Sheffield
Hallam
University

Policy for Remote Access to any Corporate System at SHU by External Suppliers

Issuing Authority: Simon Briggs,
Director of Digital Technology Services

Signed:

Effective Date: February 2023

Version: 2023.1

Policy for Remote Access to SHU Corporate Systems by External Suppliers

Objective

This document is designed to specify the process that must be followed when any external supplier wishes to access any Corporate System within the University remotely. This process must be followed to ensure secure and consistent practice.

The Connection Process for Access via a Remote Desktop

Preconditions

- A supplier-specific active directory account exists for each relevant supplier to gain access to a specific remote desktop.
- This account is disabled by default and the supplier has knowledge of the account name but not the password.
- Remote desktops, each associated with one of the accounts above, exist.
- Each remote desktop provide access ONLY to the systems relevant to the supplier.
- An appropriate account(s) exist(s) for the supplier to gain access to the specific relevant system(s), e.g. SI, specific SQL server.

Process to request and gain access

1. An Incident Management System (IMS) request is raised by the Service Team supporting the system, stipulating:
    - The system required to be accessed
    - The name of the external supplier wishing to access the system remotely
    - The name of the individual wishing to access the system remotely
    - The email address of that individual
    - The start date, end date and time of the access required
2. The IMS call is assigned to the NI Infrastructure Operations NI Network Security Unidesk group.
3. The member of the NI Infrastructure Operations NI Network Security Unidesk group enables the relevant account for access to the appropriate remote desktop for the requested length of time only, and gives this account a new password. An email is sent to the named individual, stating the password of the account to gain access to the remote desktop and the length of time this account will be enabled for. This action is recorded in the IMS record by adding an Action item.
4. The supplier uses the remote desktop to gain access to the system remotely during the allowed time period.
5. At the end of the allowed time period the remote desktop access account automatically becomes disabled and the user, if still connected, is forced off the remote desktop.