NRG Systems

Policy on Coordinated Vulnerability Disclosure

Version 1

Introduction

NRG Systems (collectively referred to herein as, "**NRG**" or "**we**" or "**us**") is committed to maintaining the security, confidentiality, integrity, availability, and lawful processing of its systems, services, applications, and data, including personal data processed on behalf of customers, employees, partners, and other stakeholders.

This Policy on Coordinated Vulnerability Disclosure ("**Policy**") provides a mechanism for individuals to report suspected security vulnerabilities relating to products with digital elements, remote data processing solutions, systems or services owned or operated by NRG.

This Policy is designed to support secure vulnerability handling while protecting the confidentiality, integrity, and availability of information assets and ensuring alignment with applicable legal, regulatory, privacy, and data protection obligations.

This Policy is informed by relevant legislation, industry guidance and standards, including:

- Cybersecurity and Infrastructure Security Agency Coordinated Vulnerability Disclosure guidance
- Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies Guideline – NIS Cooperation Group 2023National Institute of Standards and Technology SP 800-216
- International Organization for Standardization ISO/IEC 29147 - Vulnerability Disclosure
- International Organization for Standardization ISO/IEC 30111 - Vulnerability Handling Processes
- RFC 9116
- ETSI EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Requirements
- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- Directive (EU) 2022/2555 (NIS2 Directive)

This Policy should be read together with the NRG's Privacy Notice, Information Security Policies, and any other applicable legal or contractual terms.

Scope

This Policy applies to internet-accessible systems, applications, websites, APIs, and, where applicable, NRG products with digital elements, software, firmware, mobile or desktop applications, cloud services, remote data processing solutions, and other digital components owned, operated, supplied or supported by NRG.

Unless explicitly stated otherwise in writing, the following are outside the scope of this Policy:

- Social engineering or phishing attacks
- Physical security attacks
- Denial-of-service (DoS/DDoS) testing
- Spam or excessive automated scanning
- Credential stuffing, password spraying, or brute-force attacks
- Malware deployment
- Vulnerabilities requiring unrealistic user interaction
- Missing HTTP security headers without demonstrable exploitability
- TLS/SSL configuration observations without demonstrable security impact
- Cookie flags without exploitable impact
- Self-XSS
- Clickjacking affecting non-sensitive pages only
- Best-practice recommendations without an identifiable exploitable condition
- Previously disclosed or publicly known vulnerabilities

Vulnerabilities in third-party or open-source components are in scope where the component is included in a product as supplied by NRG. NRG coordinates with the upstream maintainer or vendor where appropriate. vulnerabilities in third-party products that are merely used alongside NRG's products should be reported to the relevant vendor according to their disclosure policy (if any).

Issues affecting the Company's corporate website or business IT systems are outside the scope of this Policy.

NRG reserves the right to determine whether any reported issue falls within the scope of this Policy.

This Policy applies to any individual who may discover, or set out to discover, a security vulnerability in any of the products or systems described in this Policy

References to "individuals" in this Policy can be to any member of staff or representative of NRG or a Business Partner. Business Partners must ensure that their staff and representatives comply with this Policy.

Responsible Reporting

NRG recognizes the importance of receiving information relating to potential security vulnerabilities affecting its products with digital element, remote data processing solutions, systems, services, or applications.

This Policy provides a mechanism for responsible reporting. Nothing in this Policy shall be interpreted as permission, authorization, license, or consent to access, test, scan, exploit, interfere with, or otherwise interact with any product with digital element, remote data processing solution, system, service, application, account, data set, or environment owned or operated by NRG.

NRG does not endorse, permit, or encourage:

- Unauthorized access to systems, applications, environments, or data
- Circumvention of security or privacy controls
- Exploitation of vulnerabilities
- Active security testing against production environments
- Automated scanning without prior written authorization
- Access to, extraction of, modification of, deletion of, or retention of personal data or confidential information
- Service disruption
- Public disclosure of vulnerabilities without prior written consent

Any activities conducted against NRG systems remain subject to applicable laws, regulations, contractual obligations, confidentiality obligations, privacy requirements, and terms of use.

Individuals identifying potential vulnerabilities should immediately cease further activity and report the matter through the channels described in this Policy.

Data Protection and Privacy Requirements

Protection of personal data and confidential information is a mandatory requirement under this Policy. Individuals reporting vulnerabilities must:

- Avoid accessing personal data unless strictly unavoidable to identify the existence of a suspected issue
- Immediately cease activity upon encountering personal data, special category data, confidential business information, authentication credentials, or regulated data.
- Not copy, download, transmit, retain, process, disclose, or otherwise use personal data obtained during any activity relating to a reported issue.
- Promptly notify NRG if personal data or confidential information may have been exposed, accessed, or impacted.
- Maintain strict confidentiality regarding any information observed during the course of identifying or reporting a suspected vulnerability.
- Comply with applicable privacy and data protection laws and regulations.

Any unauthorized access to personal data may constitute a breach of applicable data protection, privacy, cybersecurity, confidentiality, or criminal laws.

Reporting Requirements

Individuals submitting vulnerability reports must:

- Act responsibly and in good faith
- Avoid actions that could negatively affect the confidentiality, integrity, availability, or resilience of systems or data
- To the extent not needed for ordinary business purposes, refrain from accessing, acquiring, modifying, deleting, transmitting, or retaining data that does not belong to them
- Avoid exploitation of the vulnerability beyond the minimum necessary to identify the suspected issue
- Immediately cease activity upon discovery of sensitive information
- Maintain strict confidentiality regarding the reported issue unless expressly authorized in writing by NRG. Where the reporter is acting on behalf of an employer or other organization, the reporter should ensure that any sharing within that organization is limited to those with a legitimate need to know and remains subject to appropriate confidentiality obligations.

How to Report a Vulnerability

Suspected security vulnerabilities should be reported by completing the CVD form on NRG's website or by emailing: vulnerabilities@nrgsystems.com

Individuals are encouraged to report suspected vulnerabilities as soon as reasonably practicable, particularly where personal data, confidential information, authentication credentials, regulated information, or system availability may be affected. Prompt reporting assists NRG in assessing and, where required, complying with applicable legal, regulatory, contractual and data breach of notification obligations, including timeframes for assessing and notifying personal data breaches. This is without prejudice to any separate reporting, notification or escalation obligations that may apply under any contract, policy, law, regulation or duty owed to NRG or any other person.

Reports should include, where possible:

- Affected products, URL, system, API, or service
- The version of the product on which the vulnerability is present, or the specific configuration of the product that is vulnerable

- Detailed description of the vulnerability, including the following information:
  - A summary of the vulnerability
  - Required steps to reproduce the vulnerability
  - Required configuration to reproduce the vulnerability
  - Possible mitigation measures for the vulnerability
- Screenshots or supporting evidence, where appropriate
- Vulnerability severity (self-assessment): Critical / High / Medium / Low / Informational
- Potential impact assessment - what an attacker could do by exploiting this issue, and any evidence of real-world exploitation you're aware of
- Whether any personal data, confidential information, or regulated information may have been exposed
- Reporters contact details

NRG may request additional information to support investigation or validation of activities.

We encourage submissions via our website CVD page where possible.

Vulnerability Handling Process

NRG will make reasonable efforts to

- Acknowledge receipt of the report
- Investigate the reported issue, work to reproduce it, and determine which products and versions are affected
- Keep the reporter informed of the assessment and, where possible, the expected timeline
- Coordinate with the reporter on the timing of any public disclosure, and make fixes or mitigations available to affected customers

Submission of report does not guarantee:

- That the reported issue constitutes security vulnerability
- That remediation will occur within a particular timeframe
- Any entitlement to compensation, public recognition, or further communication

NRG may, at its sole discretion, coordinate remediation and disclosure of activities relating to reported vulnerabilities.

Public disclosure of vulnerabilities in NRG's system is prohibited unless explicitly authorized in writing by NRG.

When a vulnerability is confirmed and a fix or mitigation is available, NRG gives information about the issue, the affected products and versions, and the remediation steps available to affected customers and, where appropriate, publishes a security advisory, including, where appropriate, a CVE identifier for the issue. Nothing in

this Policy limits or delays any notification the Company is required to make to competent authorities under applicable law, including Regulation (EU) 2024/2847.

No Authorization Granted

This policy does not:

- Grant permission to access any system or data
- Authorize circumvention of security or privacy controls
- Permit testing, scanning, or exploitation activities
- Provide immunity from civil, criminal, regulatory, contractual, or data protection liability
- Waive any rights or remedies available to NRG
- Create any contractual relationship between NRG and any individual or entity

NRG reserves all legal rights relating to unauthorized activities conducted against its systems, services, applications, personnel, data, or infrastructure.

Reservation Of Rights

NRG reserves the right to

- Determine whether reported issues constitute a security vulnerability or personal data incident.
- Determine the severity, risk rating, and remediation approach for any reported issue.
- Decline to respond to reports falling outside the scope of this Policy
- Modify, from time to time, or withdraw this Policy at any time without notice. An individual who detects a security vulnerability should check this Policy before submitting a report
- Refer unlawful or malicious activities to law enforcement, regulators, supervisory authorities, or other relevant authorities where appropriate

Privacy and Confidentiality

Information submitted under this Policy will be used solely for security assessment, investigation, remediation, compliance, audit, regulatory, legal, and defensive purposes.

Reports and associated information may be shared internally, and with our advisors (who are themselves bound by confidentiality agreements) with Information Security, Legal, Privacy, Compliance, Risk, Internal Audit, and other authorized stakeholders on a need-to-know basis.

Reporters must maintain confidentiality regarding reported vulnerabilities and any associated information unless disclosure is expressly authorized in writing by NRG.

NRG will process any personal data received under this Policy in accordance with applicable data protection and privacy laws and its Privacy Notice.

No Compensation

NRG does not operate a bug bounty program and does not provide monetary compensation, rewards, or incentives for vulnerability reports unless explicitly agreed in writing.