GISP7. Onsite 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 equipment connected to the University network must be registered.
Objective	To ensure that only equipment which has been registered can connect to the network. To ensure unregistered devices have limited access to the University network containing self-registration and password reset services.
Policy	7.1. All equipment connected to the University network must be registered following the approved registration procedures 7.2. Any equipment detected as active on the network which has not been properly registered will be disconnected. 7.3. Devices that have been detected as not used on the network within the previous 6 months will be unregistered. 7.4. Changes in ownership of connected equipment should be notified to ITCS following approved change notification procedures.
Responsibility	• ITCS will provide mechanisms for registering equipment requiring connection to the University network. • Individuals should not attempt to connect any equipment which is excluded under the Conditions of Computer Use.
Incident Management	Any equipment detected on the network or access to the network which contravenes the conditions of computer use should be reported immediately to the IT Service Desk.
Audit and Accountability	ITCS will maintain a DNS/DHCP record for all equipment registered on the University network and will ensure this is up to date at all times and secure against unauthorised access.
Implementation	**University-managed equipment** • Only nominated IT Support staff may register University owned equipment on the network. • A web based form will be provided for this purpose which will enable registration of equipment on the network.

	• Registration details will be collected and processed according to defined procedures. • IT support staff should ensure that equipment being registered is virus free, has University approved anti-virus software installed (see GISP10), and poses no risk to security of the network or other equipment connected to it at the time of registration. **Personally-managed computers connected via Ethernet port in University residences** • Student and visitor owned computers do not need to be explicitly registered – the registration for the device will be automatically allocated against the person who holds the licence for the room where the connection was made. • Access to authorised University services will be mediated by policies/rules on the University Firewall. • Users should ensure that their computer is virus free and has up to date anti-virus software installed. **Personally-managed computers connected via Ethernet port on the main campus** • Personally-managed equipment cannot be connected to the University wired network. Staff can appeal directly to the IT Support Manager, or to the manager of the School's IT support team. If these are unable to amicably resolve the matter, they should refer to the appropriate authority within their Faculty/School. **Personally-managed computers connected to a University-provided wireless network (e.g. Janet Roaming Service/eduroam)** • Student, staff and visitor managed computers will be registered by the owner using the 802.1x protocol during the process of making their connection - no further registration process is required. • As for all other personally managed equipment, access to authorised University services will be mediated by policies/rules on the University Firewall. • Users should ensure that their computer is virus free and has up to date anti-virus software installed. Users should be aware that both the UEA Conditions of Computer Use and the Janet Roaming Policy will be in effect whilst they are using this service.