NC& Co., Ltd

Vulnerability Disclosure Policy

Notice:

Information contained in this document is classified NC& Co., Ltd Confidential Proprietary. No person outside the NC& Co., Ltd shall have access to the information contained in this document unless business needs dictate, otherwise. It is the responsibility of the person knowing the information contained in this document to ensure confidentiality of information contained in it and securing unauthorized access to this document at all times.

About This Document

Document Information

Issuing authority	NC& Co., Ltd
Address	5FL, Uspace1 A, 660 Daewangpangyo-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea 13494
Configuration ID	NC&_VDP_AU

Revision History

Version	Date	Comment	Author	Approver
0.1	01-05-2026	Initial Policy Establishment	Jang, Jin-Soo	Jung Chan Lee

Table of Contents

1 Introduction

1.1 Purpose

NC& Co., Ltd. (“NC&”) is committed to receiving and addressing reports of potential security vulnerabilities in NC& products and services. This policy explains how to report vulnerabilities and how NC& communicates and publishes remediation information in compliance with EN ISO/IEC 29147:2020.

1.2 Scope

This policy applies strictly to the following assets:
1. D20-Q2Plus
2. D21 4K

1.3 Audience

The target audience of this document is:
External Security Researchers, NC& Customers & Dealers, Internal PSIRT & Engineering Teams

1.4 Acronyms / Glossary

Acronym	Description
VDP	Vulnerability Disclosure Policy
PSIRT	Product Security Incident Response Team
PoC	Proof of Concept
CVSS	Common Vulnerability Scoring System
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration

1.5 Related Documents

Documents related to this document include:
[1] EN ISO/IEC 29147:2020 (Vulnerability disclosure)
[2] NC& Co., Ltd.

2 Guiding Policy & Commitments

2.1 Policy Overview

NC& recognizes the importance of the security research community. This policy outlines our commitment to resolving security issues transparently and responsibly to protect our customers and connected product for road vehicle.

2.2 Key Principles

Coordinated Disclosure: Vulnerabilities are disclosed publicly only after a fix is available.
Good Faith: We assume researchers act with good intentions to improve security.

2.3 Continuous Security Improvement

NC& integrates security throughout the entire product life cycle. We do not stop at simply fixing reported vulnerabilities; we conduct a thorough Root Cause Analysis for every valid report. The lessons learned are systematically fed back into our development processes and security training to prevent similar issues in future products and ensure long-term resilience.

2.4 Transparency & Responsibility

We are committed to disclosing security risks transparently to our customers and stakeholders. To protect our users from potential exploitation, NC& follows the principle of "Responsible Disclosure." This means we coordinate the timing of public vulnerability announcements with the availability of effective patches or remediations, ensuring that users have the means to protect themselves before technical details are made public.

3 Channels & Guidelines

3.1 Contact Channels

NC& accepts vulnerability reports through the dedicated channels below. To ensure timely handling, please submit reports through one primary channel and avoid duplicate submissions unless requested by NC&.

Email: securitysupport@nc-and.com

3.2 Report Content Guidelines

To help NC& assess validity, severity, scope, and impact, please include (as applicable):
•Product name and firmware version(s).
•Vulnerability type/class (e.g., CWE) and suspected root cause (if known).
•Clear steps to reproduce and required environment/configuration.
•Observed and expected behavior; impact description and severity estimate (if available).
•Your contact information and preferred method/time for follow-up.

3.3 Researcher guidelines (responsible disclosure)

NC& asks the security research community to:
•Make every effort to avoid privacy violations, degradation of user experience, disruption to internal or external servers, and destruction of data or physical assets during security testing.
•Provide sufficiently complete reporting details to enable verification and remediation.
•Keep information about the potential vulnerability confidential between you and NC& until a remedy is available or a mutually agreed disclosure plan is reached.
•Refrain from using any exploits or vulnerability information for commercial or business purposes.

3.4 NC& handling commitments (receipt, triage, and communication)

NC& commits to the following minimum handling practices:

•Acknowledgement: NC& will acknowledge receipt of potential vulnerability reports within 7 calendar days and provide a tracking identifier where feasible.

•Initial assessment (triage): NC& aim to perform an initial assessment of vulnerability reports within 14 calendar days, NC& will promptly inform the reporter (and other relevant stakeholders as appropriate).

•Ongoing communication: During handling, NC& will periodically (once every 30 calendar days) communicate with the reporter and relevant stakeholders, including status updates, significant new information, changes to plans, and disclosure timing until resolution of the reported issues.

3.5 Coordination (multi-vendor / supply chain)

If a vulnerability affects multiple vendors or shared components, NC& may:

•Notify other affected vendors and/or engage a coordinator to support communication and synchronized disclosure.

•Request or support assignment of common vulnerability identifiers (e.g., CVE) when appropriate.

3.6 Publication of advisories and remediation information

When appropriate, NC& publishes vulnerability advisories intended to reduce risk for users and stakeholders. Advisories will, at minimum:

•Include unique and consistent advisory identifiers, and vulnerability identifiers (e.g., CVE) where

applicable.

•State the initial publication date using an unambiguous format (DD/MM/YYY).

•Identify affected products and versions sufficiently for users to determine exposure.

•Describe impact, severity (e.g., CVSS), and remediation/workaround actions.

NC& will balance risk when deciding advisory timing, including considering active exploitation, remediation readiness, and coordination needs.

3.7 Authenticity and integrity (advisories and updates)

To reduce the risk of counterfeit advisories or malicious updates:

•NC& will provide a way to authenticate advisories and verify their integrity (e.g., digital signatures and/or published hashes).

•If users are required to apply a remediation, NC& will provide a way to authenticate and verify the integrity of remediations (e.g., digitally signed updates).