Firewall Management Policy

Title

Firewall Management Policy

Version Control

Owner	Version	Edited By	Date	Comments
Coach Direct	0.1	KL	14/07/16	First Draft

Distribution

Held By	Format	Location	Comments
	Digital / Physical		

Status

X	Status	Approved By	Date
	Working		
X	Draft		
	Provisional Approval		
	Publication		

Classification

	Please refer to ISMS 02 Information Handling & Classification Procedure
X	**Confidential**
	Restricted
	Unclassified

Relevance to Standard

Standard	Clause	Title
ISO 27001:2013	A13.1.2	Security of network services

Firewall Management Policy

1.0 Overview

The firewall management policy describes the organisation's approach to protecting the boundary of it's corporate network and network services.

2.0 Policy

2.1 Implementation

The organization will deploy suitable firewall devices at the boundaries of its corporate network to manage traffic crossing between the public (Internet) and private networks.

2.2 Configuration

The organization recognizes that some network services require rules permitting Inbound, Outbound or Both in order to function correctly.

Both user and network services access to the private network will be provided according to the Access Control Policy.

The MD will give authority to implement new firewall rules or change existing rules only, on the advice of the approved IT Support Company. Authority must be provided in writing, an email is acceptable.

Rules which are no-longer required will be removed or disabled from the firewall as soon as possible. To preserve the principles of 'need-to-know' and 'need-to-use' the approved IT Support Company may remove rules immediately and without authorization of the MD, where they are satisfied that the related service is no longer used or where permitting access through the firewall presents a significant risk to the network.

All rules configured on the firewall will be reviewed by the IT Support Company and agreed by the MD on an annual basis.

2.3 Firmware

The firewall's firmware will be kept up-to-date.

The approved IT Support Company will check for updates to the firmware a minimum of once per month, and apply all available updates within 30days of their release.

Network connectivity will be tested and verified after the firmware has been updated.

The Firewall's configuration data will be backed-up prior to the installation of new firmware and a minimum of 3 generations of the data will be held off-site.

2.4 Monitoring

The firewall retains a 30 days of log data that can be used for troubleshooting or investigatory purposes.

Due to the large volume of log data, only critical alerts will be emailed to the approved IT Support Company.

2.5 Testing

The firewall will be tested, at least annually, from outside the network using tools including:

- UPnP SSDP Test: https://www.grc.com/shieldsup
- Open Ports: http://mxtoolbox.com/PortScan.aspx

3.0 Related Policies

- Password Policy.
- Access Control Policy
- Patching Policy