Policy for access to university computer systems from off campus

Name of policy, procedure or regulation	Policy for remote access to University computer systems
Purpose of policy, procedure or regulation	A policy framework for remote network access to University computers and network devices
Who formally approved this policy, procedure or regulation?	Information Strategy Group
Who has responsibility for its update?	Information Services

To whom does this policy, procedure or regulation apply?

All University staff and students, external contractors, vendors, consultants, etc.

a) Date of approval	December 2008	**b) Proposed date of review**	Annual

1. Introduction

The University operates a large number of computer systems for various purposes (including student records, finance, e-mail, web, file store, library records and so on). Each of these may have different requirements as to who can access it, and from where. Remote access (meaning, from a network location not controlled by the university) has to be treated as a threat because the external environment can not be controlled. Nevertheless, some remote access to university computers is required, either to provide a service (web, e-mail etc), to allow students or staff to access data, or to allow external contractors to install or maintain software, and so on. This policy sets out the methods of access that are acceptable, and the process by which additional access may be requested and authorised.

2. Purpose

The purpose of this policy is:

- to provide a formal mechanism for the approval of requests relating to secure remote access to business and academic systems;
- to ensure that the nature of any remote access is such that it does not compromise the privacy of the University's systems or data;
- to ensure that usernames and passwords, and any confidential or sensitive data is encrypted while in transmission across the internet;

3. Access protocols

Policy statement: unencrypted protocols (notably FTP and Telnet) must not be used for access from off campus to University systems.

Rationale: Some internet protocols were designed for an environment in which electronic eavesdropping ("packet sniffing") was not a threat, and do not include any provision for encryption of data (including usernames and passwords) in transmission. Packet sniffing cannot be discounted as a threat to remote access across the internet.

Exceptions: the use of unencrypted protocols is permitted for non-sensitive data as follows:

- HTTP: permitted for providing web access to non-sensitive web pages, where no username and password are required for access.
  HTTPS (encrypted) is mandatory, if a username and password are required, OR the data being accessed is considered “confidential” or “sensitive” (in which case a login would normally be required).

- FTP: permitted for providing “anonymous FTP” access to non-sensitive data; in this case no username and password are required for access.
  SFTP (encrypted) is mandatory, if access is not anonymous (a username and password are required), OR the data being accessed is considered “confidential” or “sensitive” (in which case a login would normally be required).

- SMTP: internet e-mail is routinely carried on the unencrypted SMTP protocol.
  If data is sufficiently confidential or sensitive to require encryption, then this should be done at the message level using PGP (Pretty Good Privacy) or GPG (Gnu Privacy Guard) or equivalent software, without requiring a change to the transmission protocol.

4. VPN and Firewall access

Policy statement: all connections from off campus to University computers must be made via VPN.

Rationale: Providing access via a VPN has the following security benefits:

- no access is provided unless a valid username and password are presented;
- data in transmission is protected from eavesdropping;
- individual services can be provided to selected users only;
- the servers do not need to appear in the external-facing DNS and are therefore not “visible” to anyone not connecting via VPN

Exceptions: via the firewall

- Permitted unsecured HTTP, FTP and SMTP services detailed in the “access protocols” section 3;
- HTTPS connections to the University’s web servers (for the purpose of secure entry of data into forms etc);
- HTTPS connections to specified University application servers* for the purpose of gaining secure access to applications or data which are not of a confidential or “business sensitive” nature (e.g. students using MyPortal to access coursework files on their “H:” drive);

* Specified applications are currently: Blackboard; MyPortal, WebOutlook, PebblePad, EZProxy

5. Access to PCs from off campus

Policy statement: access will not be provided to desktop PCs from off campus.

Rationale: access to staff PCs can provide “proxy” access to other systems to which external access has not been authorised. Staff wishing to access data held on their PCs should store the data on their “H” drive, which is accessible via VPN connection or via the Portal system.

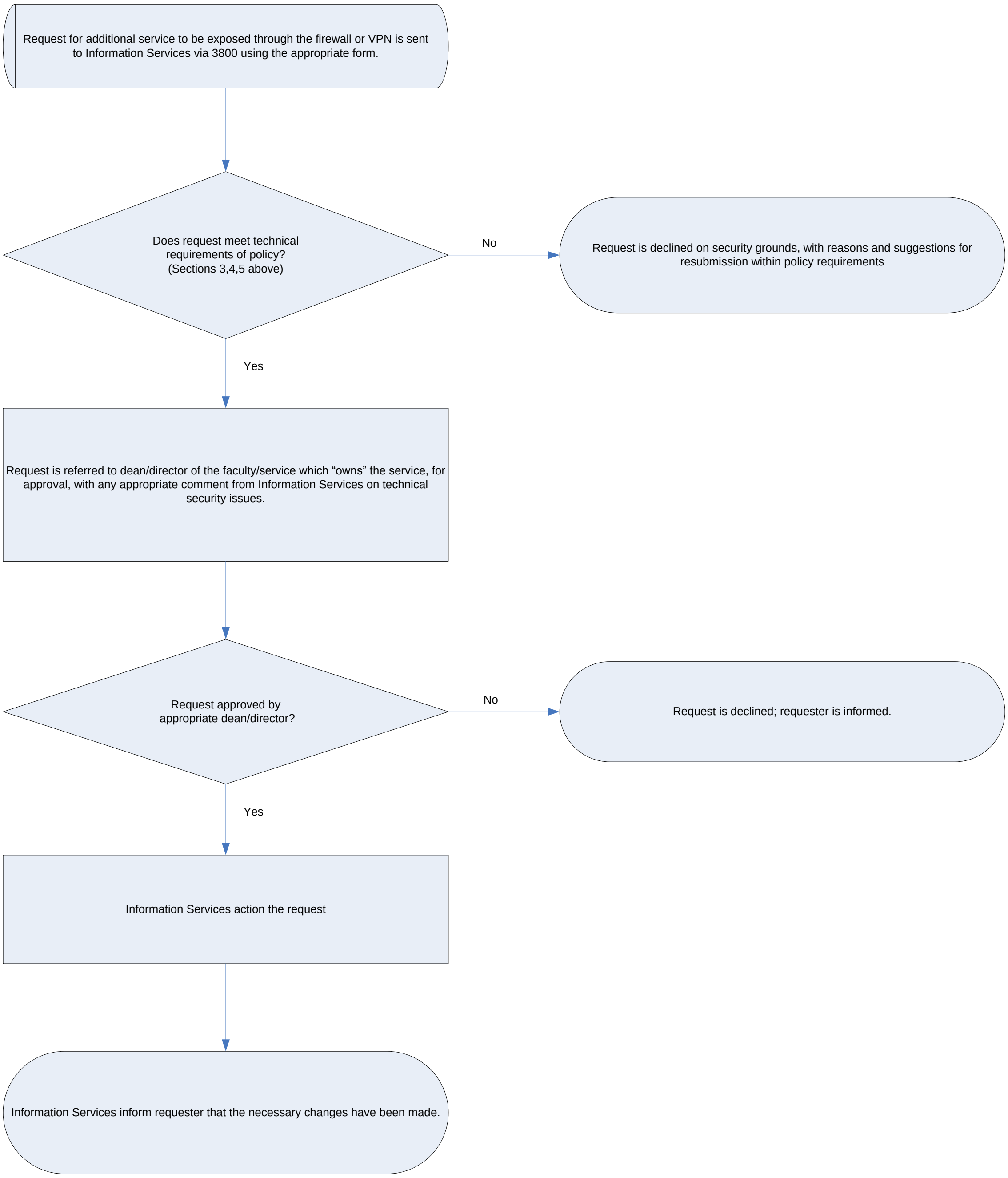
6. Emergency firewall access

In the case that a connection must be allowed through the firewall for pragmatic reasons (for example, to facilitate urgent system support work), this must be done on the basis that

- the exception is approved by the Director of IS or his nominated representative;
- the firewall rule is temporary and will be removed after a defined period;
- the connection is only allowed for a defined purpose (and the source IP address, or range of source IP addresses, associated with that purpose)

7. Procedure for requesting and approving remote access to a University system

The procedure for requesting and approving the appropriate remote access is illustrated by the following flow diagram.


Request for additional service to be exposed through the firewall or VPN is sent to Information Services via 3800 using the appropriate form.
Does request meet technical requirements of policy? (Sections 3,4,5 above)
No
Request is declined on security grounds, with reasons and suggestions for resubmission within policy requirements
Yes
Request is referred to dean/director of the faculty/service which “owns” the service, for approval, with any appropriate comment from Information Services on technical security issues.
Request approved by appropriate dean/director?
No
Request is declined; requester is informed.
Yes
Information Services action the request
Information Services inform requester that the necessary changes have been made.

8. Roles and responsibilities in relation to this policy

Information Services will manage this policy and update it appropriately in consultation with Information Strategy Group.

Firewall and VPN access rules are administered by Information Services. All requests should be addressed to 3800@staffs.ac.uk in the first instance, with the necessary information supplied on the appropriate form.

This policy takes effect from December 2008, from which date services will be migrated to the appropriate access method as detailed above, in consultation with Faculties/Services as appropriate.