University of Bristol
Information Security Policy - Network Management

Title	Network Management
Reference	ISP-12
Status	Approved
Version	3.0
Date Created	July 2014
Last Reviewed	October 2023
Next Review	October 2024
Classification	Public

Contents

1. Introduction

This Network Management Policy is a sub-policy of the University's Information Security Policy (ISP-01) and sets out the responsibilities and required behaviour of those who manage communications networks on behalf of the University.

2. Scope

All of the University's communications networks, wired and wireless, irrespective of the nature of the traffic carried over the networks (data or voice), provided and managed either by the University or on behalf of the University.

3. Policy

3.1. Management of the Network

The University's communications networks will be managed by staff with the relevant skills and training to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability).

Network management requires staff to have a high level of privileged access to critical infrastructure assets and as such, play a key role in ensuring University information assets are protected. Staff are expected to understand the entirety of the University's Information Security Policies and how they apply to their specific role.

Network staff are required to escalate and act promptly and within guidelines specified by change management to protect the security of the University network but must be proportionate in the actions that they take, particularly when undertaking actions that have a direct impact on the users of the University network. Any actions which may be potentially invasive of users' reasonable expectations of privacy must be undertaken in accordance with the University's Investigation of Computer Use Policy (ISP-18) and the associated Guidelines for System and Network Administrators document.

Network staff must immediately report any information security incidents to the Information Security Manager (or, if unavailable, by email to cert@bristol.ac.uk).

3.2. Network Design and Configuration

The network must be designed and configured to deliver high levels of performance, availability and reliability, appropriate to the University's business needs, whilst providing a high degree of control over access to the network.

Ongoing and future designs for network configuration must be agreed by the Architecture Review Board.

3.3. Physical Security and Integrity

Networking and communications facilities, including wiring closets, data centres and computer rooms must be adequately protected against accidental damage (fire or flood, for example), theft, or other malicious acts.

Network switches will be located in approved comms rooms only. This is to ensure physical access is restricted to authorised staff. Temporary exceptions may be made where this is not practical, and associated risk logged and tracked. Any exceptions will require the approval of the Network Manager.

3.4. Change Management

All changes to network components (routers, firewalls etc) are subject to IT Services' established change management processes and procedures.

3.5. Connecting Devices to the Network

Any device which poses a risk to the security or operation of the network is liable to physical or logical disconnection from the network without notice.

All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing, in accordance with standard University practices and in line with Investigation of Computer Use Policy (ISP-18).

Acceptable Use Policy (ISP-09) has further details on what is and is not acceptable to connect to University networks.

3.6. Network Address Management

The allocation of network addresses (IPv4 and IPv6) used on the University networks is the responsibility of IT Services which may delegate the management of subsets of these address spaces to other teams or Third Parties.

Network addresses (IPv4 or IPv6) assigned to end-user systems will, wherever possible, be assigned dynamically (and will therefore be subject to change).

3.7. Network Boundary Management

Access to network resources must be controlled to prevent unauthorised access. Access control procedures must provide safeguards through robust identification and authentication techniques.

For more information on administrative account access refer to User Management Policy (ISP-08).

IT Services or authorised third parties are responsible for the management of the gateways which link the University network to the Internet. Controls, such as firewalls will be enforced at these gateways to limit the exposure of University systems to the Internet in order to reduce the risks of hacking, denial of service attacks, malware infection and propagation and unauthorised access to information. Controls will be applied to both incoming and outgoing traffic.

The same network boundary management principles will apply to internal network segmentation.

4. Further Guidance

- Guidelines for System and Network Administrators: http://www.bristol.ac.uk/media-library/sites/infosec/documents/sysadmin.pdf
- Investigation and Computer Use Policy ISP-18: https://www.bristol.ac.uk/infosec/policies/investigation-of-computer-use-policy/
- Acceptable Use Policy ISP-09: https://www.bristol.ac.uk/infosec/policies/acceptable-use-policy/
- User Management Policy ISP-08**:** https://www.bristol.ac.uk/infosec/policies/user-management-policy/
- ITS Change Management Process: https://uob.sharepoint.com/sites/it-services/SitePages/IT-Service-Management/change-management.aspx