National Cyber Security Centre
a part of GCHQ

Guidance (/)

10 Steps: Removable Media Controls

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)
This section from within the NCSC's '10 Steps To Cyber Security' concerns Removable Media Controls.

Summary

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

What is the risk?

Removable media introduces the capability to transfer and store huge volumes of sensitive information as well as the ability to import malicious content. The failure to manage the import and export of information using removable media could expose you to the following risks:

- **Loss of information:** Removable media is very easily lost, which could result in the compromise of large volumes of sensitive information stored on it. Some media types will retain information even after user deletion, placing information at risk where the media is used between systems (or when the media is disposed of)
- **Introduction of malware:** The uncontrolled use of removable media can increase the risk of introducing malware to systems.
- **Reputational damage:** The loss of media can result in significant reputational damage, even if there is no evidence of any specific data loss.

How can the risk be managed?

Produce corporate policies: Develop and implement policies and solutions to control the use of removable media. Do not use removable media as a default mechanism to store or transfer information. Under normal circumstances information should be stored on corporate systems and exchanged using appropriately protected mechanisms.

Limit the use of removable media: Where the use of removable media is required to support the business need, it should be limited to the minimum media types and users needed. The secure baseline build should deny access to media ports by default, only allowing access to approved users.

Scan all media for malware: Removable media should be automatically scanned for malware when it is introduced to any system. The removable media policy could also require that any media brought into the organisation is scanned for malicious content by a standalone machine before any data transfer takes place.

Formally issue media to users: All removable media should be formally issued to individual users who will be accountable for its use and safe keeping. Users should not use unofficial media, such as USB sticks given away at conferences.

Encrypt information held on media: Sensitive information should be encrypted at rest on media. If encryption is not employed then appropriate physical protection of the media is critical.

Actively manage the reuse and disposal of removable media: Where removable media is to be reused or destroyed then appropriate steps should be taken to ensure that previously stored information will not be accessible. The processes will be dependent on the value of the information and the risks posed to it and could range from an overwriting process to the physical destruction of the media by an approved third party. For more information refer to Secure sanitisation of storage media(/guidance/secure-sanitisation-storage-media).

Educate users and maintain awareness: Ensure that all users are aware of their personal responsibilities for following the removable media security policy.

Learn more

- Our End User Devices Security Guidance(/guidance/end-user-devices-security-guidance-introduction-0) provides help on the effective configuration of popular platforms.
- The Secure sanitisation of storage media(/guidance/secure-sanitisation-storage-media) guidance provides help on appropriate sanitisation and disposal of media.

Further reading

Secure sanitisation of storage media(/guidance/secure-sanitisation-storage-media)

Topics

Secure storage(/topics/secure-storage)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No