Policies around vulnerability and patch management

 Template

# Using this document

* This policy was drafted so that the document can be used for the 3 different **CyFun** assurance levels. (**Basic**, **Important**, **Essential**)
* The needs required to meet a certain level of assurance will be made clear by indicating the proposed text in the colour mentioned above.

Content

[Using this document 2](#_Toc160457572)

[Authority and review 3](#_Toc160457573)

[Document control and review 3](#_Toc160457574)

[Version management 3](#_Toc160457575)

[Intro 4](#_Toc160457576)

[Managing vulnerabilities 4](#_Toc160457577)

[Risk assessment 4](#_Toc160457578)

[Scanning for internal vulnerabilities 4](#_Toc160457579)

[Scanning for external vulnerabilities 4](#_Toc160457580)

[IDS/IPS 5](#_Toc160457581)

[Policy for Coordinated Disclosure of Vulnerabilities CVDP (Important, Essential) 5](#_Toc160457582)

[Patch management 5](#_Toc160457583)

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document check**  |  |
| Author  |  |
| Owner |  |
| Date created |  |
| Last revised by  |  |
| Last revision date |  |

.

## Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date of approval** | **Approved by**  | **Description of change** |
|  |  |  |  |

# Intro

A vulnerability is a flaw or weakness, a design or implementation error, lack of updates in the light of existing technical knowledge, that can compromise the security of information technologies. A vulnerability can lead to an unexpected or unwanted event and be exploited by malicious third parties to violate the integrity, authenticity, confidentiality or availability of a system or to harm a system. More than 90% of malware infections or cybercrimes start with the exploitation of a known leak. Especially systems that allow incoming connections to the Internet, such as web servers and e-mail servers, face numerous attacks every day.

Therefore, it is vital that we eliminate as many known vulnerabilities as possible. For this, we need a good patch management system and vulnerability monitoring.

This policy document is part of a set of policy documents that **support [Organisation]** in establishing a sound cybersecurity strategy.

# Managing vulnerabilities

## Risk assessment

**[Organisation]** conducts an annual risk assessment that determines risk based on threats, vulnerabilities and impacts on business processes and assets. These vulnerabilities refer to a weakness in [Organisation]'s hardware, software or procedures.

## Scanning for internal vulnerabilities

Critical and confidential systems should be scanned for vulnerabilities at least **annually**, **quarterly**, **continuously**. Highly critical and highly confidential systems should be scanned at least monthly.
Vulnerability scanning tools or penetration tests\* can be used to investigate the vulnerabilities of systems. These tools contain a database of known vulnerabilities and can scan a single system or even an entire network for vulnerabilities. Scanning tools only scan vulnerabilities to which they have access. For example, if services are blocked by firewalls, it cannot report on them.

The tools classify weaknesses into different levels of risk. However, be aware that the highest risk is when the vulnerability can be exploited from the internet. If this is not the case, it is still a risk as it can be used by an infected system to spread malware to other machines on the network, but the probability is lower.

## Scanning for external vulnerabilities

In addition to the internal scan, an external vulnerability scan (pen test) should be performed **annually, quarterly**, **continuous scanning**. The results of this external pen test should form the basis for an annual, 6-monthly, monthly vulnerability improvement plan and also serve as an independent measure of system security.

## IDS/IPS

While vulnerability scanners are used to detect potential risks, intrusion detection (IDS) and intrusion prevention (IPS) systems provide real-time network monitoring to see if malicious actions are taking place. IDS systems can send an alert the moment suspicious behaviour is noticed. IPS can even take action, for example by blocking traffic in the firewall.

 IDS/IPS should be considered for critical and confidential systems if the risk outweighs the cost.

## Policy for Coordinated Disclosure of Vulnerabilities CVDP (Important, Essential)

Organisations pursuing the CyFun assurance level **Important** or **Essential** should establish a coordinated vulnerability disclosure policy.

This is a set of rules predetermined by [Organisation] responsible for information systems that allows participants (or "ethical hackers"), with good intentions, to detect possible vulnerabilities in its systems, or to provide it with any relevant information about them. These rules, usually made public on a website, allow for the establishment of a legal framework for cooperation between the responsible organisation and policy participants. Among other things, these rules should guarantee the confidentiality of the information exchanged and frame any disclosure of discovered vulnerabilities in a responsible and coordinated manner.

Please refer to the Guide on the Coordinated Vulnerability Disclosure Policy prepared by the Centre for Cybersecurity Belgium when preparing this CVDP.

[\*https://en.wikipedia.org/wiki/Penetration\_test](https://en.wikipedia.org/wiki/Penetration_test)

# Patch management

All managed servers, firewalls, switches and clients should be updated with the latest relevant patches at least every 2 months, unless explicitly decided otherwise.

Security patches should be installed as soon as possible. This can only be done after a thorough impact analysis on the environment of the patch to be installed.

There must be a system or process to know which security patches are available and applicable.

Security patches include those of operating systems, server software such as databases and services and applications.

**NOTE:** If a system is unable to apply security patches, even though vulnerabilities are known, the system should be isolated from the Internet and other systems connected to the Internet and physically secured.