**University of Bristol**
**Information Security Policy**

| | |
|---|---|
| **Title:** | **Network Management** |
| **Reference:** | **ISP-12** |
| **Status:** | **Draft** |
| **Version:** | **1.2** |
| **Date:** | **July 2014** |
| **Reviewed:** | **June 2021** |
| **Classification:** | **Public** |

## Contents



## 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.

## Scope

All of the University's communications networks, whether wired or wireless are in scope, irrespective of the nature of the traffic carried over the networks (data or voice).

## Management of the Network

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

Network staff are in highly privileged positions and play a key role in contributing to the security of the University's information assets. They are expected to be aware of

the University's Information Security policy in its entirety and must always abide by the policy.

Network staff are authorised to act promptly to protect the security of their networks, but must be proportionate in the actions which they take, particularly when undertaking actions which have a direct impact on the users of the 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 (ISP-18)" policy 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).

**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.

The network must be segregated into separate logical domains with routing and access controls operating between the domains in order to prevent unauthorised access to network resources and unnecessary traffic flows between the domains.

**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. Exceptions may be made where this is not practical. Any exceptions will require the approval of the Network Manager.

The network should, where appropriate and possible, be resilient to help mitigate the impact of the failure of network components.

**Change Management**

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

**Connecting Devices to the Network**

It is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the University's wireless networks.

Any device connected to a University network must be managed effectively. Devices which are not are 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 normal operational practices.

## Network Address Management

The allocation of network addresses (IPv4 and IPv6) used on the University's networks shall be managed by IT Services' Network Team, which may delegate the management of subsets of these address spaces to other teams within IT Services.

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

## Access Controls

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

IT Services is responsible for the management of the gateways which link the University's network to the Internet. Controls 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.

## Further Guidance

The "Guidelines for system and network administrators" document is available at:

http://www.bristol.ac.uk/media-library/sites/infosec/documents/sysadmin.pdf