GISP19. Personnel security

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	Controls ensuring that appropriate consideration is given to information security roles and responsibilities of staff.
Objective	To ensure that staff using information processing facilities within the University understand their responsibilities in regard to information security, and the risk of human error, theft, fraud or other misuse is minimised.
Policy	19.1. Where appropriate to the post, staff job descriptions should contain details of information security roles and responsibilities. 19.2. Pre-employment checks (e.g. taking up of references) should take account of the information security requirements of a post and ensure that the candidate is suitable in this respect. 19.3. All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after their employment with the organisation. 19.4. All staff with information processing duties will receive appropriate guidelines and training in regard to information security and compliance. 19.5. Training in information security threats and safeguards for technical staff is mandatory, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards. Where IT staff change jobs, their information security needs must be reassessed and any new training provided as a priority. 19.6. Staff with responsibility for system administration will have training in secure system configuration. 19.7. Staff should only have access to information that is required for the role.

	19.8. Persons responsible for Human Resources management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and to external parties. 19.9. When roles change, procedures should be followed to ensure that access rights are reviewed. 19.10. Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources management and the Strategy, Policy and Compliance team. 19.11. Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges. 19.12. On termination of employment, procedures should be followed to ensure that all access rights to University information or information processing facilities are removed. 19.13. Departing staff must return all information assets and equipment belonging to the organisation, unless agreed otherwise with the designated owner responsible for the information asset. 19.14. Periodic training for appropriate staff within the Strategy, Policy and Compliance team is to be prioritised to educate and train in the latest threats and information security techniques.
Responsibility	• The Human Resources Division (HRD) is responsible for ensuring that procedures and guidelines for the drafting of job descriptions and appointment of staff take adequate account of information security roles and responsibilities. • ITCS are responsible for ensuring that all staff are reminded of information security and compliance matters on an annual basis. • Line managers are responsible for providing staff with the appropriate guidelines and training in regard to their information security roles and responsibilities. • Staff should be aware of their information security roles and responsibilities and carry out their work in accordance with these.
Incident Management	If it is suspected that the above controls/policies have not been followed, the matter should be reported to HRD.