Sheffield Hallam University

Information Security Policy for Suppliers, Contractors and other Third Parties

Issuing Authority: Simon Briggs,
Director of Digital Technology Services

Signed: 

Effective Date: February 2023

Version: 2023.1

Information Security Policy for Suppliers, Contractors and other Third Parties

Objective

To control access to the University's information and information systems by third parties who are contracted to design, develop or operate information systems for the University.

Policy Requirements

1. All external suppliers used by the University shall agree formally in writing to adhere to the University's ***IT Security Policies, Procedures and Related Guidance*** (Formally the EISF) and supporting regulations, and the ***Regulations for the use of IT Facilities.*** The Policy, or the elements of the Policy relating to access by third parties, shall be delivered to any supplier before the supply of any services.

2 Any external supplier who is commissioned to develop information systems or services for the University, to enhance existing information services and systems, or to provide staff who will access University IT systems, shall agree as part of their contract to conform to the University's ***IT Security Policies, Procedures and Related Guidance*** and supporting regulations.

3 External suppliers appointed to process data on behalf of the University shall agree to a data protection clause in their contract with the University, or shall agree to the University's standard letter for appointing a data processor, in accordance with the ***Data Protection Guidance.***

4 Visitors who require access to University systems may use a temporary user account that will be allocated by **ITHelp**.

5 Any third party equipment (including loan or trial equipment) should, before being attached to the University's network, be checked to ensure that it installed with all current service packs, security patches and anti-virus software. Virus protection on third party equipment is the responsibility of the supplier or owner, and must be of equivalent functionality to that provided by the University on its own equipment. Remote control software or any other software that might compromise the security of the University's network and information systems should be disabled, unless a formal agreement has been made that the software may be used for providing external support.