration errors in our implementation: within scope
- Vulnerabilities in the SaaS platform itself: report directly to the vendor

Sensitive vulnerabilities

For vulnerabilities that are particularly sensitive in nature (e.g. affecting journalistic sources or internal communications systems):

- PGP encryption is mandatory
- Contact us by telephone for escalation: +31 (0)35 677 9222 (Front Office)
- Provide only minimal details in the initial report
- Await a secure communication channel before sharing full details

9. Contact

Security team	informatiebeveiliging@nos.nl
24/7 hotline	+31 (0)35 677 9222 (Front Office)
Data Protection Officer	privacy@nos.nl
Security.txt	https://nos.nl/.well-known/security.txt

Feedback on this policy

We welcome suggestions for improving this policy from the security research community. Please send your feedback to informatiebeveiliging@nos.nl.