Sheffield
Hallam
University

Network Management Policy

Issuing Authority:	Leon Etherington, Acting Chief Information Officer, Information Systems and Technology
Signed:	
Date Effective:	March 2016
Review date:	February 2018
Version:	2016.2

Network Management Policy

Objective

To ensure the secure operation of network facilities, whilst minimising the risks of systems failure and maintaining the integrity and availability of IT services, software, and data.

Scope

This policy applies to all University staff, students, data processors, partners, suppliers and contractors and other authorised users when working with University IT systems and infrastructure.

Policy Requirements

Operations

1. Operations staff shall maintain and keep current documentation of:
   - daily and weekly schedules of operations activities
   - data back-up procedures
   - procedures for dealing with alerts and alarms from the VESDA (Very Early Smoke Detection Apparatus) system
   - equipment maintenance and warranty arrangements
2. Logs shall be maintained of:
   - the temperature in data centres and inspected weekly to identify any fluctuations
   - power outages affecting data centres

Capacity and Continuity

3. Rigorous, systematic and resilient backup procedures shall be implemented to secure all University information and data. .
4. Backups shall be maintained of the configuration of network devices.
5. Capacity Planning shall be carried out as part of the annual business planning process, to ensure that efficient information processing is not impeded by inadequate capacity, slow response times or inappropriate configuration
6. Appropriate contingency plans shall be developed for each service supported by the University Network
7. New systems, or enhancements to existing systems, shall be developed and tested, wherever feasible, on a discrete test network.
8. To minimise the risk of systems and services being made unavailable by a virus attack, the network shall be protected by appropriate virus detection and control products. Advice will be available to staff and students regarding obtaining relevant software for the protection of their personal devices to provide fuller coverage against virus attack.

Network security

9. Personally owned equipment shall not be attached to the wired University network.
10. 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, in accordance with the Information Security Policy for ***Suppliers, Contractors and other third parties*** and the ***External Supplier Remote Access Policy.***
11. On the University's wireless network:
    - staff and students using University-owned wireless devices running the currently supported managed desktop may access the University's full managed desktop, using their normal username and password
    - a restricted service shall be offered to staff and students using their own wireless devices

- a guest service shall be maintained for visitors which will offer no services other than access to their home institution or organisation
- a log shall be kept of all wireless accesses, recording details of devices and usernames used to log in to the network

12. For external access to the University network:
    - Staff Remote Desktop may be used, with a user's normal username and password, to gain access to personal filestore, the Intranet, and Blackboard
    - Virtual Private Network (VPN) access is preferred when access to sensitive documents or financial information is required. Staff with University accounts, will have access to VPN automatically. Third party support and contractors may also be granted access but must be registered with a username on the appliance to use the VPN service and traffic will be encrypted. Certain types of student accounts may also be granted VPN access, especially those in remote locations or distance learning.

Security Documentation

13. Separate documentation on implementation of policy requirements (such as tools used, configuration of specific products, and system security standards) shall be maintained by technical specialists in their own area of expertise.

Inward and outward traffic

14. Firewalls shall be configured to have a deny-all policy as default:
    - systems for which off-campus access is required must be registered with the Network Security Team. A security check shall be undertaken before the system can be made available externally.
    - access logs shall be kept and reviewed regularly to determine which systems are not currently being accessed externally: any such system shall be closed to external access

For outbound traffic

- some common ports shall be blocked if there are known security vulnerabilities
- registered ports shall be blocked as a rule, but traffic may be enabled for specific requirements. These exceptions must be authorised and recorded by the IT Security Analyst.