SDHS Data Destruction and hardware disposal

Purpose

This document details the responsibilities of CSCS in the destruction of data that has been stored electronically within the Secure Data Hosting Service (SDHS).

It covers 3 different types of destruction:

1. Removal of files, folders or objects from volumes that will remain active
2. Removal of entire volumes
3. Removal of physical storage

Scope

All storage, both physical and logical, that contains data contained within or directly relating to the SDHS.

Related Documentation

Guidance on data destruction has been adopted from the 'NHS Digital: Destruction and Disposal of Sensitive Data Good Practice Guidelines', version 3.2, published January 2017.

This document can be found here: http://content.digital.nhs.uk/media/23585/Data-destruction-standards/pdf/HSCIC_Data_Destruction_Standard_v3.2.pdf

Supporting Guidelines for Media Sanitisation from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

1 - Removal of files, folders or objects from volumes that will remain active

This activity covers day-to-day data management. Files, folders and objects (such as virtual machines) may be removed as part of the normal workflow for a study.

Volumes within the SDHS have snapshots taken for backup purposes. These snapshots are retained for up to 90 days. During this period, any object that has been deleted can be recovered through the snapshot by a user that has adequate permissions.

After the snapshot retention time has been exceeded the snapshots will be removed. This process in itself does not typically remove the data from disk, but instead removes the pointers to the data and allows that section of disk to be overwritten.

It is not possible to recover data using the storage system software from snapshots that have been deleted.

2 - Removal of entire volumes

This activity covers the removal of an entire volume of data from the SDHS. Typically this will occur when a study is closed, and there is no requirement to retain the data.

When CSCS receive a notification that a volume is to be removed, the volume will be taken offline. This removes any end user access to the volume and the contained data. Volumes remain in the offline state for 30 days, allowing users to request the volume to be re-activated.

Once the 30 day grace period has expired, the volume will be deleted from the storage system. Some storage systems have a built in volume recovery option which may retain the volume for a further 12 hours following the deletion of the volume.

Similar to snapshots, the actual data is neither removed nor zeroed at this point, but the disk blocks are made available for writing by other applications.

It is not possible to recover data using the storage system software from volumes that have been deleted.

More thorough removal techniques are not able to be employed when removing a volume as the underlying hardware is shared amongst many study volumes, and would be disruptive to the operation of other studies.

CSCS will record the removal of the volume within their request record.

This process follows the NHS Digital Guidance section 8.4 for 'Data Removal from Live Systems'.

3 - Removal of physical storage

This activity covers the removal of the physical storage systems in their entirety that have held SDHS data. An example of this is the replacement of the storage hardware as part of a regular refresh .

Any change to the storage hardware used to host data for the SDHS will be accompanied by a Change Record.

As CSCS operate multiple environments that may or may not include sensitive data, we make no distinction between hardware that is being retired and hardware that is being re-used. All storage hardware will be purged of data, as defined in section 8.3 'Purging' of the NHS Digital Guidance.

These actions may be performed by CSCS using suitable tools, or may be outsourced to a 3rd party specialist in data destruction. Hardware will be erased to HMG Infosec S5 Enhanced - multi pass pattern wiping (minimum of 3 passes).

Records of all hardware components, with serial numbers, will be recorded in the Change Record alongside a Certificate of Destruction.

4 - Disposal of hardware

In the event that the hardware is to be disposed it will be collect by the University WEEE disposal contractor. As stated below under hardware failaure no disks or removable media shall be left in the device being disposed ensuring the device contains no information assets.

Hardware Failure

All hardware systems are at risk of failure. CSCS operate storage systems that can tolerate component failures without affecting the availability or integrity of the data that is being held. Storage hardware that is maintained by CSCS is accompanied by a service contract with a 3rd party provider which includes the replacement of defective hardware.

If the service contract requires that the defective hardware be returned to the supplier, then CSCS will either:

- Ensure that the supplier has robust procedures in place for the handling of components containing potentially sensitive data
- Ensure that any data on the component has been sufficiently destroyed prior to return

If neither of the above options are available, then CSCS will arrange with the supplier to retain the defective part and independently arrange destruction of the data on the component.

Records of all hardware components, with serial numbers, replaced as part of a hardware failure will be recorded in the Incident record.