Boundary Firewall Rules Policy

Version 1

Document History and Reviews

Author	Version	Date Issued	Changes	Approval
P.Jones	0.1	September 2017	Initial Draft	
T. Dyhouse	0.2	September 2017	QA & amendments	
P.Jones	0.3	October 2017	Document name change. Minor updates.	
T. Dyhouse	1	May 2018	Approved Version	IGSSG

Review Distribution

Name	Title
	Exeter IT Senior Management Team

Approval

Name	Position	Signature	Date
	Members of the IGSSG		May 2018

1. Introduction

1.1 The University of Exeter (UoE) IT infrastructure covers many campuses which contain a variety of types of networks. There are firewalls both physical and logical that are managed by Exeter IT which pertain to the Information Services Active Directory (ISAD) network.

2. Purpose

2.1 The purpose of this document is to regulate how firewall rules are setup, reviewed and maintained on the ISAD network which is managed by Exeter IT.

3. Scope

3.1 This policy covers all boundary firewalls that are managed by Exeter IT on the ISAD network.

4. Definitions

4.1 IT Services refers to:

Services which are either provided directly by University departments and managed by University staff OR provided to the University by third parties under bilateral outsourcing or cloud computing arrangements. Examples include:

- University file sharing 'One Drive' system - hosted by Microsoft and managed by IT Services
- University e-mail service - provided by Microsoft under the terms of a formal contract meeting the University's requirements

5. Policy

5.1 All default usernames and passwords must be changed upon installation. Passwords with the password policy which stipulates at least 10 characters, comprised of at least 3 of the following types – Upper case letters, lower case letters, numbers, special characters.

5.2 All open ports and services are provisioned by a request process which is approved by authorised representatives via the firewall admin team within Exeter IT. All requests and decisions are documented and implemented by Exeter IT. All requests should be made in writing to sid@exeter.ac.uk

5.3 The UoE runs a "Deny All" policy for inbound traffic and "Explicit Deny All" policy for certain ports within the UoE.

5.4 Requests for specialist services are tracked through the IT Helpdesk and regularly reviewed. The user can request either temporary or permanent services.

5.5 Firewall rules shall be reviewed every 6 months and the review documented. The Firewalls should be regularly reset to "Deny All" and rules re-applied in accordance to their requirements and relevance to the organisation. Legacy firewall rules which directly connected the JANET through to Plymouth University and the Penryn Campus, shall be reviewed on a regular basis.

5.6 Remote Management Interfaces of the firewalls that are Internet facing shall be disabled. Internally, the interfaces are restricted to a set range of IP addresses.

5.7 All end user devices are provided by the University and have software firewalls (as provisioned by the vendors) which are enabled. Unapproved connections are blocked.

6. Policy Review and Maintenance

6.1 This policy will be reviewed and updated, annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.