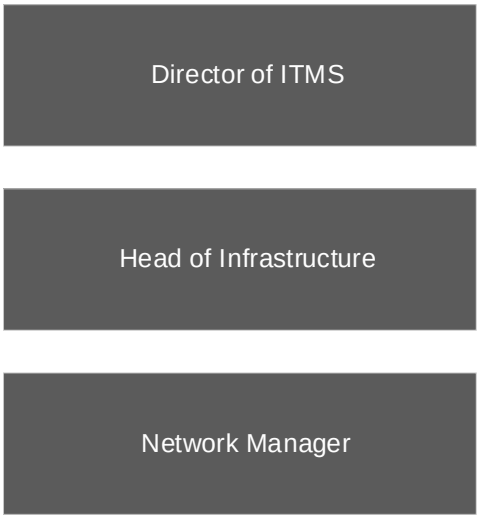
Network Management Policy

4. Management of the Network



5.1.4 To

8. Controlling Access

ITMS is responsible for the management of the university data network devices that link multiple buildings and data centres together and ultimately to the internet. It is imperative that access to these devices must be controlled to prevent unauthorised access in order to reduce the risks to the university from cyber-attacks.

8.1 Access to the university network devices must be strictly controlled and will only be permitted from authorised users and devices over suitably secured connections.

9. Configuration Management

9.1 A record of the configuration of all network devices will be kept.

9.2 Any changes to the network device configuration will be recorded with a record of prior and post configurations kept.

9.3 A risk assessment of any changes to the networks that are not 'Business as Usual' must be performed and documented prior to any changes being carried out and the results presented to the ITMS Change Advisory Board for their response to the risk.

9.4 Prior to implementation of changes to any network device that are not 'Business as Usual' the configuration changes must be tested before introduction into the live environment.

9.5 Restoration testing must be carried out on a regular basis that will be set by the Network Manager.

9.6 All network devices must have a secure version of software loaded.

10. Capacity Management

The data network must deliver high performance, reliability, resilience and security suitable for the requirements of the university. To maintain this network devices must perform at optimal levels.

10.1 The Network Manager and Head of Infrastructure will agree on optimal levels of performance of the following:

10.1.1 Network traffic capacity

10.1.2 Network devices

10.1.3 Phee7387 Tw 1.674 0 Td c66.6 (w)1(he)10.52.6 (ed TJ 0.0)0.6 (r-11.2 (rTj EM28.9 ( )H.6 (ol)228

12. Document History

12.1 5th October 2012 –