Oneview Responsible Disclosure Policy

Version	**1.0**
Date of Version	**18 March 2026**
Created By	**Richard Eibrand**
Approved By	**Declan Bright**
Confidentiality Level	**TLP:GREEN**

Change History

Date	Version	Created By	Description of Change
13 Feb 2026	0.1	Richard Eibrand	Based on Drata policy template and imported into Oneview template
13 Feb 2026	0.2	Declan Bright	Minor edits
16 Mar 2026	0.3	Richard Eibrand	Approved edits
18 Mar 2026	1.0	Declan Bright	Reviewed and approved

Table of Contents

PURPOSE **3**

SCOPE **3**

BACKGROUND **3**

LEGAL POSTURE **4**

POLICY **5**

VULNERABILITY REPORT/DISCLOSURE 5

How to Submit a Vulnerability 5

Preference, Prioritisation, and Acceptance Criteria 5

What Oneview would like to see from you 5

What you can expect from Oneview 5

WHISTLE BLOWING 6

How to Submit a Report 6

Preference, Prioritisation, and Acceptance Criteria 6

What Oneview expect from you 6

What you can expect from Oneview 6

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. This policy also allows Oneview Healthcare (Oneview) to meet its legal obligations under the NIS2 Directive, including requirements for vulnerability handling and disclosure (Article 21(2)(e)).

Scope

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

Excluded from scope:

- Social engineering attacks against Oneview staff.
- Physical security testing.
- DDoS or availability-based attacks.
- Unauthorised access to PHI, where applicable HIPAA and GDPR policies apply

Background

Oneview is committed to ensuring the safety and security of its customers and employees. Oneview aims to foster an environment of trust, open partnership with the security community, and recognises the importance of vulnerability disclosures and whistleblowers in continuing to ensure the safety and security of all customers, employees and the company. Oneview has developed this policy to both reflect the companies' corporate values and to uphold its legal responsibility to good-faith security researchers that are providing their expertise and whistleblowers who add an extra layer of rigour to security posture.

Legal Posture

Oneview will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Reporting inbox. Oneview openly accepts reports for the currently listed Oneview products. Oneview agrees not to pursue legal action against individuals who:

- Engage in testing of systems/research without harming Oneview or its customers.
- Engage in vulnerability testing within the scope of our vulnerability disclosure program.
- Engage in testing 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 Oneview. For example, violating terms and conditions that would only result in a claim by Oneview (and not a criminal claim) may be acceptable as Oneview is authorising 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.
- Oneview is not legally bound to provide any monetary or financial rewards for disclosed potential or actual vulnerabilities

Policy

Vulnerability Report/Disclosure

How to Submit a Vulnerability

To submit a vulnerability report to Oneview's Product Security Team, please send details to the following email address: security@oneviewhealthcare.com

Preference, Prioritisation, and Acceptance Criteria

Oneview will use the criteria from the following sections to prioritise and triage submissions.

What Oneview would like to see from you

- Well-written reports in English will have a higher probability of resolution.
- Reports that include proof-of-concept steps and/or code will enable faster 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 Oneview

- A timely response to your email (within 2 business days).
- After triage, Oneview 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 Oneview are unable to resolve communication issues or other problems, Oneview may engage with 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 send details to the following email address: security@oneviewhealthcare.com

Preference, Prioritisation, and Acceptance Criteria

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

What Oneview 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 wilful 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 Oneview

- Your report will be submitted to the Head of Information Security 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 the HR Director.
    - 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 investigation
- 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.