COORDINATED VULNERABILITY DISCLOSURE (CVD) POLICY

Document: P-001

Version: 1

NYRSTAR GROUP POLICY

Contents

Revision History

Cover page, header and footer information and control			
Document title	Coordinated Vulnerability Disclosure (CVD) Policy		
Document number	P-001		
Latest publish date	3/09/2024	Latest version number	1
Version history			

Author/reviewer	Position	Version	Concept	Date approved NMC
Ashmeet Kaur	Group Manager Information Security	001		DocuSigned by: Ashmeet Kaur EE37A55D7488485...
Rob Geraats	Legal Counsel	001		Signed by: Rob Geraats 00CECA2EBE5243B...
Hans Lauwers	Global Head of IT/OT	001		DocuSigned by: 2FAC09D4172F4E4...

1. Introduction

Nyrstar recognizes the importance of cybersecurity in protecting the network and information systems that are essential for the provision of our services. In order to improve the performance and security of our networks and information systems, we have adopted a Coordinated Vulnerability Disclosure (CVD) policy. This policy provides guidelines for the responsible reporting and management of vulnerabilities to ensure the protection of our systems and data.

2. Scope

This policy applies to any individual or organization that discovers a security vulnerability affecting Nyrstar's information systems, services, or networks, which may impact the continuity and security of services offered by Nyrstar.

3. Policy

3.1 Mutual Obligations of the parties

3.1.1 Proportionality

The participant undertakes to comply strictly with the principle of proportionality in all their activities, i.e. not to disrupt the availability of the services provided by the system and not to make use of the vulnerability beyond what is strictly necessary to demonstrate the security flaw. Their approach must remain proportionate: if the safety problem has been demonstrated on a small scale, no further action should be taken.

3.1.2 Actions that are not allowed

Participants are not permitted to take the following actions:

- copying or altering data from the IT system or deleting data from that system;
- changing the IT system parameters;
- installing malware: viruses, worms, Trojan horses, etc.;
- Distributed Denial of Service (DDOS) attacks;
- social engineering attacks;
- phishing attacks;
- spamming;
- stealing passwords or brute force attacks;
- installing a device to intercept, store or learn of (electronic) communications that are not accessible to the public;
- the intentional interception, storage or receipt of communications not accessible to the public or of electronic communications;
- the deliberate use, maintenance, communication or distribution of the content of non-public communications or of data from an IT system where the participant should reasonably have known it had been obtained unlawfully.

3.1.3 Confidentiality

The participant must strictly refrain from sharing or disclosing any information collected under our policy with third parties without our prior and explicit consent.

Similarly, it is not permitted to reveal or disclose computer data, communication data or personal data to third parties. Information about vulnerabilities, their status, and remediation efforts will be disclosed only to necessary parties.

3.1.4 Safe Harbor

In line with the NIS2 Directive's focus on security and resilience, Nyrstar will not engage in legal action against individuals who adhere to this policy and report vulnerabilities responsibly. The participant must be free of fraudulent intent, intent to harm, intent to use or intent to cause damage to the visited system or its data.

3.1.5. Processing of Personal Data

The purpose of a CVDP is not to intentionally process personal data, but it is possible that the participant may have to process personal data, even incidentally, in the course of his or her vulnerability research.

The processing of personal data is broad in scope and includes the storage, alteration, retrieval, consultation, use or disclosure of any information that could relate to an identified or identifiable natural person.

In the event of processing such data, the participant undertakes to comply with the legal obligations regarding the protection of personal data and the terms of this policy, in particular:

- The participant undertakes to process personal data only in accordance with the instructions of Nyrstar, as described in this policy, and exclusively for the purpose of investigating vulnerabilities in the systems, equipment or products of our organisation. Any processing of personal data for any other purpose is excluded.
- The participant undertakes to limit the processing of personal data to what is necessary for the purpose of vulnerability scanning.
- The participant shall ensure that the persons authorised to process personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality.
- The participant shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (e.g. encryption).
- The participant may not keep any personal data processed for longer than necessary. During this period, the participant must ensure that this data is stored with a level of security appropriate to the risks involved (preferably encrypted). At the end of his/her participation in the policy, this data must be deleted immediately.

3.2. Reporting a Vulnerability

Report a vulnerability responsibly by contacting us at security@nyrstar.com with an encrypted message providing the following details:

- A detailed description of the observed vulnerability.
- The steps required to reproduce the vulnerability (Proof of Concept scripts or screenshots are welcome).
- Any technical information that may be relevant to understanding the vulnerability.

Public disclosure of the vulnerability is discouraged until it has been addressed and explicit permission has been granted by Nyrstar.

3.4. Acknowledgments

We value contributions from security researchers and will acknowledge those who report vulnerabilities following the resolution, unless anonymity is requested.

3.5. Response and Remediation

Following a vulnerability report, Nyrstar's information security team will:

- Confirm receipt within 72 hours
- Validate and assess the vulnerability
- Prioritize and address the vulnerability
- Provide status updates to the reporter
- Inform the reporter when the vulnerability is resolved

4. Additional information

Nyrstar will conduct an annual review of this policy to ensure it remains aligned with evolving cybersecurity challenges and new regulatory requirements.

5. Contact Information

For questions about this policy or to report a vulnerability, please contact security@nyrstar.com