Amsterdam University of Applied Sciences

Policy Coordinated Vulnerability Disclosure

Adopted by the Executive Board as decision no. 2021hcb061 on 2 March 2021

Creating Tomorrow

Contents

References

[IB]	Amsterdam University of Applied Sciences Information Security Policy, 23-10-2018

Definitions

A. **Coordinated Vulnerability Disclosure** (Dutch: Verantwoorde Openbaarmaking (VO)), refers to the responsible and joint disclosure of ICT vulnerabilities by the notifier and the organisation based on a policy adopted by organisations for this purpose.

B. This was previously referred to as Responsible Disclosure.

C. A **vulnerability** is a (suspected) weakness or breach in the security features of the ICT infrastructure of Amsterdam University of Applied Sciences (AUAS).

D. The notifier is the person or body who/which reports a vulnerability by means of the VD procedure.

1 Introduction

The dependence on the digital infrastructure is increasing. It is very important to the AUAS to ensure the security of its systems. In spite of the attention paid to information security, the organisation may still fail to detect a weakness in a product or service, which may, however, be noticed by someone else.

It is therefore important for the AUAS to promote and publish a Coordinated Vulnerability Disclosure policy. For both the organisation and the notifier, the policy clarifies what responsibilities both of these parties have.

2 Target group

This policy is aimed at management, higher management and the security organisation in order to define the policy that will provide direction and establish the preconditions for carrying out a VD procedure.

The VD procedure is a way for the AUAS to offer third parties, such as external security researchers, students, guests, visitors and external researchers and contacts, which do not (usually) have a contractual relationship with the AUAS, the opportunity to report vulnerabilities.

The VD procedure does not apply to people who are in any way internally involved in (any aspects of) the operational processes, such as employees, lecturers or suppliers, since these parties are obliged in accordance with the information security policy to report any infrastructure vulnerabilities to the ICTS service desk or the CERT.

3 Scope

The VD policy is an elaborated version of a section of the information security policy, which refers to a ‘guideline for Responsible Disclosure’[2]. The VD policy describes the

[1] See Chapter 8 of the information security policy [IB].

[2] See Appendix B of the information security policy [IB].

responsibilities of the organisation and the notifier and specifies the components of the VD procedure. The operational process description [ProcVD] is not part of this policy.

There is an important relationship and partial overlap with contiguous policy areas:

- **Privacy:** a VD report can also have a (negative) effect on the processing of personal data, as a result of which it may also be required to follow the data breach reporting procedure.
- **Incident management**: whilst the VD procedure does involve several concrete actions of its own, the internal handling and, if applicable, upscaling of reports takes place via the procedure 'reporting and handling incidents' as referred to in the information security policy[1].

4 Goal of Coordinated Vulnerability Disclosure

Digitalisation has an increasing influence on society. Vulnerabilities can potentially have a significant impact on users. The social significance is a key motivation for notifiers to expose vulnerabilities and risks. VD enables vulnerabilities to be dealt with in a socially responsible and effective manner.

The AUAS can help reduce the reluctance to report vulnerabilities. The AUAS frequently comes into contact with researchers and students who are knowledgeable about ICT and these parties are likely to recognise vulnerabilities and want to report these in a responsible manner. VD enables steps to be taken more quickly to avoid potential damage and raises the level of information security. It also offers a way to prevent vulnerabilities being disclosed before having been resolved.

Whether or not vulnerabilities have been actively searched for by a notifier, criminal or civil proceedings can be instituted against them. Having a VD policy in place can take away some of the uncertainty with regard to the risk of being charged. The VD policy ensures there are agreements in place between the notifier and the AUAS.

5 Basic principles

The following basic policy principles are applied:

1. The AUAS demonstrates the willingness to receive information about vulnerabilities.
2. With VD, it is of prime importance that the AUAS and the notifier both abide by the agreements with regard to reporting the vulnerability and how it is dealt with. The AUAS publishes the agreements on the website.
3. Provided that the notifier abides by the agreements, the AUAS will not take any (further) legal action. Should it emerge that the notifier has not honoured the agreements, (further) legal action may still be taken.
4. The notifier of a vulnerability not previously reported or known to the AUAS will receive a reward provided that action has been taken in conformity with the agreements. The size of the reward will be determined on the basis of the seriousness of the vulnerability and the quality of the report and can range from an honourable mention to a gift.
5. The VD policy relates to all of the AUAS's ICT service provision, whether in-house or outsourced to third parties such as Cloud-based service providers.

6. VD reports may be made anonymously provided this is done directly to or through a trusted party of the AUAS. This may help prevent a notifier who would rather remain anonymous failing to report a vulnerability or disclosing it.
7. The notifier will receive confirmation of receipt as soon as possible and at the latest within two days after receipt of the VD report. If the report triggers a fast response, this indicates that it is being taken seriously. This may keep the notifier from seeking to disclose the vulnerability later.
8. If a VD report is made (to the AUAS) concerning a vulnerability found in a system owned by a third party which is not otherwise connected to the AUAS, the notifier will be referred to the third party and the AUAS VD procedure will be terminated. The notifier remains responsible, and it is up to the notifier to decide whether or not to contact the third party.

6 Roles and responsibilities

In the VD procedure, the focus is on the AUAS and the notifier entering into discussions with each other. In the process, it is important that there are as few links as possible between the person who reports the vulnerability and the person in the organisation who is responsible for addressing it. VD reports are handled primarily by the CERT. This section also sets out the other roles and responsibilities involved.

Central roles of the Executive Staff

6.1 Chief Information Security Officer (CISO)

The CISO is the person ultimately responsible for the VD procedure, including for its drafting, adoption, publication, execution and evaluation.

Matters relating to the VD reports are reported to the CISO. The CISO informs the AUAS's spokespersons of every VD report received. Depending on its seriousness, the Executive Board member holding the Information Security portfolio will also be informed. The CISO is also the one who ultimately decides about granting a reward. The CISO's periodic report includes a list of the VD reports made during the period in question. This report is made available to the Executive Board member holding the Information Security portfolio.

Information security at ICTS

6.2 CERT

The CERT coordinates the acceptance and handing of reports. The CERT has a direct escalation line with CISO, if required. Its responsibilities are as follows:

- In the first instance, to determine the seriousness and validity of the report.
- To maintain contact with and provide periodic updates to the notifier.
- To coordinate the investigation and take the initiative to put together the team which will get to work on the report. The composition will depend upon the nature of the vulnerability and the involved systems.
- To report on the course of the report.

The CERT chair monitors the following:

- The quality of the manner in which the report is handled.
- The time frame in which the report is handled.

The CERT chair will coordinate the incidents and report these to the CISO. If it concerns a report which may involve a violation of the privacy legislation, the CERT chair will notify the data protection officer immediately.

External roles

6.3 Notifier

The notifier has no formal relationship with the AUAS, but the AUAS expects them to assume the following responsibilities to ensure successful collaboration:

- To refrain from abusing vulnerabilities, for example by downloading more data than required to demonstrate the vulnerability, or inspecting third-party data or deleting or modifying data and to exercise extra restraint if personal data is encountered.
- All confidential data obtained as a result of vulnerabilities must be deleted immediately.
- To refrain from making use of attacks on the AUAS's infrastructure, social engineering, distributed denial-of-service (DDOS) attacks, spam, and the like.
- To provide sufficient information to enable the vulnerability to be identified and resolved.
- To allow enough time for the breach to be stopped before the vulnerability can be disclosed.
- To determine the period of time of possible disclosure in consultation with the AUAS. This period will also depend a great deal on the nature of the vulnerability and the type of system. A period of 60 days is taken as a guideline for software vulnerabilities and 6 months for hardware vulnerabilities. An extension or reduction of this period can be negotiated, depending upon the impact and scope of the vulnerability.

7 Policy implementation

The implementation of the VD policy is reflected in the 'Coordinated Vulnerability Disclosure procedure', in which this policy is elaborated, giving attention to:

- Elaboration of roles and responsibilities
- Guidelines for rewards
- Timely feedback to the notifier
- Publication on the website

An awareness initiative is to be held in order to raise employee awareness about the obligation to report vulnerabilities.