GISP8. Offsite access control

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	All connections to University systems will be secured against unauthorised access.
Objective	• To ensure that only authorised users can connect to University computer systems. • To ensure that connections to University computer systems use secure protocols unless appropriate not to, for example the web site.
Policy	8.1. All University computer systems will be protected against unauthorised connections from external computers (i.e. those not registered on the University's network). 8.2. Authorised connection to University computer systems from external computers will be available by VPN or will be enabled by rules on the firewall, which will be approved and configured according to defined policies and procedures 8.3. Where possible all connections to University computer systems will use secure protocols which ensure that information, including usernames and passwords, are passed between systems in an encrypted format
Responsibility	• ITCS is responsible for maintaining the University firewall and for authorising any requests for external access to University systems. • ITCS will provide secure channels for connecting to computer systems. They will also ensure suitable software is provided on the University's Standard Staff and Student Desktops to enable users to securely connect to services, including login access, file transfer and email. • Users should not attempt to circumvent system access control mechanisms.
Incident Management	Any suspected breaches of the University's system access controls should be reported immediately to the IT Service Desk.

Audit and accountability	An annual review of all Firewall rules will be carried out by ITCS in consultation with Faculty/School/Unit IT support staff and other relevant authorities where appropriate. Interim review of some specific rules will be carried out where those rules were indicated as 'temporary' at the time their creation was requested. Firewall logs will be inspected daily by ITCS staff for evidence of attacks and regular summary reports will be emailed to relevant IT support staff and service managers alerting them to the level and type of attacks on the service/system they are responsible for. ITCS will monitor network traffic and log any insecure connection methods (telnet, FTP etc.) being used. They will liaise with the relevant system administrators and IT support staff to ensure that use of such ceases and secure connection methods are used.
Implementation	**Firewall** • The Firewall will be set to deny all external connections to University computer systems, unless a rule on the Firewall permits access to the system via a specified Data Service (e.g. WWW, SMTP etc.). • Those Data Services which will be allowed to access internal systems via a specified port will be based on recommendations from Janet/CERT. • Requests for changes to Firewall rules in order to allow external access to Faculty/School/Unit systems, must be made by the nominated IT support person responsible for the security of the system(s). Such requests must be submitted in writing, with the awareness and approval of relevant authorities within the Faculty/School/Unit. Requests must include details of the access required, business justification for the request and the duration required for the rule. Where requests may affect specific working groups within a Faculty/School/Unit, the requester is expected to have made such working groups aware. • ITCS reserves the right to refuse requests if implementation of a request would pose a serious security threat to University systems/services. **Secure Connections** • ITCS will provide secure connection methods and client software for staff and student desktop computers for accessing email, connecting to central filestore (mapped network drives), file transfer and login access.