GISP4. Identification, authentication and authorisation

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	Individual usernames and passwords will be used to authenticate access by users to authorised University computer systems and IT services.
Objective	• To ensure that only authorised users can access University computer systems and IT services. • To ensure that individuals accessing computer systems and services can be identified. • To control access to restricted computer systems and IT services.
Policy	4.1. All individuals using University computer systems or IT services must be authorised to do so. 4.2. All authorised users will be assigned a unique University username and password in accordance with defined policies and procedures (GISP5). 4.3. Access to sensitive data such as personnel data will be authorised by designated service owners following defined policies and procedures. 4.4. Access controls shall be maintained at appropriate levels for all systems by on-going proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained.
Responsibility	• The Registrar and Planning Office are responsible for defining who is a member of the University. • The Information Strategy and Services Committee is responsible for deciding which IT services are made available to members of the University. • ITCS will provide and implement authentication mechanisms to control access, following defined policies and procedures. • Service owners are responsible for authorising individual's access to sensitive data. • Individuals must not attempt to access systems or services for which they are not authorised (see also GISP2 and Conditions of Computer Use).

Incident Management	All suspected breaches of authentication mechanisms should be reported immediately to ITCS via the IT Service Desk who will initiate investigation and appropriate action, including liaising with data owners/administrators where necessary.