SDHS: External Resource Exceptions

Some studies may require access to specific resources which are not available within the SDHS environment. The default position is that there is no access to any external resources from within the SDHS. There are however circumstances where direct access from the SDHS to an external resource is required for procedural reasons related to a study. In some cases exceptions are allowed in order to reduce risks, by removing the requirement to download and access sensitive data from outside the SDHS and then use the Transfer Service to ingest the data.

As IT service provider, CSCS reserves the right to reject a request for an external resource access exception if it is deemed to have an unacceptable level of information security risk or insufficient technical/governance information has been provided. Disputes will be resolved through an escalation with the Information Governance Office and the CSCS Management Team.

Application

If your study requires access to an external resource, then you will need to complete the SDHS Amendment Request form, which can be found here: https://cscs.medschl.cam.ac.uk/server-services/secure-data-hosting-service/sdhs-amendment-request-form/

You will need to provide a number of pieces of information before your request will be considered. This information covers the resource you are looking to access, where it is hosted and the frequency you are looking to use the access. There is a requirement to provide details of the company that is hosting the resource, details of the physical location of the data/resource and a justification.

What happens next?

Your request will be reviewed by the CSCS Infrastructure Team. We will check various parts of the resource, including the security of the connection, certificates and reputation. We will also check that we are able to provide access to the resource without jeopardising the integrity, availability or confidentiality of the SDHS. The request will be reviewed by at least 2 people within CSCS.

Once CSCS are satisfied that the risks created by the exception are acceptable, the request will be passed to the Information Governance Office (IGO). The IGO will then confirm that the request is justifiable and valid within the context of any approvals that have been given and in compliance with any policies that may apply.

After the IGO has confirmed the request is valid, CSCS will implement and document the exception.

Reviews

All external resource exceptions will be reviewed every 6 months by CSCS. During the review we will validate that the site is still upholding the standards we require, that the resource is available, and that the resource is being actively used.

If for any reason we decide that the exception is no longer secure, we will be in contact with the Data Manager for the Study to identify resolutions.

Guidelines

The following guidelines should help you in ensuring that your request is processed without delay.

- Resources must have a Fully Qualified Domain Name. Direct IP address connections are not allowed.
- Websites must use HTTPS or SFTP, with a valid certificate, using SHA256.
- Websites should offer TLS1.2, TLS1.1 or TLS1.0. SSL3.0 connections will be rejected.
- Other resources should employ a minimum of 256-bit encryption for all data in transit
- The resource should require users to log in to access data, preferably with unique logins for each user
- Provide the full contact details of the company that is hosting the resource
- Wherever possible, if a resource or service is made available by the University, it should be used