Security contact and bug bounty

How to responsibly report a vulnerability in USDN.

VERSION	LAST UPDATED	STATUS
0.1	November 17, 2026	Draft

1. Report a vulnerability

If you believe you have found a security issue in the USDN contracts, the website or related systems, please tell us privately before sharing it publicly. Send your report to [security contact email], encrypted with [PGP key link] if possible.

Include a clear description, steps to reproduce, the affected address or URL, and the potential impact. A proof of concept is helpful but not required.

2. What to expect

Stage	Target
Acknowledgement of your report	[for example, within 2 business days]
Initial assessment	[for example, within 7 days]
Fix and disclosure plan	Agreed with you based on severity

3. Scope

- In scope: the USDN token contract on every official network, and neosmartchain.com.
- Out of scope: social engineering, physical attacks, denial of service, third-party services and issues already reported.

4. Rewards

Severity	Reward
Critical	[amount]
High	[amount]
Medium	[amount]
Low	[amount]

Rewards are decided by the security team based on impact and report quality. Bounty status: [active or planned].

5. Safe harbour

We will not take legal action against researchers who act in good faith: avoid accessing other people data, do not disrupt services, test only with your own funds and accounts, and give us reasonable time to fix the issue before disclosure.

This document is for information only and is not financial, legal or tax advice. Highlighted items in square brackets are still to be confirmed by the issuer. The latest version is always available at neosmartchain.com/tokens/usdn/docs/bounty