Communications Networks Management Policy

This policy applies to all Communications Networks under the control of the University of Reading.

1. The University shall have a single Network Design Authority responsible for the physical and logical design of all networks. This Authority is currently vested in the IT Services department.
2. The University will provide and manage ubiquitous communications networks across its campuses. The establishment of specialist localised networks for particular purposes shall be agreed in discussion with the University's Network Design Authority.
3. The University's networks shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. All network management staff shall be given relevant training on information security issues.
4. Networks must be designed and configured to deliver suitable performance and reliability to meet the organisation's needs whilst providing an appropriate degree of access control and a range of privilege restrictions.
5. The data network must be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting the organisation's systems.
6. Access to resources on the network must be controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust authentication and authorisation techniques.
7. Remote access to the data network will be subject to robust authentication and appropriately encrypted during transit across the network. VPN connections to the data network are only permitted for authorised users ensuring that use is robustly authenticated.
8. The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all significant changes to critical systems or network components. Changes must be appropriately tested, reviewed and authorised before moving to the live environment.

9. Moves, changes and other reconfigurations of users' network connections will only be carried out by staff authorised by IT Services according to procedures laid down by them.
10. Networks and communication systems must all be adequately configured and safeguarded against physical, environmental and technical threats.

approved by IFSG