**Technical Vulnerability**

**Management Policy**

**Security Classification: Protected**

**Document Ref. ISMS18015**

**Version: 1.0**

**Draft 1**

**Document Author: Cybersecurity Unit**

**Document Owner: NCS/ TMP**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Change Number** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Review**

|  |
| --- |
| **Date of Next Scheduled Review** |
|  |

Distribution

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

**Contents**

[1 Introduction 5](#_Toc379371165)

[1.1 Risks Addressed 5](#_Toc379371166)

[1.2 Scope 5](#_Toc379371167)

[1.3 Related Documents 5](#_Toc379371168)

[1.4 Purpose 5](#_Toc379371169)

[2 Technical Vulnerability Management 6](#_Toc379371170)

[2.1 The Threat 6](#_Toc379371171)

[2.2 What is a Technical Vulnerability? 7](#_Toc379371172)

[2.3 Sources of Information 7](#_Toc379371173)

[2.4 Patches and Updates 8](#_Toc379371174)

[2.5 Vulnerability Assessment 8](#_Toc379371175)

[2.6 Hardening 9](#_Toc379371176)

[2.7 Awareness Training 9](#_Toc379371177)

# Introduction

## Risks Addressed

This document describes a control that was identified in [ISMS06004 Information Security Risk Treatment Plan](../06.%20Planning/ISMS06004%20Information%20Security%20Risk%20Treatment%20Plan.doc) to address the following risks:

|  |  |
| --- | --- |
| **Reference** | **Description of Risk** |
|  |  |
|  |  |
|  |  |

## Scope

This control applies to all systems, people and processes that constitute the Project Management Office (PMO)information systems, including management, employees, and other third parties who have access to Project Management Office (PMO)systems.

## Related Documents

The following policies and procedures are relevant to this document:

* [ISMS12002 Mobile Computing Policy](../A6.%20Organisation%20of%20information%20security/ISMS12002%20Mobile%20Computing%20Policy.doc)
* [ISMS12003 Teleworking Policy](../A6.%20Organisation%20of%20information%20security/ISMS12003%20Teleworking%20Policy.doc)
* [ISMS12004 Bring Your Own Device Policy](../A6.%20Organisation%20of%20information%20security/ISMS12004%20Bring%20Your%20Own%20Device%20Policy.doc)
* [ISMS13001 AUP and Personal Commitment Statement](../A7.%20Human%20resources%20security/ISMS13001%20AUP%20and%20Personal%20Commitment%20Statement.doc)
* [ISMS13002 Email Policy](../A7.%20Human%20resources%20security/ISMS13002%20Email%20Policy.doc)
* [ISMS13003 Internet Acceptable Use Policy](../A7.%20Human%20resources%20security/ISMS13003%20Internet%20Acceptable%20Use%20Policy.doc)
* [ISMS18004 Change Management Policy](ISMS18004%20Change%20Management%20Policy.doc)
* [ISMS18008 Software Policy](ISMS18008%20Software%20Policy.doc)
* [ISMS18010 Anti-Malware Policy](ISMS18010%20Anti-Malware%20Policy.doc)

## Purpose

This document sets out the Project Management Office (PMO)policy on how the Service will assess and manage technical vulnerabilities within the IT environment. Its intended audience is IT and information security management and NCS Cybersecurity Unit who will implement and maintain the organisation’s defences.

# Technical Vulnerability Management

What is a Technical Vulnerability?

A vulnerability is defined in NIST Special Publication 800-30 Rev 1 as “an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source.”

The software development process is complicated and its output in the form of software programs is rarely bug free. Most of these bugs simply affect the functionality of the software so that it doesn’t work as intended. However, if manipulated in the correct way, some can allow an attacker to gain some form of advantage or access which was not intended by the developer. This type of bug is commonly considered to be a software vulnerability.

These vulnerabilities are constantly being found and corrected via software updates or patches. Unfortunately, it is not always the developer or user who discovers these vulnerabilities. When discovered by a potential attacker the vulnerability becomes something to be exploited for gain and kept secret for as long as possible. A newly discovered vulnerability is often referred to as a “zero-day exploit” and is difficult to defend against.

PMO policy with respect to technical vulnerabilities is to be aware of them and to close them where possible, either directly or via other means.

## The Threat

Malware is any code or software that may be harmful or destructive to the information processing capabilities of the Service and is one of the primary tools used by attackers to circumvent security to make some kind of gain or to disrupt the normal operation of the business.

It is essential that effective precautions are taken by the Project Management Office (PMO) to protect itself against these threats which can come from several sources including organised groups, politically motivated groups, rogue employees, nation state sponsored “cyber-warfare” units or simply individuals exercising curiosity or testing their skills.

Whatever the source, the result of a successful security breach is that the PMO and its stakeholders are affected, sometimes seriously, and harm is caused.

Malware comes in many forms and is constantly changing as previous attack routes are closed and new ones are found. The most common types of malwares found today are:

* Virus
* Trojan
* Worm
* Logic bomb
* Rootkit
* Keylogger
* Backdoor

Often these types of malwares will be used in combination with each other.

For malicious software to carry out its intended purpose it needs to be installed on the target device or computer. There are a number of keyways in which malware infects computers and networks, although new ways are being created all the time.

The most common infection techniques are as follows.

* Phishing
* Websites and Mobile Code
* Removable Media
* Hacking

But for these techniques to be used by an attacker, they must take advantage of a Vulnerability in our defences.

## Sources of Information

The first step in managing technical vulnerabilities is to become aware of them. Since we are talking about technical vulnerabilities these will of course depend upon the technology employed within the Service. It is necessary then to gain a full appreciation of the technology components that make up the Service’s infrastructure and their versions (since most technical vulnerabilities are very version-specific).

This should include:

* Operating systems e.g. Windows, LINUX
* Databases e.g. SQL Server, MySQL
* Web servers e.g. IIS, Apache
* Desktop software e.g. Office, Acrobat
* Web technologies e.g. Flash, Java
* Application software e.g. SAP, Agresso
* Hardware e.g. servers, routers

This information should be available from the organisation Configuration Management Database (CMDB) and [ISMS18014 Software Catalogue](ISMS18014%20Software%20Catalogue.doc).

Information about vulnerabilities with any of the above components is generally available from the vendor who will issue updates and patches to fix those that it becomes aware of.

A process should therefore be put in place to ensure that all relevant information about updates is being received and reviewed by competent staff members. This will usually give guidance about the level of urgency associated with each update.

Where configuration changes are recommended to close off vulnerabilities, these should be actioned through the Service’s change management process so that appropriate controls are in place for testing, risks assessment and backout.

## Patches and Updates

Patches and updates will typically be issued by software vendors on a regular schedule as cumulative packages. These will be linked to the specific version of software that they relate to and may have dependencies stipulated with other software modules, products or operating systems.

Procedures should be put in place to obtain copies of the software updates electronically when they are issued by the vendor. The scheduling of the installation of updates will depend upon a few factors including:

* The criticality of the systems being updated.
* The expected time taken to install the updates (and requirements for service outages to users).
* The degree of risk associated with any vulnerabilities that are closed by the updates.
* Co-ordination of the updating of related components of the infrastructure
* Dependencies between updates.

An update release plan should be created and maintained to keep track of when various system will be updated, considering the factors listed above. The plan must be managed through the change management process. For updates that are low risk and regular, a standard change may be defined within the change management process to allow this to happen without excess administrative overhead (see [ISMS18004 Change Management Policy](ISMS18004%20Change%20Management%20Policy.doc)).

## Vulnerability Assessment

In addition to the regular application of vendor-supplied software updates, Project Management Office (PMO)will conduct a vulnerability assessment at least twice a year. The focus of the vulnerability assessment should be guided by the most recent risk assessment.

The purpose of this assessment is to identify existing vulnerabilities in systems that could be exploited by an attacker. These could include known software vulnerabilities that have not been patched, configuration errors that need to be corrected or examples of inadequate security practice that need to be addressed.

The assessment may be carried out in-house, by an external company or a combination of both and as a minimum should cover:

* Assessment of the security of all routes into the Service’s internal network from the Internet.
* Externally facing web servers.
* Business critical servers on the internal network.
* A selection of typical user computers.

If resources permit, additional areas should be assessed such as the vulnerability of employees to phishing attacks.

It is not the Service’s policy to attempt to exploit the vulnerabilities found as a matter of course. This type of penetration test may be commissioned as required using external specialist resources as part of a carefully planned exercise performed outside of normal business hours.

## Hardening

A further action that should be taken to reduce the number and extent of vulnerabilities within Project Management Office (PMO)ssystems is the hardening of server and other device configurations. This involves the shutting down of services and protocols that are not needed so that the attack surface is reduced.

These hardening activities should be carried out according to vendors’ guidelines and under the control of the change management process.

## Awareness Training

As a result of vulnerability assessment it may be necessary to increase efforts in security awareness training for employees and third-partiesS. This training should explain the nature of vulnerabilities and what can be done to reduce them.