Information security policy review

Author: Raymond Scott (ISD)

Date: 20 November 2012

Version: 1.0

Summary of changes

Main areas covered:

- Policies updated
- Policies restructured
- Policies expired
- Main changes to GISP:
    - Combined security manual documents into GISP
    - Combined sections on staff, students and visitors where appropriate to reduce duplication
    - Reviewed for additional policy areas against the UCISA Information Security Toolkit
    - Added a new key points summary section to the introduction
    - Added three new policy areas on 'Working with Third Parties', 'Mobile Devices' and 'System Management and Development'
- Changes to other IT policies

An excerpt from ISD Managed Document Register[1] is included giving a summary of the changes made to the each policy, and a list of the feedback received from consultation on the policies at the end of the document.

Introduction

During the summer 2012, members of the Information Services Strategy, Policy and Compliance team (SPC) led by the Director of Information Services conducted an extensive review of all information security policies. This review was informed by reference to the UCISA Information Security Toolkit[2] and JANET information security training courses attended in July 2012 and run by their Chief Regulatory Adviser, Andrew Cormack.

The scope of the review included all policies listed on the Information Services web site at https://intranet.uea.ac.uk/is/itregs/ictpolicies, with a particular focus on the General Information Security Policy and Security Manual.

The existing set of information security policies were developed over a period of eight years. Some of the policies had not been updated since their original drafting, and therefore predate the more significant shifts in technology now posing the primary risks to information security such as mobile devices (particularly smartphone and portable storage devices), use of off-site storage (such as cloud providers), and collaboration tools hosted and managed by companies external to the University and therefore outside the control of its security measures.

[1] https://intranet.uea.ac.uk/is/strategies/policy
[2] http://www.ucisa.ac.uk/en/representation/activities/ist.aspx

Some of the policies date from a time when Information Services did not have in place such extensive governance structures providing transparency and accountability to the University community. These are no longer required, and they have been withdrawn and retired.

An extract from the ISD Document Register[3] included in this document summarises the actions for each of the existing policies subject to this review.

Consultation

Draft policies were first made available for comment on 21 Sept 2012, and consultation was closed on 19 October 2012. During the consultation, the policy development team engaged with the ISD Operations Group (esp. technical leads), the ISD IT Directors group (1 Oct 2012), and the IT Forum (10 Oct 2012). The draft policies were made available on the ISD web site and an ISD news item advertised their availability. A final review and approval was made by the ISSC on 8 November 2012.

High level information security policy (HLISP)

This policy sets out the University's commitment to information security, and how it proposes to go about embedding it with the University's practices and procedures. In particular, it clarifies where responsibilities for information security lie, and how governance is to be provided.

This has been updated to reflect the most recent style for ISD policies and current staffing and management structures within the University.

General information security policy (GISP)

The previous version of the GISP contained 33 separate policy areas divided into four groups: all users, staff, students, and visitors. Linked to the policy areas, more detail was provided in the 12 separate Security Manual sections.

The revised version of the GISP has the following changes:

- The separate sections for all users, staff, students and visitors have been combined to reduce duplication.
- Almost all sections were renumbered. Original numbers are shown in *italic* in this document
- The additional security advice and controls described in more detail in the Security Manual has been brought into the appropriate GISP section. This means the Security Manual is no longer required.
- It was reviewed for additional policy areas against the UCISA Information Security Toolkit.
- The introduction has new wording on Governance and implementation and Key points to be drawn from the set of policies
- Three new policy sections were added:
    - GISP22 – working with third parties. This will include use of third party hosted services as well as contractors on site.
    - GISP23 – mobile devices. As mobile device present a significant information security risk, a new separate section has been added.
    - GISP24 – systems management and development. The previous version of the GISP did not directly address the information security needs of information systems.

Security manual

Most sections of the security manual have been copied into the appropriate GISP section.

[3] https://intranet.uea.ac.uk/is/strategies/policy

Desktop computer policies

Most of these policies are no longer required and they have been retired and withdrawn.

Conditions of Computer Use (COCU)

The Conditions of Computer Use is subject to annual review and update, and the 12/13 version was approved by the ISSC at their June 2012 meeting. The review of the security policies and advice from the UCISA Information Security Toolkit raised one issue and a small edit is to be carried forward to the next review and revision for the 13/14 academic year.

Information security policies, procedures and guidelines

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
Policy	**Anti-malware and workstation specific controls [SM10.1]**	To ensure that workstations are protected against malware attacks from malicious software, and against unauthorised access	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM10.1+Anti-malware+and+workstation+specific+controls	ISSC	Approved	1.1	14/06/2011	Withdraw this policy – move key policy statements moved to GISP10 section on Protection against malicious software
Policy	**Conditions of Computer Use (COCU)**	Users of the University network and computing facilities must abide by usage policies	http://www.uea.ac.uk/is/itregs/usepols	ISSC	Approved	AY 12/13	12/06/2012	Add new statements covering use of email and expectations of visitors
Policy	**Desktop Computer Data Storage Policy**	Policy on storage of work data generated by or stored on University owned computer systems	http://www.uea.ac.uk/is/itregs/ictpolicies/desktopcomputerdatastoragepolicy	ISSC	Approved	1.0	12/11/2004	Withdraw this policy – move key policy statements to GISP13 section on Business continuity and disaster recovery
Policy	**Desktop Computer Hardware Policy**	Policy details which hardware platforms will be used as standard for University owned staff and student desktop computers as well as the level of support delivered from central services	http://www.uea.ac.uk/is/itregs/ictpolicies/desktopcomputerhardwarepolicy	ISSC	Approved	1.0	12/11/2004	Withdraw this policy – not needed

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
Policy	**Desktop Computer Operating Systems Policy**	Policy details how operating systems on University owned staff and student desktop computers will be deployed and supported by ISD	http://www.uea.ac.uk/is/itregs/ictpolicies/desktopcomputeroperatingsystemspolicy	ISSC	Approved	1.0	22/06/2004	Withdraw this policy – move key policy statements to new GISP24 section on System management and development
Policy	**Desktop Computer Procurement and Deployment Policy**	Policy details procurement and deployment of University owned desktop computer systems and level of support available from central IT	http://www.uea.ac.uk/is/itregs/ictpolicies/desktopcomputerprocurementdeploymentpolicy	ISSC	Approved	1.3	04/02/2011	No change
Policy	**Desktop Computer Software Policy**	Policy details application software installed and supported on staff and student desktop computers owned by the University by central IT services	http://www.uea.ac.uk/is/itregs/ictpolicies/desktopcomputersoftwarepolicy	ISSC	Approved	1.0	12/11/2004	Withdraw this policy – not needed
Policy	**Encryption policies and controls [SM21.1]**	To ensure that encryption is used in a consistent and manageable manner in line with the GISP and applied only to confidential or secret information	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/Encryption+policies+and+controls	ISSC	Approved	1.2	14/06/2011	Withdraw this policy – move key policy statements to GISP18 section on Encryption

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
Policy	**File and email restoration policy**	The policy on the restoration of digital assets. Backups are taken for disaster recovery purposes. End users are responsible for their own file management	http://www.uea.ac.uk/is/itregs/ictpolicies/File+and+email+restoration+policy	ISSC	Approved	1.0	10/11/2011	Add to policy suite on information management
Policy	**General Information Security Policy**	The General Information Security Policy addresses security concerns regarding all electronic information at the University	http://www.uea.ac.uk/is/itregs/ictpolicies/generalinformationsecuritypolicy	ISSC	Approved	3.8	04/02/2011	Removed: *GISP16 Health and Safety, GISP20 System specific (staff), GISP22 Corporate responsibilities and conduct (staff), GISP24 Liability of student's own systems and content (student), GISP26 Identification, authentication and authorisation of student systems (student), GISP27 Encryption use and personal liability (student), GISP28 Student responsibilities and conduct (student), GISP30 Identification, authentication and authorisation (visitors), GISP31 Key messages (visitors), GISP32 Encryption use and key handling (visitors), GISP33 Visitor responsibilities and conduct (visitors)*

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
								Added new sections on GISP22 third parties, GISP23 mobile devices, and GISP24 system management and development. Introduction has new sections on Governance and Key Points
Policy	**High Level Information Security Policy**	The Information Security policy is intended to ensure business continuity and minimised business damage by preventing and managing to an acceptable level the impact of security incidents	http://www.uea.ac.uk/is/itregs/ictpolicies/highlevelinformationsecuritypolicy	ISSC	Approved	Final	25/03/2005	Updated policy
Policy	**Information classification and data management [SM11.1]**	Provide a classification system for all University data and documents by which an appropriate security class can be assigned	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM11.1+Info-Classification-Data-Mgt	ISSC	Approved	2.0	12/06/2012	Removed from SM and recast as a separate policy alongside other information compliance/access to information policies
Policy	**IT security for secure areas [SM12.1]**	To ensure that IT and computing systems in secure areas have good IT security to guard against unauthorised access, theft or compromise	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM12.1+IT+security+for+secure+areas	ISSC	Approved	1.0	16/07/2007	Withdraw this policy – move key policy statements to GISP12 section on Secure areas

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
		of data						
Policy	**IT Service/Systems Security Risk Log [SM1.1]**	Risk log to be used for regular assessment and management of IT service security risks	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM1.1+-+IT+Services+%26+systems+security+risk+log	ISSC	Approved	1.1	19/02/2008	Withdraw this policy – move key policy statements to GISP1 section on Risk assessment
Policy	**Password assignment [SM5.1]**	Policies governing assignment of passwords. Ensure that all University computer systems conform to a single set of secure password rules/policies	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM5.1+Password+assignment	ISSC	Approved	1.3	10/05/2011	Withdraw this policy – move key policy statements to GISP5 section on Use of passwords
Policy	**Physical security for IT systems [SM3.1]**	Controls to ensure good physical security of IT systems	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM3.1+Physical+security+for+IT+systems	ISSC	Approved	1.0	16/07/2007	Withdraw this policy – move key policy statements to GISP3 section on Physical and environmental security
Policy	**Procedures for reporting and handling security incidents [SM14.1]**	To ensure that security incidents are effectively and consistently reported and handled	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM14.1+Procedures+for+reporting+and+handling+security	ISSC	Approved	1.0	03/08/2007	Withdraw this policy – move key policy statements to GISP14 section on Incident reporting and handling

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
			+incidents					
Policy	**Registration of equipment on the University network [SM7.1]**	To ensure that only registered equipment can connect to the University network and a University Domain Name Service (DNS) for that equipment is maintained	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM7.1+Registration+of+equipment+on+the+University+network	ISSC	Approved	1.2	09/06/2008	Withdraw this policy – move key policy statements to GISP7 section on Onsite access control
Policy	**Secure connection to services [SM8.2]**	To ensure that secure connection methods are used for email, connection to filestore, login access and file transfer, and that data transmitted over such connections is encrypted	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM8.2+Secure+connection+to+services	ISSC	Approved	1.0	17/01/2006	Withdraw this policy – move key policy statements moved to GISP8 section on Offsite access control
Policy	**Self-registered Equipment Terms and Conditions**	Additional terms and conditions applying to self-registered equipment such as that in student residences and connected to the UEA wireless network	http://www.uea.ac.uk/is/itregs/selfregtc		Approved		09/06/2008	Update ITHD contact details, remove reference that all computers must have network card registered, add note that equipment interfering with the wireless network will be prohibited

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
Policy	**Site Licensed Software Policy**	Policy on procurement and management of site licensed software for use in teaching and research on University owned computer systems	http://www.uea.ac.uk/is/itregs/ictpolicies/sitelicensedsoftwarepolicy	ISSC	Approved	1.0	29/11/2004	Withdraw this policy – not needed
Policy	**Skype Policy**	Policy on the use of Skype (www.skype.com) for voice and video calls through the internet by staff and students	https://intranet.uea.ac.uk/is/itregs/ictpolicies/UEAskypepolicy	ISSC	Approved	1.3	05/01/2009	Withdraw this policy – not needed
Policy	**System administrator passwords [SM5.3]**	Policies governing assignment and handling of system administrator passwords. To ensure that system administrator passwords are assigned, maintained and stored securely	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM5.3+System+Administrator+passwords	ISSC	Approved	1.3	17/03/2011	Withdraw this policy – move key policy statements moved to GISP5 section on Use of passwords
Policy	**UEA Exchange mobile devices security policy**	Mobile devices configured to work with Exchange must have a secure PIN to reduce the risk of unauthorised access	http://www.uea.ac.uk/is/itregs/ictpolicies/UEA+Exchange+mobile+devices+security+policy	ISSC	Approved	2.1	15/06/2012	Withdraw this policy – move key policy statements moved to new GISP23 section on mobile devices

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
Policy	**University firewall [SM8.1]**	To ensure a firewall is in place with a managed set of policies/rules to protect University systems against unauthorised access from external computers	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SM8.1+University+firewall	ISSC	Approved	1.0	17/01/2006	Withdraw this policy – move key policy statements moved to GISP8 section on Offsite access control
Procedures	**ICT Contingency Plan - Top Level**	This document provides a description of the management process and guide for the recovery of the information systems and associated processes immediately following an incident interrupting service.	https://intranet.uea.ac.uk/is/itregs/businesscontinuitydisasterrecovery	ISSC	Approved	2.1	17/06/2010	No change
Procedures	**PC and Laptop Admin Rights**	Policy on the availability of local administrator rights to end users on UEA supplied PC equipment (laptop and desktop).	http://www.uea.ac.uk/is/itregs/ictpolicies/PC+and+Laptop+Admin+Rights	ISSC	Approved	2	03/02/2012	No change
Procedures	**Procedures for communicating passwords to users [SP1]**	Basic procedure for communicating passwords to users: new users or when dealing with incidents that required a	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/Procedures+for+Communicating+Passwo	ISSC	Approved	1.0	04/02/2011	Added to GISP5 Use of passwords – Implementation section

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
		password change	rds+to+Users					
Procedures	**Procedures for dealing with malware infected desktop computers [SP2]**	Procedures that should be followed when a desktop computer has been detected as being infected by malware	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman/SP2-malware-infected-computers	ISDMT	Approved	1.1	21/03/2011	No change
Procedures	**Reporting emails with inappropriate content**	Guidance on which inappropriate emails should be reported and how to do this	https://intranet.uea.ac.uk/is/itregs/Reporting+emails+with+inappropriate+content		Approved		22/03/2007	No change
Procedures	**Security Manual**	The Security Manual contains information about a number of security controls. Each security control is maintained separately	https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman	ISSC	Approved		12/05/2009	Withdraw the Security Manual and combine it with associated GISP sections
Procedures	**Software Copyright Acknowledgement**	Statement applying to use of software, computer readable datasets, or courseware by students or members of staff	https://intranet.uea.ac.uk/is/itregs/softwarecopyright					No change

Type	Title	Description	Link	Authorised by	Review status	Current Version	Date released	Review action
Guidelines	**Email guidelines for effective communication**	Advice on how to use email as an effective communication tool	https://intranet.uea.ac.uk/is/itregs/userguide/emailguide	ISDMT	Approved		Dec-2009	Add statement on taking care with unsolicited email and links on use of encryption