SECURITY CONSULTANTS

REMOVABLE MEDIA POLICY

Contents

1 Overview

1.1 Risk to IL7

Removable media devices represent a risk to business-critical information on which IL7 depends for its business. Removable media is any type of portable storage device that can hold data, including (but not limited to) CDs, DVDs and USB drives.

These devices are often capable of running applications and/or have large data storage capabilities, giving the user the ability to import unauthorised data, unlicensed software, malicious code, games, screensavers and other inappropriate material. In addition, they can be used to remove information from IL7 Security systems, potentially leading to data leakage if removable media is lost or stolen, or as a result of a malicious insider. This could lead to significant negative impacts to the IL7 Security's business operations and individuals affected, as well as negatively impacting the reputation of the organization. It could also expose the IL7 Security to financial penalties from the Information Commissioners Office if personal information is involved or lead to a Parliamentary investigation if sensitive or valuable data is compromised. Therefore, in order to support the use of removable media, appropriate controls need to be in place to ensure that security is maintained.

1.2 Purpose

This Policy sets out the requirements by which the IL7 Security shall ensure the secure and authorised use of removable media in order to minimise the risks to the IL7 Security.

1.3 Scope

This Policy covers any portable device capable of running an application or storing data. This Policy applies to all removable media used, owned and/or maintained by the IL7 Security. Types of removable media covered by this policy include, but are not limited to:

- Optical discs, including CDs, DVDs and Blu-Ray discs.
- Floppy discs.
- Flash memory storage devices, including CompactFlash cards, SD cards and USB memory sticks.
- External hard drives.
- Zip drives.
- Magnetic tapes.

Note that mobile devices with their own storage capacity, such as mobile phones and laptops, are covered in a separate Mobile Device Policy. Therefore, no specific requirements relating to the use of a mobile device to transfer information are included within this policy.

1.4 Applicability

This policy applies to all IL7 systems and projects, including those systems delivered by third parties on behalf of the IL7.

2 Removable Media Policies

The following requirements relating to removable media will be adhered to at all times to ensure the protection of IL7 Security information technology resources.

2.1 Policy and Controls

• SP09	End User Devices (Ref [2])
• SP12	Unauthorised Release (Ref [3])
• SP15	Access Control (Ref [4])

This Policy is one of several that are required to support principles above.
This Policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 [5]:

• MP-1	Media Protection Policy and Procedures.
• MP-2	Media Access.
• MP-3	Media Marking.
• MP-4	Media Storage.
• MP-5	Media Transport.
• MP-6	Media Sanitization.
• MP-7	Media Use.
• MP-8	Media Downgrading.

This policy represents IL7 Security's compliance with NIST Control MP-1.

2.2 Security Requirements

Policy ID	Policy Requirement
2.2.1	The use of removable media with IL7 Security systems is limited according to legitimate business need, as per NCSC guidance/
2.2.2	Only removable media devices supplied via IL7 Security are attached to the IL7 Security environment: no personally owned devices may be used. [NIST MP-7]
2.2.3	Removable media devices are attached to IL7 Security environment for specific business purposes only, and their issue and justification for issue shall be recorded. [NIST MP-2]
2.2.4	Removable media is encrypted in accordance with the Encryption Policy. [NIST MP5 (4)]
2.2.5	*Use of removable media to transport information is authorised, based on strong business need and security assessment by IL& Security and the Information Owner prior to issue.*
2.2.6	Issue removable media to named individuals only, explicitly authorised for use as per 2.2.5 for the period required to perform necessary business. Usage must be recorded and audited.
2.2.7	All IL7 Security-owned removable media are numbered, labelled and recorded in an asset register including issue status, which must be checked regularly and kept up to date. Marking of removable media must not indicate that it is IL7 Security owned. [NIST MP-3]
2.2.8	Loss or suspected loss of removable media is raised as an incident as per Security Incident Management Policy (Ref [8]).
2.2.9	Securely erase data in line with the Secure Data Erasure Policy [NIST MP-6, 8]

2.3 Configuration Requirements

IL7 System Designers and Administrators responsible for the design and configuration of IL7 Security systems shall:

Policy ID	Policy Requirement
2.3.1	Design and configure IL7 Security systems to manage and use removable media in accordance with NCSC guidance.
2.3.2	Design systems in a manner that allows control over whether: Removable media can be accessed by the system. The system can be accessed by removable media. [NIST MP-4]
2.3.3	Not permit the use of removable media to store PCI-DSS cardholder data, other than backup tapes and designated backup storage area network (SAN). [NIST MP-7].

2.4 User Responsibilities

Policy ID	Policy Requirement
2.4.1	Where legitimate business need requires data to be transferred with removable media: Review and gain approval for what is being transferred with the information owner, providing the data type, file size, media type, method of transportation, and recipient of the media. Review the risks and agree security controls with IL7 Security (including monitoring of information transfer, encryption, password protection, physical security, packaging used to transport device, secure courier etc.). Obtain written approval from the information owner and IL7 Security regarding the agreed security controls. Adhere to all other policy statements within this document [NIST MP-5, MP-7]
2.4.2	Apply physical transport security controls over the removable media, suitable for the classification of the data that it holds. This includes: Two-person controls. Accountability. Restricting locations or transport (e.g. not leaving the UK). [NIST MP-5]
2.4.3	Do not connect removable media that has been used on an unassured system to a IL7 Security device/system without authorisation and adequate precautions (e.g. antivirus checking), in accordance with the Malicious Code Protection Policy (Ref [10]). [NIST MP-2, MP-7]
2.4.4	Use backup tapes in accordance with the Backup and Restore Policy (Ref [11]).
2.4.5	Keep all removable media devices physically secured in line with the classification of information held on the device and deny access to unauthorised individuals. [NIST MP-2, MP-4]
2.4.6	Treat IL7 Security storage devices entrusted to them appropriately (e.g. not exposed to excessive heat or cold) in accordance with manufacturer's guidelines.
2.4.7	Do not use removable media devices to: Load non-work related data onto IL7 Security systems e.g. music, videos, pictures, games or any illegally sourced copyrighted material. Illegally copy material protected under copyright law or make that material available to others for copying. Run non-IL7 Security-approved applications or to disable/bypass installed security mechanisms. Copy corporate data that is not relevant to their job function; Copy company confidential data or external client information for provision to an external source. [NIST MP-7]

3 Exemptions, Exceptions and Breaches

3.1 Exemptions and Exceptions Policy

All IL7 systems and personnel must make every effort to comply with the entirety of the policy set, however, in the case that either some aspect of the policy set is not applicable, or that a system or member of staff is unable to comply with it, refer to the IL7 Security Manager,

3.2 Breach of Policy

The IL7 reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this Policy. IL7 members of staff or contractors who breach this Policy may be subject to disciplinary action, including suspension and dismissal as provided for in the IL7 Disciplinary Procedure.

Breaches of this Policy by a third-party-managed service provider may lead to the withdrawal of IL7 information technology resources to that third-party service provider and/or the cancellation of any contract(s) between IL7 and the third-party service provider.

The IL7 will refer any use of its IT resources for illegal activities to the Police.