Removable Media and Cloud Storage Policy

Fusion-IT

February 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.7

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This removable media, cloud storage and Bring Your Own Device (BYOD) policy defines the objectives, requirements and implementing instructions for storing data on removable media, in cloud environments, and on personally-owned devices, regardless of data classification level.

b. This policy applies to all information and data within the organization's information security program, as well as all removable media, cloud systems and personally-owned devices either owned or controlled by the organization.

c. This policy applies to all users of information systems within the organization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily available to all users.

2 Background

a. This policy defines the procedures for safely using removable media, cloud storage and personally-owned devices to limit data loss or exposure. Such forms of storage must be strictly controlled because of the sensitive data that can be stored on them. Because each of these storage types are inherently ephemeral or portable in nature, it is possible for the organization to lose the ability to oversee or control the information stored on them if strict security standards are not followed.

b. This document consists of three sections pertaining to removable media, cloud storage, and personally-owned devices. Each section contains requirements and implementing instructions for the registration, management, maintenance, and disposition of each type of storage.

c. Within this policy, the term sensitive information refers to information that is classified as RESTRICTED or CONFIDENTIAL in accordance with the Data Classification Policy (reference (a)).

3 References

a. Data Classification Policy

b. Asset Inventory

c. Security Incident Response Policy

d. Encryption Policy

4 Policy

a. *Removable Media*

    i. All removable media in active use and containing data pertinent to the organization must be registered in the organization's Asset Inventory (reference (b)).

    ii. All removable media listed in reference (b) must be re-inventoried on a quarterly basis to ensure that it is still within the control of the organization.

        1. To re-inventory an item, the owner of the removable media must check in the item with the organization's Information Security Manager (ISM).

        2. The ISM must treat any removable media that cannot be located as lost, and a security incident report must be logged in accordance with the Security Incident Response Policy (reference (c)).

    iii. The owner of the removable media must conduct all appropriate maintenance on the item at intervals appropriate to the type of media, such as cleaning, formatting, labeling, etc.

    iv. The owner of the removable media, where practical, must ensure that an alternate or backup copy of the information located on the device exists.

    v. Removable media must be stored in a safe place that has a reduced risk of fire or flooding damage.

    vi. If the storage item contains sensitive information, removable media must:

        1. Be stored in a locked cabinet or drawer.

        2. Store only encrypted data that is securely enciphered in accordance with the Encryption Policy (reference (d)).

    vii. All data on removable media devices must be erased, or the device must be destroyed, before it is reused or disposed of.

    viii. When removable media devices are disposed, the device owner must inform the ISM so that it can be removed from reference (b).

b. *Cloud Storage*

    i. All cloud storage systems in active use and containing data pertinent to the organization must be registered in reference (b). Registration may be accomplished by manual or automated means.

    ii. All cloud storage systems listed in reference (b) must be re-inventoried on a quarterly basis to ensure that it is still within the control of the

organization. To re-inventory an item, the owner of the removable media must check in the item with the organization's Information Security Manager (ISM). Re-inventory may be accomplished by manual or automated means.

   iii. The owner of the cloud storage system must conduct all appropriate maintenance on the system at regular intervals to include system configuration, access control, performance monitoring, etc.

   iv. Data on cloud storage systems must be replicated to at least one other physical location. Depending on the cloud storage provider, this replication may be automatically configured.

   v. The organization must only use cloud storage providers that can demonstrate, either through security accreditation, demonstration, tour, or other means that their facilities are secured, both physically and electronically, using best practices.

   vi. If the cloud storage system contains sensitive information, that information must be encrypted in accordance with reference (d).

   vii. Data must be erased from from cloud storage systems using a technology and process that is approved by the ISM.

   viii. When use of a cloud storage system is discontinued, the system owner must inform the ISM so that it can be removed from reference (b).

c. *Personally-owned Devices*

   i. Organizational data that is stored, transferred or processed on personally-owned devices remains under the organization's ownership, and the organization retains the right to control such data even though it is not the owner of the device.

   ii. The ISM is responsible for conducting overall management of personally-owned devices, to include:

      1. Installation and maintenance of Mobile Device Management (MDM) software that can effectively manage, control and wipe data under the organization's control from personally-owned devices.

      2. Maintain a list of job titles and/or persons authorized to use personally-owned devices for the organization's business, as well as the applications and databases that may be accessed from such devices.

      3. Maintain a list of applications prohibited from use on personally-owned devices, and ensuring that device users are aware of these restrictions.

iii. Personally-identifiable information (PII) may not be stored, processed or accessed at any time on a personally-owned device.

iv. The following acceptable use requirements must be observed by users of personally-owned devices:

    1. All organizational data must be backed up at regular intervals.

    2. MDM and endpoint protection software must be installed on the device at all times.

    3. Sensitive information stored on the device must be encrypted in accordance with reference (d).

    4. The device must be secured using a password, pin, unlock pattern, fingerprint or equivalent security mechanism.

    5. The device must only connect to secure and encrypted wireless networks.

    6. When using the device outside of the organization's premises, it must not be left unattended, and if possible, physically secured.

    7. When using the device in public areas, the owner must take measures to ensure that the data cannot be read or accessed by unauthorized persons.

    8. Patches and updates must be installed regularly.

    9. Classified information must be protected in accordance with reference (a).

    10. The device owner must install the ISM before the device is disposed of, sold, or provided to a third party for servicing.

    11. It is prohibited to:

        a. Allow device access for anyone except its owner.

        b. Store illegal materials on the device.

        c. Install unlicensed software.

        d. Locally-store passwords.

        e. Transfer organizational data to other devices which have not been approved by the organization.

#i. Illegal activities and the use of pirated software is stricly prohibited on authorised remote hosts.

i. The organization must reserve the right to view, edit, and/or delete any organizational information that is stored, processed or transferred on the device.

ii. The organization must reserve the right to perform full deletion of all of its data on the device if it considers that necessary for the protection of company-related data, without the consent of the device owner.

iii. The organization will not pay the employees (the owners of BYOD) any fee for using the device for work purposes.

iv. The organization will pay for any new software that needs to be installed for company use.

v. All security breaches related to personally-owned devices must be reported immediately to the ISM.

5 Authorship and Approval

Last edit made by Lotana (louis.tant@gmail.com) on Mon, 7 Dec 2020 22:25:04 -0500.

Approved by Lotana (louis.tant@gmail.com) on Mon, 7 Dec 2020 22:25:04 -0500 in commit 0ef43289396c1cdfeab2840e8d508897bd420ccd.