CIO Platform Nederland

CEG Information Security

# Coordinated Vulnerability Disclosure

*Implementation guide*

## A publication of the CIO Experience Group Information Security

CIO Platform Nederland, February 2016

www.cio-platform.nl/publicaties

# Contents

# 1 Introduction

Conducting a Coordinated Vulnerability Disclosure policy can have a major impact on the business operations of an organisation. It is therefore important that the implementation of a Coordinated Vulnerability Disclosure policy and procedure are carefully considered.

The CIO Platform Nederland has drawn up a model policy for Coordinated Vulnerability Disclosure and an operational procedure for Coordinated Vulnerability Disclosure, for use by companies and organisations. This guide has been developed as a tool for thorough implementation of policy and procedure.

This implementation guide is aimed at the person responsible for the formulation of an organisation's data security policy. The implementation guide is an aid for achieving proper interpretation of the Coordinated Vulnerability Disclosure policy.

There are examples, in practice, of undesired results flowing from incorrectly drawn up policy and procedure. An improperly formulated reward structure may attract (professional) bounty hunters, who regularly submit reports in order to collect as many rewards as possible. Rules that do not properly describe the requirements regarding publication can also be a significant issue, for instance for a vulnerability reporter who wants to present his findings at a security conference.

The objectives of Coordinated Vulnerability Disclosure include:

a) Helping to ensure that vulnerabilities identified by external persons are disclosed to your organisation;
b) Helping to ensure that a vulnerability can be addressed before it is exploited and made publicly known;
c) Equipping your organisation to responsibly handle the personal information of clients and others;
d) Providing insight and direction with regard to the legal and communication process applied by your organisation when handling vulnerability reports.

## 1.1 Definition of Coordinated Vulnerability Disclosure

There are various definitions of Coordinated Vulnerability Disclosure, which is also referred to as Responsible Disclosure. The definition used in this document is that of the National Cyber Security Center (NCSC): "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." The definition of the NCSC shows that Coordinated Vulnerability Disclosure can only take place when an organisation has a policy in this regard. In this publication we will use the internationally more acceptable phrase of Coordinated Vulnerability Disclosure instead of Responsible Disclosure, they are interchangeable.
[https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html]

## 1.2 Overview

Chapter 2 contains the arguments for implementing Coordinated Vulnerability Disclosure. The positioning of the model policy and the procedure are covered in chapter 3. Chapter 4 looks more closely at harmonisation between the parties involved. Chapter 5 describes the decision points for Coordinated Vulnerability Disclosure and describes, per decision, the considerations to be taken into account in the organisation's decision-making. Chapter 6 sets out the steps of a plan to be used in implementing Coordinated Vulnerability Disclosure.

## 1.3 Special thanks

Our special thanks are due to the authors of documents that form the foundation of this publication. We would specifically like to mention Cooperation SURF, the Dutch National Cyber Security Centre and Floor Terra. Their prior work has made it easier for us to offer a helping hand to all organisations aiming to implement Coordinated Vulnerability Disclosure. By working together we make the digital world safer.

# 2 Arguments for a Coordinated Vulnerability Disclosure policy

ICT plays an increasingly important role in all organisations, while services are increasingly delivered via the Internet. Organisations are expected to reliably manage information. A number of the arguments that show the importance of Coordinated Vulnerability Disclosure for organisations are summarised below:

## 2.1 Reduce the reporting threshold

An organisation can lower the threshold for the reporting of vulnerabilities by its target audience.

## 2.2 Establishing the rules

The behaviour of an investigator identifying vulnerabilities can go too far, according to criminal law[1], although such behaviour may be justified in terms of the interests of society. The organisation can specify how far a reporter may go in carrying out his investigation, by setting out what it expects of the reporter in a Coordinated Vulnerability Disclosure policy. This provides clarity in the grey area of legislation on Coordinated Vulnerability Disclosure.

## 2.3 Trust

Organisations process a lot of customer data. This should be handled carefully. Every contribution to increased security of this data is relevant and builds customers' trust.

## 2.4 Communal interest

ICT has a growing influence on society. The potential impact of vulnerabilities on users is significant. A key driver for reporters in exposing vulnerabilities and risks is public interest. Coordinated Vulnerability Disclosure is a socially responsible and effective way of handling of vulnerabilities.

## 2.5 Raising the level of data protection

No organisation has all the knowledge it needs in-house. Coordinated Vulnerability Disclosure can be applied to utilise knowledge about vulnerabilities

[1] In this publication legal comments are based on Dutch laws and regulations. Take care to check the specific laws and regulations in each country that you apply this policy in, as they may change from country to country.

that exists outside the organisation. Offering well-intentioned security investigators the opportunity to report vulnerability in a responsible manner means they can make a contribution to increasing the organisation's data security.

## 2.6 Trend

Coordinated Vulnerability Disclosure is increasingly being dealt with on an industry-wide basis in the Netherlands. Examples of industry-wide stimulation of Coordinated Vulnerability Disclosure are to be found in the Dutch government, major Dutch telecom providers, the Dutch banks and the Dutch Hosting Provider Association. Outside the Netherlands there is also a growing interest in this kind of information sharing.

# 3 Positioning

Coordinated Vulnerability Disclosure can have a major impact on the business operations of an organisation. Coordinated Vulnerability Disclosure policy must be aligned with existing policy documents, procedures and agreements, in order to ensure that those involved are properly informed and able to work together on a Coordinated Vulnerability Disclosure report. Figure 1 graphically displays the positioning of Coordinated Vulnerability Disclosure policy. [NB: Not every organisation has all of these elements - customise to fit your organisation and environment].

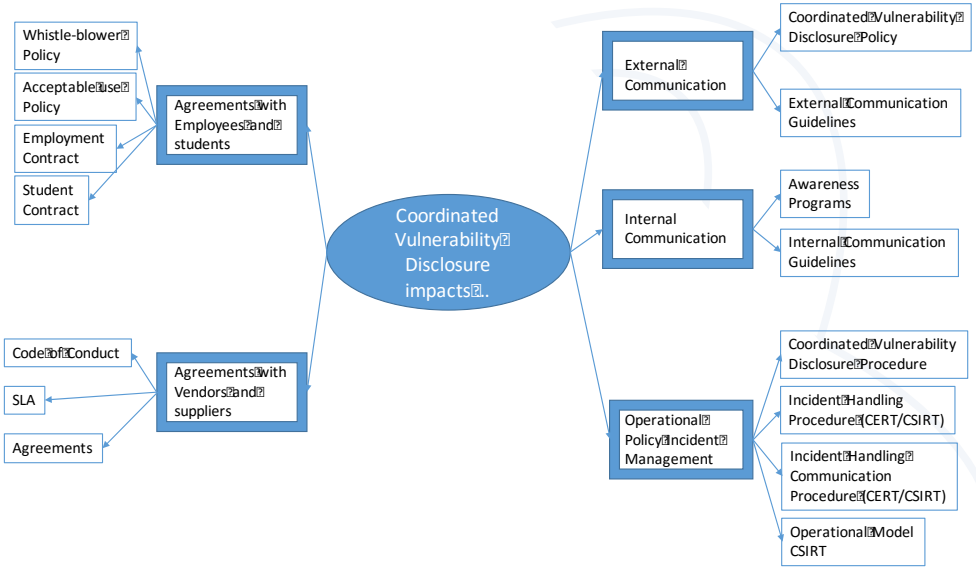


Figure 1

## 3.1 Internal

### 3.1.1 Operational policy documents for incident management

Coordinated Vulnerability Disclosure policy shares many similarities with incident management. The policies might, to a large extent, even be the same. The biggest factor distinguishing it from normal incident procedure is the extensive communication with the reporter and the way information is revealed and

rewarded. Coordinating Vulnerability Disclosure policy and incident management as regards damage limitation, exposure assessment, remediation and restoration will avoid the creation of significant overlap between these policies.

### 3.1.2 Agreements regarding communication

The organisation is expected to keep the reporter and other stakeholders informed on progress of the process. The reporter's interests may sometimes conflict with the interests of the organisation. Furthermore, reports can be highly technical, making it necessary for communication to proceed directly via technical, operational personnel. It is therefore of great importance to establish policy rules with regard to the reporter's communication.

### 3.1.3 Whistleblower policy

While notification of organisational wrongs may be covered by a whistleblower scheme, reports of (technical) vulnerability in the organisation's systems are often not covered by such a scheme.[2]

## 3.2 External

### 3.2.1 Agreements with suppliers

In addition to the reporter, other third parties may also be involved in reporting a vulnerability. These may include the provider hosting the vulnerable website or the manufacturer of a vulnerable network element. The actions of a reporter may impact the reliability of a third party's system. Prior arrangements with suppliers on the basis of conditions of purchase with regard to Coordinated Vulnerability Disclosure inform suppliers that organisations have a Coordinated Vulnerability Disclosure policy and enable suppliers to align their own policies and organisations accordingly. This avoids any problems that prevent the desired, rapid reaction to vulnerability, as well as preventing the supplier taking civil law action against the reporter.

[2] The Dutch government's model for a whistleblower scheme for instance doesn't provide for the protection of employees in the event of a Coordinated Vulnerability Disclosure report by an employee.

### 3.2.2 Agreements with users

An organisation is responsible for managing sensitive customer and employee information such as pay slips, personnel files, etc. Agreements with employees as well as customers about the handling of this information and the associated rights and obligations may be recorded, for instance, in employment contracts, agreements with suppliers and customers and also in an Acceptable Use Policy (an employee and user guide on handling information sources). Since the reporter of a vulnerability may also access information on customers and employees, it is important to inform these parties about the possible impact of Coordinated Vulnerability Disclosure. Coordinated Vulnerability Disclosure may also be mentioned in these documents with a view to preventing disagreement or civil law actions between a customer/employee and a reporter.

### 3.2.3 External communication

Coordinated Vulnerability Disclosure is a means of lowering the threshold for reporting vulnerability and of establishing ground rules for investigating vulnerabilities. The reporter must be informed that the organisation has a Coordinated Vulnerability Disclosure policy. To this end the Coordinated Vulnerability Disclosure policy must be published and findable on the website.

Moreover, it is relevant for the organisation to maintain a good relationship with the reporter of a vulnerability. To this end, external communication is also important.

# 4 Consulting with stakeholders

When drawing up a Coordinated Vulnerability Disclosure policy various factors must be taken into account and the relevant agreements recorded. This chapter describes the chain structure of the Coordinated Vulnerability Disclosure process, definition of responsibility and decisions that need to be taken.

## 4.1 Chain structure

Implementation of Coordinated Vulnerability Disclosure is not limited to the organisation itself. A vulnerability report is often not only relevant to the organisation but also to parties with which the organisation deals. It is worthwhile consulting these parties before implementing Coordinated Vulnerability Disclosure. They may include:

- Providers of web hosting, cloud services, networking equipment, software licenses, etc.
- Employees via, for instance, the works council

## 4.2 Consultation with internal stakeholders

Consultation with stakeholders is important in order develop the most effective Coordinated Vulnerability Disclosure process. Before establishing policy and procedure the following groups must, in any event, be consulted (this can vary by company):

| Who | Why |
|---|---|
| Person responsible for handling ICT incidents (e.g. CERT/CSIRT) | The procedure for Coordinated Vulnerability Disclosure coincides closely with the handling of ICT incidents. The main role in handling a Coordinated Vulnerability Disclosure report will be often be taken by this party |
| Legal department | Coordinated Vulnerability Disclosure often carries legal implications as between the organisation and the reporter. Involving the legal department in the process can prevent the report having major consequences for the organisation or reporter. |
| Person responsible for data security (CISO) | The person responsible for data security is often also responsible for the Coordinated Vulnerability Disclosure process. |
| ICT Help desk | A help desk or service desk is often the first point of contact for employees experiencing computer problems. |
| Control | As in incident handling, mandating plays a major role. Authorisation to implement the correct intervention or reward a reporter is an essential requirement. |
| Communication department | Communication plays a major role in Coordinated Vulnerability Disclosure and can affect the image of the organisation. Communication between reporter and organisation, but also with users, employees, the ICT community and the outside world, should be properly coordinated. |

# 5 Implementing Coordinated Vulnerability Disclosure policy

Implementation of Coordinated Vulnerability Disclosure requires determining exactly how the organisation wishes to interpret the policy and procedure. A broad range of steps has been formulated to help specify the relevant decisions. These can be adapted to fit the implementation approach within the organisation.

## 5.1 Defining responsibilities

**As with any policy, it is important to allocate responsibilities for Coordinated Disclosure Vulnerability.**

Allocation of the following responsibilities is in any event essential to the success of Coordinated Vulnerability Disclosure:

- First determination of the seriousness and validity of the report
- Deciding how the report will proceed if the report appears serious (for example a leak of personal data)
- Monitoring the quality of the processing of the report
- Monitoring the time taken to process the report
- Communication with the reporter
- Determine the timing of release of the (individual) report
- Allocating the reward
- Approval for publication
- Overall responsibility for the Coordinated Vulnerability Disclosure process

When allocating responsibilities, pay special attention to communication between the various layers of the organisation. It has happened in practice that a reporter has contacted the press in order to publish a vulnerability, after making a Coordinated Vulnerability Disclosure report. This is a result of poor coordination of the communication between a number of departments. This can result in the organisation being unsure about where a report was received and how it was subsequently processed.

## 5.2 Scope of Coordinated Vulnerability Disclosure policy

**Determine which of your organisation's products and services are covered by the policy.**

*For consideration:*

Inclusion of all applications and infrastructure in the scope can result in a large number of reports. Restrictions, such as 'only web applications', can exclude important findings relating to offline applications, for example.

## 5.3 Type of report

### 5.3.1 Method of receipt

**Determine how your organisation wants to receive reports.**

For instance:

- E-mail
- By post
- Digital form (whether or not via SSH)
- Telephone

*Consideration(s):*

Digital forms can force reporters to provide information, such as contact details.

This can raise the threshold to making a report. There is a lower threshold to reporting via email and telephone. The necessity for email encryption, however, once again raises the threshold for some reporters.

Reports regarding vulnerabilities in systems containing confidential information should be handled confidentially. Encryption of information exchange, in accordance with the data security policy, is then often necessary.

### 5.3.2 Anonymous - or not?

**Decide whether reporting may take place anonymously.**

Options:

- The report may be delivered anonymously, under a pseudonym or via an intermediary/confidential counsellor
- Reports under pseudonym, made anonymously or made via intermediary/counsellor are not acceptable
- Reports may be made anonymously or under a pseudonym. Reports via an intermediary/counsellor are neither permitted nor processed
- Reports are only accepted when contact is possible, whether under pseudonym or fully identified

*Consideration(s):*

Anonymous reporting may impede communication, with uncertainty preventing coordination, reward and information exchange. Anonymity may also prevent or complicate detection in the event of violation of the rules of Coordinated Vulnerability Disclosure policy. Finally, an anonymous report may not deliver an accurate impression of the person behind the report, making it difficult to judge the reporter's intentions.

An advantage of anonymous reporting is the low threshold for the reporter. This prevents a reporter who wants to remain anonymous from approaching the press or opting for full disclosure.

### 5.3.3 Speed of confirmation

**Determine how quickly your organisation should send an acknowledgment of receipt of the report to the reporter.**

Options:

- Within 1 working day
- Within 2 working days
- Within 3 working days
- Within a week

*For consideration:*

A quick reaction to the report gives the reporter the impression that the report has been taken seriously. Obliging the organisation to react quickly can stimulate more rapid processing of reports. Contact with the press or full disclosure can be prevented if the reporter feels he is being taken seriously.

## 5.4 Waiving prosecution

**Determine whether the organisation will waive prosecution if the reporter has complied with the rules of the Coordinated Vulnerability Disclosure policy**.

Options:

- Yes or No

*For consideration:*

An explicit statement of waiver of prosecution, in the policy, may reassure the reporter and increase the likelihood of a report being made. However, it is important to state clearly that the organisation may nevertheless be obliged to take legal action.

If this is not explicitly stated, the risks of obligatory legal action and conflict with the Coordinated Vulnerability Disclosure policy are reduced.

In principle, the organisation's standpoint should be that prosecution is waived if there is compliance with the rules.

## 5.5 Reports that impact third parties

**Determine how your organisation should react when a report within your system also impacts the system of a third party which does *not* have a Coordinated Vulnerability Disclosure policy.**

Alternative ways to react:

- Consult with the reporter on the action to be taken
- Your organisation mediates between the reporter and potentially affected party
- The report must be passed on by your organisation to the potentially affected party

*Consideration(s):*

When the reporter is involved in the decision on further steps to be taken, the responsibility remains with the reporter and the choice of contacting the third party is up to him/her.

Mediation between the organisation and the potentially affected party carries a social responsibility towards the reporter, that any reported problem will be resolved - and towards the third party, that its potential problem will be reported.

The problem can be resolved quickly if the message is passed to the potentially affected party. However, the decision whether to maintain the reporter's anonymity must still be made.

**Determine how your organisation is to act in the event that a reporter finds a vulnerability in the system of a third party and reports this to your organisation.** Does this mean that the Coordinated Vulnerability Disclosure process is halted as the report does not apply to your organisation's systems?

Alternative ways to react:

- Consult with the reporter on the action to be taken
- Your organisation mediates between the reporter and the potentially affected party
- The report must be passed on by your organisation to the possibly affected party

*Consideration(s):*

When the reporter is involved in the decision on further steps to be taken, the responsibility remains with the reporter and the choice of contacting the third party is up to him/her.

Mediation between the organisation and the potentially affected party carries a social responsibility towards the reporter, that any reported problem will be resolved - and towards the third party, that their potential problem will be reported.

The problem can be resolved quickly if the message is passed to the potentially affected party. However, the decision whether to maintain the reporter's anonymity must still be made.

## 5.6 Impose limitations

**Determine how far the reporter may go in his investigation.**

Alternative courses of action:

- You explicitly state what is and is not permitted
- You provide a clear guideline, with which the reporter must comply
- You provide no guideline

*For consideration:*

Rules that explicitly state what is and is not allowed may thwart the reporter. The reporter may feel restricted and, if he has acted in breach of the rules (without causing damage), may decide not to report - to avoid the possibility of prosecution. This does, however, create clear, quantified rules and contributes to managing expectations.

Clarity can also be provided by means of a guideline with which the reporter must comply. This does not impose any strict rules but, for example, requires the reporter not to modify or delete any data and may impose certain restrictions.

In the absence of any guideline, misunderstanding may arise regarding what is reasonable. While the reporter is free to identify and report all vulnerabilities.

## 5.7 Rewarding the reporter

**Determine whether the reporter should be rewarded.**

Alternatives are:

- Yes, by means of a reward in money or vouchers
- Yes, in kind, for instance a t-shirt, tour of your organisation, seminar or invitation to a presentation
- Yes, with a place in our organisation's Hall of Fame
- No - no reward
- Etc….

*For consideration:*

The potential financial implications for the organisation must be considered.

Paying a monetary reward increases the chance of reporters with financial motivations. This means more reports, which also cost the organisation more money and time. The chance of receiving useful, high quality reports is, however, increased.

In fact, ethical reporters are often motivated by social interests or to build good reputation. This could mean that a non-financial reward increases the chances of only getting ethical reports.

### 5.7.1 Personal data

**Determine how to handle reports of vulnerabilities through which personal data has been obtained.**

An explicit prohibition on obtaining personal data may stop a report, if the reporter unintentionally obtained personal data in the process of detecting a leak.

Your organisation's choices in this situation:

- Your organisation cannot permit this, at any time. If personal data is taken the reporter is charged, in any event
- Handle the report in the normal way, taking the legal obligations to report to the authorities into account
- Look at it case by case - for instance if there's no evidence of forced entry, but only faulty software, the reporter can't be blamed

*For consideration:*

An explicit prohibition on obtaining personal data may stop a report, if the reporter unintentionally obtained personal data in the process of detecting a leak.

### 5.7.2 Agreements with third parties

**Determine whether agreements should be made with suppliers and/or users with regard to Coordinated Vulnerability Disclosure.**

*For consideration:*

Supplier support may be needed in order to remedy a vulnerability. Moreover, a vulnerability may be reported in a supplier's system. It is therefore advisable to make arrangements with suppliers in advance - regarding, for example, the time required to remedy vulnerabilities.

It is possible that reporters will gain access, in the course of an investigation, to a system's user data - such as that of your employees. It may therefore be useful to make agreements or in any event to inform the users of the Coordinated Vulnerability Disclosure policy in force.

# 6 Coordinated Vulnerability Disclosure implementation plan

A broad description of the stages of a typical organisation's implementation project:

1. **Determine the organisation's state of readiness**
   Coordinated Vulnerability Disclosure is only successful if an organisation can properly react to a vulnerability report. The lack of an IT incident procedure, or lack of mandate to shut down products or services can be signs that an organisation is not yet ready for Coordinated Vulnerability Disclosure. A reporter may choose to reveal a vulnerability via the media or full disclosure if an organisation cannot adequately handle reports.
2. **Determine decision points**
   The application of a Coordinated Vulnerability Disclosure policy can affect the image of an organisation. Chapter 5 of this document outlines the important decision points - such as scope, permitted approaches and reporter rewards.
3. **Reaching agreement with stakeholders (suppliers, employees/users, legal, communication, etc.)**
   The introduction of a Coordinated Vulnerability Disclosure policy affects the organisation, those related to the data and the relevant suppliers of services, hardware and software. In relation to the possible impact of Coordinated Vulnerability Disclosure on them, it is good to consult with these parties on its introduction.
4. **Drawing up Coordinated Vulnerability Disclosure policy and procedure**
   The organisation can draw up policy and procedure using the "model Coordinated Vulnerability Disclosure policy and procedure".
5. **Presentation to the management of the organisation**
   Coordinated Vulnerability Disclosure may affect the way an organisation is structured. It is also important that the person charged with implementing Coordinated Vulnerability Disclosure is sufficiently mandated to carry out the required actions. Appendix A contains a management summary to be used in presenting Coordinated Vulnerability Disclosure to the board of an organisation.

6. **Internal communication policy and procedure**
   As Coordinated Vulnerability Disclosure involves various internal parties such as the ICT department, the legal department and communication, there should be clarity as to the allocation of responsibilities and how to act. Mentioning Coordinated Vulnerability Disclosure during staff awareness training can be useful as it increases data protection awareness and, potentially, early recognition of vulnerabilities.
7. **Practice report**
   A practice report enables measurement of aspects such as mandate, timely handling, communication and cooperation between the various actors.
8. **Evaluation**
   The results of the practice report can be used to effect any necessary adjustments to the policy and procedure.
9. **Publishing the Coordinated Vulnerability Disclosure policy**
   The Coordinated Vulnerability Disclosure policy must clearly visible to reporters. This could be achieved by means of an extra link on the contact page or a reference on the security page of a website.

# Appendix A: Template, offer letter

The Coordinated Vulnerability Disclosure policy is based on the Guidelines for Responsible Vulnerability Disclosure, that were published in 2013 by the National Cyber Security Centre in the Netherlands, and the best practices of government and the financial and telecommunications sectors.

## What is Coordinated Vulnerability Disclosure Policy?

There are several ways for reporters to communicate ICT vulnerabilities. A vulnerability can be communicated directly to the public (full disclosure) or it can be handled in a more private and responsible way (Coordinated Vulnerability Disclosure). Coordinated Vulnerability Disclosure is a strategy aimed at solving and remedying a vulnerability and preventing exploitation of that vulnerability. It can be anchored in policy.

An organisation clarifies what is expected from both a reporter and from the organisation itself by drawing up a policy for responsible reporting of ICT vulnerabilities. The policy indicates how far the reporter may go in investigating a vulnerability and that the organisation waives legal action provided there is compliance with the rules set by the policy. Reporter and organisation thus know what to expect of each other.

## Why a Coordinated Vulnerability Disclosure policy?

An ethical hacker investigating a vulnerability can easily find himself in conflict with the Dutch Computer Crime Act. This law does not take into account the ethical motives of the reporter and how far a reporter may go is often not clearly defined. This raises the threshold for a reporter intending to report a vulnerability to an organisation. Reporters may then choose to report a vulnerability anonymously, via the press, in order to protect their information source. Reporting via the press can enable the vulnerability to be exploited, and result in damage to the image of the organisation.

At the end of 2012 the Dutch minister of Security and Justice drew up a 'Guide to developing the practice of Coordinated Vulnerability Disclosure'. This is a guideline for the establishment of a policy for responsible disclosure of ICT vulnerabilities. The Dutch Ministry of Security and Justice has indicated that

Coordinated Vulnerability Disclosure is primarily a matter between the reporter and the organisation concerned[3]. Moreover, the public prosecution service has published an internal policy document, in line with the Coordinated Vulnerability Disclosure guideline. There is no legislation that directly provides for Coordinated Vulnerability Disclosure. Organisations are therefore considered responsible for drawing up their own Coordinated Vulnerability Disclosure policies. This proposal provides for the implementation of such policy.

A short summary of the procedure that forms part of Coordinated Vulnerability Disclosure policy:

Reports of ICT vulnerabilities are received by <<*CERT*>> and sent through to the <<*Security officer*>>. The <<*Security Officer*>> evaluates the report and remedies the vulnerability, if necessary in consultation with the reporter. In the case of a serious vulnerability or a leak of personal data the <<*Corporate Security Officer*>> is involved in the process. Any breach of the rules is legally reviewed. During the investigation the reporter is regularly informed of progress. The <<*Organisation*>> decides if the reporter qualifies for (financial) reward. The decision as to whether the vulnerability is made public is then made, in consultation with the reporter.

The following may be considered in addition to the arguments already listed in favour of the implementation of a Coordinated Vulnerability Disclosure policy for <<*Organisation*>>:

*Reduce the disclosure threshold*
An organisation can lower the threshold for the reporting of vulnerabilities by its target audience. It is more likely that investigators will recognise and want to responsibly report an ICT vulnerability in the absence of legal complications.

*Transparency*
The transparent conduct of the <<*Organisation*>> is in line with its social responsibilities. By publishing a Coordinated Vulnerability Disclosure policy, the <<*Organisation*>> demonstrates its standpoint on this issue.

*Social importance*

[3] This may well be different in other countries, so check this please!

ICT has a growing influence on society. The potential impact of vulnerabilities on users is significant. A key driver for reporters in exposing vulnerabilities and risks is public interest. Coordinated Vulnerability Disclosure is a socially responsible and effective solution for dealing with ICT vulnerabilities.

"De vereniging van ICT eindverantwoordelijken in grote organisaties van de vraagzijde"

www.cio-platform.nl