# Firewall Policy

| | |
|---|---|
| Owner: | |
| Approver (Date): | |
| Review due date: | March 2022 |
| Current Version: | 1.0 |
| Update history: | N/A |
| Document Type: | Operational Policy |
| Classification: | Internal Only |

To discuss receiving the document in an alternative format, please contact University Secretariat.

# Contents



## 1. Introduction

1.1 The university has an obligation to provide appropriate and adequate protection of its IT infrastructure, including but not limited to Servers (Virtual and Physical), Network components, End User Compute Devices, Mobile Phones and Tablets

1.2 The University of Roehampton has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems.

1.3 Effective implementation of this policy reduces the likelihood of compromise which may come from a malicious threat actor or threat source.

## 2. Scope

2.1 All firewalls and equivalent network devices in use within the University of Roehampton are within the scope of this procedure.

## 3. Responsibilities

3.1 The Chief Information Officer is accountable for

- ensuring that firewalls and equivalent network devices are all configured in line with this instruction prior to their use within the University of Roehampton
- ensuring that the rules governing whether network traffic is permitted to pass through the firewall are suitable, thorough and effective
- ensuring that the device configuration is still valid through regular checks

3.2 The Network and IT Security Manager is responsible for implementing the configuration and processes as described below.

## 4. Definitions

4.1 Firewall refers to both physical and virtual appliances

4.2 Equivalent Network Devices includes any network device that is capable of applying rules to control the flow of traffic into, out of and around the University network such as host based firewalls or routers.

## 5. Firewall Policy

5.1 All firewalls and equivalent network devices are recorded by the University of Roehampton in its Firewall Asset Register.

5.2 All points of access between the internet and the University of Roehampton's network must be controlled by at least one firewall or equivalent network device.

5.3 All points of access between different networks used within the University of Roehampton (e.g.: research, staff, students etc.) are controlled by at least one firewall or equivalent network device. These points of access are recorded in the University's Firewall Asset Register.

5.4 The default administrative account password for all firewalls or equivalent network devices is changed to a password that complies with the password rules described in the Password Guidance for University Network Accounts prior to implementation.

5.5 The administrative account password must be changed upon known or suspected compromise. This could be as a result of employee movers and leavers, malware infection or if advised to do so by the manufacturer.

5.6 All University owned or managed laptop and desktop computers will be configured with a host based firewall with profiles suitable for when the device is connected to both trusted and untrusted networks.

5.7 Firewalls and equivalent network devices should limit network traffic to only that which is needed. These points of contact and associated rules should be recorded in the University of Roehampton's Firewall Asset Register.

5.8 Firewalls and internet gateways are deployed with specific configurations defined, including a set of default rules that block all network traffic.

5.9 Default rules that specifically allow network traffic to pass should be subject to approval by the Network and IT Security Manager and listed with the business justification in the University of Roehampton's Firewall Asset Register

5.10 Additional firewall rule requests should be submitted to the IT Helpdesk on the Firewall Rule Change Request Form. Approved and implemented requests will be recorded in the University of Roehampton's Firewall Asset Register.

5.11 Temporary rule additions should be removed within 7 days of the supplied end date.

5.12 Vulnerable services should be blocked (denied) by default on all firewalls and equivalent network devices unless approved by the Network and Telecoms Manager with a suitable business justification. Approved use of these services should be recorded in the University of Roehampton's /Firewall Asset Register.

Examples of vulnerable services include:

- Server Message Block (SMB)
- NetBIOS
- Trivial File Transfer Protocol (TFTP)
- Remote Procedure Call (RPC)
- Remote Login (RLOGIN)
- Remote Shell (RSH)
- Remote Execution Command Protocol (REXEC)

5.13 The administrative interfaces used to manage the boundary firewalls are configured to deny access over the internet.

5.14 All firewalls and equivalent network devices are reviewed every three months to ensure that the configuration is accurate and up to date and that rules that are no longer required are either disabled or removed.

5.15 This policy is subject to review every 2 years to ensure that it is accurate, effective and up to date.