

Responsible Disclosure Policy

Nixelus

Purpose

To allow for the reporting and disclosure of vulnerabilities discovered by external entities, and anonymous reporting of information security policy violations by internal entities.

Scope

Nixelus' Responsible Disclosure Policy covers applies to Nixelus' core platform and its information security infrastructure, and to internal and external employees or third parties.

Background

Nixelus is committed to ensuring the safety and security of our customers and employees. We aim to foster an environment of trust, and an open partnership with the security community, and we recognize the importance of vulnerability disclosures and whistleblowers in continuing to ensure safety and security for all our customers, employees and company. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise and whistleblowers who add an extra layer of security to our infrastructure.

Roles and Responsibilities

The acting Information Security Compliance Officer and Manager HR will facilitate and maintain this policy and ensure all employees have reviewed and read the policy.

Legal Posture

Nixelus will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Reporting inbox (vulnerability@nixelus.net). We openly accept reports for the currently listed Nixelus products. We agree not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming Nixelus or its customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program.
- Test on products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices/software, etc.
- Adhere to the laws of their location and the location of Nixelus. For example, violating laws that would only result in a claim by Nixelus (and not a criminal claim) may be

acceptable as Nexelus is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.

- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires.

Policy

Vulnerability Report/Disclosure

How to Submit a Vulnerability

To submit a vulnerability report to Nexelus' Product Security Team, please utilize the following email vulnerability@nexelus.net

Preference, Prioritization, and Acceptance Criteria

We will use the criteria from the next sections to prioritize and triage submissions.

What we would like to see from you:

- Well-written reports in English will have a higher probability of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.
- Please include any plans or intentions for public disclosure.

What you can expect from Nexelus:

- A timely response to your email (within 2 business days).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- Credit after the vulnerability has been validated and fixed.

If we are unable to resolve communication issues or other problems, Nexelus may bring in a neutral third party to assist in determining how best to handle the vulnerability.

Whistle Blowing

How to Submit a Report

To anonymously report an information security program violation or a violation of related laws and regulations, please utilize this link [Microsoft Forms](#) to submit the violation.



Preference, Prioritization, and Acceptance Criteria

We will use the criteria from the following sections to prioritize and review submissions.

What we expect from you:

- Detailed report made in *good faith* or based on a *reasonable belief*.
 - *Good Faith* means the truthful reporting of a company-related violation of information security policies, procedures, or regulations, as opposed to a report made with reckless disregard or willful ignorance of facts.
 - *Reasonable Belief* refers to the subjective belief in the truth of the disclosure AND that any reasonable person in a similar situation would objectively believe based on the facts.
- Details of the violation (i.e., what, how, why).
- Details of the reported event, with facts (i.e., who, where, when).
- You are NOT responsible for investigating the alleged violation, or for determining fault or corrective measures.

What you can expect from Nexelus:

- Your report will be submitted to the **HR and the leadership** for review.
- Protection of your identity and confidentiality.
 - CAVEAT: It may be necessary for your identity to be disclosed when a thorough investigation, compliance with the law, or due process of accused members is required.
- Protection against any form of retaliation and harassment, such as termination, compensation decreases, or poor work assignments and threats of physical harm.
 - If you believe that you are being retaliated against, immediately contact <role>.
 - Any retaliation or harassment against you will result in disciplinary action.
 - CAVEAT: Your right for protection against retaliation does not include immunity for any personal wrongdoing alleged in the report and investigated
- Due process for you and for the accused member(s).
- Corrective actions taken to resolve a verified violation and a review and enhancement of applicable policies and procedures, if necessary or appropriate.
- Continuous information security awareness training and understanding your rights as a whistleblower.