National Cyber Security Centre
Ministry of Security and Justice

» **Policy** *for arriving at a practice for Responsible Disclosure* »

Table of contents

Introduction

Information and communication technologies (ICT) have ingrained themselves into the very fabric of our society. On the one hand, they offer an enormous range of user applications. On the other, the breadth and depth of their application increases the potential impact of their vulnerabilities. As their importance rises, so too does the social importance of effectively dealing with the vulnerabilities of ICT.

The ICT security community is made up of a wide variety of players that gain their knowledge of vulnerabilities in systems in an equally wide variety of ways. One of the primary motivations of white hat hackers and security researchers is improving the safety of ICT systems by probing vulnerabilities and risks. Well-intentioned hackers and security investigators can be an important ally to the parties using vulnerable systems.

This represents a significant interest for both public and private parties, who are, to a very large degree, dependent on the uninterrupted functioning of information systems in their day-to-day work. This makes learning about the vulnerabilities in your own systems and how to improve their security a necessary part of your operations.

Current practice among security researchers tends to avoid directly reporting a vulnerability to the affected users, for fear of revealing the vulnerability to the world at large through the media or other indirect avenue. This would, of course, be extremely undesirable for a vulnerability that has not yet been dealt with. In some cases, there is even specific software available designed to exploit known vulnerabilities. Often, the disclosure of a vulnerability leads to an incident that is both damaging to the well-intentioned party and in which the vulnerable organisation is not immediately in a position to address the vulnerability with increased security.

This proves the importance of bringing these parties together. This policy guideline is intended to help bring together disclosers with knowledge of vulnerabilities and the desire to remedy them, and the organisations affected by them and that are dependent on these vulnerable systems.

Over a third of vulnerabilities have the potential to fully compromise security[1]

In over one-third of cases, successful exploitation of known vulnerabilities results in security being completely compromised, allowing the hostile actors to:
- render the system fully unavailable (availability)
- modify any files on the system (integrity)
- gain access to any files on the system (confidentiality)

Even as the number of known vulnerabilities grows, they can be expected to remain a major cause of future incidents. The most significant reason for this is that they are not, and cannot be, remedied by the organisations themselves.

It is advisable to set out commitments for working together in this partnership. Good arrangements give all the parties more certainty on their respective positions and can contribute to the common goal of increasing the security of information systems. This policy guideline offers organisations a look at how a coherent responsible disclosure policy can be structured so as to facilitate reporting of vulnerabilities in proper cooperation with the ICT security community. For hackers and researchers, it is a method that provides its own safeguards.

It does not violate applicable criminal law frameworks, but the guideline is meant to offer organisations a tool for working together with all parties that highly value the security of ICT systems in a constructive and custom-tailored policy. This actively contributes to reducing the security risks that vulnerabilities represent and their potential negative societal, economic and financial impact.

It has been put together based on discussions with a broad and diverse group of potential disclosers and private and public parties. These discussions were the foundation for the building blocks described later in this policy guideline, which in turn can serve as a starting point for organisations interested in defining their own policy on responsible disclosure in order to facilitate good disclosure. Recent months have seen numerous parties taking initiatives to put forward responsible disclosure policies, and aspects of these initiatives have most definitely been incorporated into the final version of this guideline.

The following chapters will look at, in turn, vulnerabilities, the definition of responsible disclosure and the building blocks of responsible disclosure.

[1] For more information, see the Cyber Security Report Netherlands 2 (CSBN-2).

Chapter 1

What is a vulnerability

Vulnerabilities in ICT are encountered in numerous places in hardware and software in various different gradations. Their common denominator is that their exploitation presents potential security risks.

The vulnerability is a particular property of a society, organisation or information system, or component thereof, that compromises the resilience of the entity. A vulnerability presents a hostile actor with the opportunity to inflict damage at a point where the protection against such damage is weak. For example, a hostile party might impede and influence legitimate access to information or functionality, or access that information/functionality in an unauthorised manner. Vulnerabilities are the 'gateways' through which threats can lead to incidents. Remedying vulnerabilities is a direct method of reducing threats and the chance of incidents.

By exploiting vulnerabilities, systems can be brought down (availability), data within the system can be changed (integrity) and data can be made accessible to unauthorised persons (confidentiality).

The more dependent an organisation is on ICT, the bigger the impact an attack on availability, integrity or confidentiality can have, especially if the organisation is not yet aware of the vulnerability or vulnerabilities being exploited.

Chapter 2
Responsible Disclosure

In the ICT world there are several different practices for revealing ICT vulnerabilities. Examples include the 'full disclosure' method, in which the vulnerability is fully disclosed to the public, and the more restricted method of responsible disclosure. Fully disclosing a vulnerability to the public while the vulnerability itself still exists can create a security risk. This is why responsible disclosure is much more preferable in practice.

Within the ICT community, there is a great deal of knowledge (and the will to share it) on vulnerabilities in ICT and the ways to remedy them. As such, cooperation with the ICT community is critically important in the collective pursuit of cyber security.

In the ICT world, responsible disclosure is revealing ICT vulnerabilities in a responsible manner in joint consultation between discloser and organisation based on a responsible disclosure policy set by organisations.

Goal of responsible disclosure

The goal of responsible disclosure is to contribute to the security of ICT systems and control the vulnerabilities in them by reporting those vulnerabilities in a responsible manner and acting on the reports appropriately so as to prevent or limit potential damages to the maximum possible extent. Part of this means allowing sufficient time for action before divulging the vulnerability.

A central aspect of working with a responsible disclosure policy is remedying the vulnerability and increasing the security of information systems.

Fundamental to responsible disclosure is that the parties involved adhere to the arrangements on reporting and dealing with the vulnerability. A party that adopts a responsible disclosure policy may, for example, undertake the obligation to not report a vulnerability if the rules applicable under the policy are not complied with.

The primary actors in responsible disclosure are the discloser and the organisation that is the owner/administrator of the system. It is important to have the minimum possible number of links in the chain between the person disclosing the vulnerability and the organisation responsible for solving the problem. The discloser and the organisation may, however, jointly decide to inform the National Cyber Security Centre (NCSC) or other parties in the ICT security community of the vulnerability, particularly if the vulnerability is not a known vulnerability, so as to prevent or limit the direct and indirect impact of the vulnerability elsewhere.

Chapter 3 takes a closer look at the parties' respective responsibilities. Chapter 4 presents the building blocks of responsible disclosure.

Chapter 3
Responsibilities

The point of pursuing a policy of responsible disclosure is to allow the discloser and organisation to collectively contribute to reducing vulnerabilities in information systems. However, working with responsible disclosure does not diminish any existing responsibilities and obligations. All actors involved in responsible disclosure have their own roles. Their respective responsibilities are outlined briefly below.

The owner/administrator organisation of the information system
The organisation that is the owner/administrator of the information system has the primary responsibility for the security of that system. This makes that organisation equally responsible for the way in which the disclosure of a vulnerability is acted on. Based on the guidelines, the organisation may opt for an open policy of responsible disclosure.

The discloser of a vulnerability
The implementation of any responsible disclosure policy hinges on the discloser. The discloser has in some way observed a vulnerability and wants to contribute to the security of the information system by revealing the vulnerability so that the organisation can remedy it. The discloser of a vulnerability is responsible for his/her own actions and the way in which he/she discovered the vulnerability. Reporting the vulnerability does not absolve the discloser from criminal investigation and prosecution if the discloser committed a crime in demonstrating the vulnerability. The organisation and the discloser may agree under a responsible disclosure policy that no charges will be filed in regard to specific criminal activities of the discloser. A similar arrangement may be made for civil actions.

The NCSC
Responsible disclosure is primarily an issue for the organisation and the discloser, and which an organisation can regulate with a policy. This, however, does not diminish the fact that the NCSC has a role in promoting the implementation of a responsible disclosure policy. The NCSC also has a role in propagating knowledge of ICT vulnerabilities to the government and the vital sectors. Where necessary, organisations may engage the NCSC to inform other organisations of vulnerabilities observed. If a vulnerability is reported directly to the NCSC, the NCSC will attempt to put the discloser in direct contact with the impacted organisation.

Chapter 4
Building blocks for Responsible Disclosure

The building blocks for responsible disclosure are listed below. They are grouped by relevance to the organisation, the discloser and the NCSC.

4.1 The organisation

Responsible disclosure starts with an organisation that is owner of information systems or the vendor of a product. After all, the owner/vendor has primary responsibility for the information security of the system or product. An important part of this is that the organisation has the choice to adopt and pursue a responsible disclosure policy, to give the organisation an effective approach to resolving vulnerability issues.

By drafting its own responsible disclosure policy, the organisation makes clear how it intends to handle reports of vulnerabilities. As we have seen from the number of parties that have done so already, this can be done as follows:
The organisation drafts a policy for responsible disclosure and makes it publicly accessible.

- The organisation ensures that the threshold for someone wishing to report a vulnerability is low. The method can be standardised, for example, by means of an online form for making reports. The organisation may wish to consider whether anonymous reports should be allowed.

- The organisation sets aside the capacity for an adequate response to any report received.

- The organisation receives the report of a vulnerability and ensures that it is routed as quickly as possible to the department best able to evaluate and act on the report.

- The organisation sends the discloser a confirmation of receipt of the report, preferably digitally signed to emphasize the priority. The organisation and the discloser then enter into contact to discuss the next steps.

- If the vulnerability is to be made public, the organisation will set a date for when the vulnerability will be made public in consultation with the discloser. A reasonably standard term that can be used for software vulnerabilities is 60 days. Remedying hardware vulnerabilities is much more difficult; for these, a term of six months can be considered reasonable under normal circumstances.

- In consultation between the parties it may be prudent to extend or reduce this term depending on how many systems are dependent on the system with the vulnerability.

- If a vulnerability is difficult or impossible to resolve, or if resolving it will involve high costs, the disclosure and the organisation may agree to not disclose the vulnerability.

- The organisation will keep the discloser and any other stakeholder parties abreast of the progress in the process.

- The organisation may adhere to a policy of giving the discloser credit for the report, if the discloser so desires.

- The organisation may choose to give the discloser some form of remuneration/recognition for reporting a vulnerability in ICT products or services if the discloser followed the rules of the responsible disclosure policy. The amount of the reward may be based on the quality of the disclosure.

- In consultation with the discloser, the organisation may decide to inform the broader ICT community of the vulnerability if it is likely that the vulnerability is more widespread than the organisation itself.

- In the policy, the organisation will express its position on declining to take legal action where the discloser acts in accordance with the policy.

4.2 The discloser

The implementation of any responsible disclosure policy hinges on the discloser. The discloser has in some way observed a vulnerability and wants to contribute to the security of the information system by revealing the vulnerability so that the organisation can remedy it. By doing so, disclosers recognise that they have an important social responsibility and are living up to it by disclosing vulnerabilities in a responsible way. For the discloser, a successful practice for responsible disclosure must be built on the following building blocks:
The discloser is responsible for his/her own actions and must make sure that the report is made, in the first instance, to the system/information owner.

- The discloser must report the vulnerability as quickly as is reasonably possible, to minimise the risk of hostile actors finding it and taking advantage of it.

- However, the discloser must do so in a manner that safeguards the confidentiality of the report so that others do not gain access to the information.

- The discloser's response must not be disproportionate, such as:
  - by using social engineering to gain access to the system
  - by building his or her own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, because doing so can cause additional damage and create unnecessary security risks
  - by utilising a vulnerability further than necessary to establish its existence
  - by copying, modifying or deleting data on the system. An alternative for doing so is making a directory listing of the system.
  - by making changes to the system
  - by repeatedly gaining access to the system or sharing access with others
  - by using brute force attacks to gain access to the system. This is not a vulnerability in the strict sense, but rather repeatedly trying out passwords.

Finally, the discloser and the organisation can make arrangements on informing the broader ICT community. This might be the right choice if the vulnerability is new and it is clear that it may be present on other systems or at other organisations. In such cases the NCSC could be contacted to serve the government and vital sectors.

4.3 The NCSC

Principally, responsible disclosure is a matter for the organisations and the discloser. Nonetheless, the NCSC's task is to promote the use of a responsible disclosure policy. The NCSC can also be part of consultations between the discloser and the organisation in the process of sharing information on the vulnerability with the target group to limit the further security risks the vulnerability represents. If a discloser or potential discloser contacts the NCSC directly, the NCSC will attempt to put the discloser in contact with the organisation.

Where possible the NCSC will use the information obtained on technical vulnerabilities in consultation with organisations and disclosers to pass the information on to the ICT community. This can be done by publicly disclosing a portion of the information, writing or updating a fact sheet or white paper, or informing organisations in a coordinated manner.

- In any situation in which a report is made to the NCSC, the NCSC will attempt to put the discloser/potential discloser into contact with the organisation.

- Whenever it is informed of a vulnerability, the NCSC will inform other parties within the target group of government organisations and vital sectors.

National Cyber Security Centre
Ministry of Security and Justice

Nationaal Cyber Security Centrum

Wilhelmina van Pruisenweg 104 | 2595 AN | Den Haag
Postbus 117 | 2501 CC| Den Haag

T 070 888 75 55
F 070 888 75 50

info@ncsc.nl
www.ncsc.nl