Firewall Access & Configuration Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins

Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	08/08/2018
V 0.2	Andrew Clarke	PWG Approval	30/09/2018
V 1.1	Andrew Clarke	Revisions – Andy Cripps (Network Operations Manager) & Simon Furber (Network & Infrastructure Manager)	30/07/2019
V 1.1	Andrew Clarke	Annual Review	27/07/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 30 Jul 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 30 Jul 2019
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London (BUL) covering perimeter firewall administration, determines the technology standard used by the firewall hardware and software, assigns firewall administration responsibilities and defines the filters applied to campus networks.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Chief Information Security Officer	• Responsible for security architecture including firewalls
Network & Infrastructure Manager	• Responsible for implementing, configuring and maintaining Firewalls
Head of Infrastructure and Operations	• Responsible for ensuring security architecture is implemented in accordance with Policy

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A13 – Communications security
ISO 27001:2013 Conformance Control	Information Classification Objective A.13.1 Network security management

1.4 Scope

All Firewalls operated by Brunel University London are within scope of this Policy.

Endpoint firewalls are out of scope.

1.5 Policy Overview

Brunel University London (BUL) Information Services manages a perimeter firewall between the Internet connection with JANET and the University campus network to establish a secure environment for the campus' network and computer resources. This firewall filters Internet traffic to mitigate the risks and potential losses associated with security threats to the campus network and information systems. In addition the firewall secures a number of other 'networks/zones controlling traffic between clients and servers and other parts of the BUL data network.

The perimeter firewall is a key component of the University's Network Security Architecture.

2.0 Firewall Management

2.1 Firewall Management

a. Firewalls can only be accessed, configured and maintained by authorised members of the IS Network Team

b. Firewall administrators must be competent persons to be permitted access to firewalls

c. Configuration files are backed up and stored in a restricted area of the network

d. Vendor sites are monitored and subscriptions configured for all security alerts and firewall firmware/software updates

e. Events are handled in line with the incident management procedure and logged in compliance with the BUL-POL-16-1 Infosec Incident Management Policy

f. Firewall software versions are updated when there is a vulnerability with the current version or when desired new functionality is required

g. All changes[1] made to University Firewalls may be made by authorised personnel when required by the University with documented[2] authorisation through CAB (held weekly).

h. Authorisation through CAB is exempted for exceptions where there is no impact to service availability and these changes must be authorised by either the Head of Infrastructure & Operations or the Chief Information Security Officer

i. Emergency changes invoked in response to incidents may be authorised by a Senior Incident Officer in the absence of authorisation by either the Head of Infrastructure & Operations or the Chief Information Security Officer

j. All upgrades, software or firmware updates are subject to change control

2.2 Policy for Perimeter Firewalls

The perimeter firewall(s) permit(s) the following outbound and inbound Internet traffic:

- Outbound - All Internet traffic to hosts and services outside of Brunel University's networks except those specifically identified are blocked

- Inbound - Allow stateful and role-based Internet traffic that supports the operation of the University. All inbound unsafe services are blocked

[1] Additions, modifications or deletions to rules, configuration changes and upgrades
[2] Email or Service Desk management solution (Remedy)

The configuration of the firewall zones and their use is the responsibility of the Network & Infrastructure Manager

2.3 Reason for filtering ports or applications

- Protecting Brunel University Internet Users - certain ports are filtered to protect Brunel University networks and users.
- Protecting Brunel University outbound bandwidth - If Brunel University Internet users overuse the outbound bandwidth by running high-traffic servers or by becoming infected with a worm or virus, it can degrade the service of other Brunel University systems.
- Protecting the rest of the Internet - some filters prevent personnel who are associated with the University from either knowingly or unknowingly attacking other computers in the Internet.

In addition to being in Brunel University's interests for protecting our bandwidth, it is the University's responsibility to prevent abuse of its network.

2.4 Firewall Standards

Brunel University is committed to operate fully supported and maintained resilient enterprise class firewalls.

Access to read or write firewall configurations for both internal or perimeter devices are required to be by unique identity which can be logged and audited.

2.5 Policy for Internal / Data Centre Firewalls

Internal firewalls establish secure communications between different segments of the University's network where different levels of security and/or protection are warranted and are the responsibility of IS network services to maintain.

Installation of an internal firewall needs to be approved by the Head of Infrastructure and Operations. Administrators of internal firewalls should expect IS to influence specification, network connectivity, network design and rule sets of any existing or new installation.

2.5.1 Campus resident Third-Parties

Third Party organisations resident on the Brunel campus that traverse the University Firewalls must install firewalls adopting the guidelines and advice from the University Networks team and adhere to University policy.

2.6 Operational Procedures (Perimeter security)

Brunel University staff may request that access be granted from the Internet to services inside Brunel University for a new or existing application or service. These requests must be approved by the requesters department lead and submitted to the Service Desk management solution (Remedy) as a Firewall Request with all the relevant necessary information provided. If information is missing, the request will be rejected.

The Networks Team will evaluate the risk of implementing the rule change on the firewall to accommodate requests.

All requests for changes to existing rules or rules for access to new services will be initially reviewed by the Network Team and the Cyber & Information Security Team and then passed to the Head of Infrastructure and Operations before submission to CAB for approval to generate the change within the firewall configuration.

Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the requestor and alternative solutions will be explored.

Users should expect IS to require standard services to run on standard TCP/UDP ports.

Certain critical systems may require outside vendors and other entities to have secure limited access to University Information Systems achieved by way of the Internet. Such access must to be approved, signed and then coordinated using the Third Party Remote Access policy.

2.7 Operational Procedures (Internal security)

The main procedures are as above. Additional notes:

- Security zones are added by the networks team with authorisation from the Head of Infrastructure and Operations
- Requests that deviate from the policy must be authorised by Head of Infrastructure and Operations

2.8 Change Management Procedures

Configuration changes must follow the appropriate Change Control Procedure.

2.9 Periodic Review of Firewall Settings

New rules for services are reviewed by the Networks Team before firewall changes are implemented. Alternatively, when an application is phased out or upgraded, the firewall rules are changed. This minimises the presence of old and potentially insecure rules that are no longer needed.

Firewall installations and rules should be audited on an annual basis.

This Firewall policy will be reviewed annually.