University of Strathclyde Glasgow

INFORMATION SECURITY POLICY

14/5/2013

Information Security Working Group

University wide policy for Information Security produced by the Digital Campus Sub Committee.

Contents

1 BACKGROUND

“Information is now critical to many organisations and education is one of the sectors that is most dependent upon it. In many ways information is the main business of education”

JANET, Training Information Security Policies

“Information security is the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have a right to do so”

UCISA Information Security Toolkit

“The purpose of an information security policy is to help manage risk and reduce it to an acceptable level”

Information Security, BIS

Within the University of Strathclyde the importance of information as a corporate asset is well recognised. For this reason the University has charged the Digital Campus Sub Committee of the Information Strategy Committee with developing, implementing and managing an Information Security Policy with the following objectives:

- Improving the operation of the Institution by ensuring that information is available to the appropriate individuals when and where it is needed
- Maintaining the integrity of information
- Ensuring that appropriate levels of confidentially are maintained
- Reducing the risk to the Institution due to poor information management
- Ensuring compliance with the Institutions’ legal and regulatory responsibilities
- Improving the understanding of all relevant parties of their information security and information management responsibilities.

2 SOURCE

This policy has been adapted from the guidance in the “UCISA Information Security Tool Kit” which, in turn, is based upon the guidelines set out in the industry standard ISO 27001. This guidance has been adapted to fit the needs of the University of Strathclyde rather than conforming exactly to a particular standard.

3 UNDERLYING PRINCIPLES

The principles of this policy are:

- To ensure that the University complies with all legal requirements
- To ensure the appropriate availability, confidentiality and integrity of all University held information, regardless of its format

- To have a risk aware approach that addresses any unacceptable risks, while allowing a knowledgeable and reasoned acceptance of other risks
- To ensure that individuals (staff, students and other people managing information within the University) understand that they have personal responsibilities for ensuring information security
- To follow UK standards where relevant

4 STRUCTURE

The Information Security Policy of the University consists of this high-level overarching document and a number of supporting documents. These supporting documents can be policies, procedures, guidelines, frameworks, codes of practices, or a combination thereof. The list of these supporting documents will change overtime and is located at:

https://moss.strath.ac.uk/infostratportal/infosecurity/Lists/Underlying%20Policy%20Documents/AllItems.aspx

Appendix 1 has a list of these documents as of the 2nd of May 2013.

5 SCOPE

This policy applies throughout the University. It applies to anyone within the University who creates, manages or uses information that is owned, managed or stored by the University. This includes staff, students and any third parties with specific responsibilities relating to such information.

The scope of the individual supporting documents is specified within the list of those documents.

6 GOVERNANCE

Responsibility for the production, implementation, maintenance, approval and communication of this overarching Information Security Policy is delegated to the Digital Campus Sub Committee of the University’s Information Strategy Committee. The operational framework for the Digital Campus Sub Committee in managing this responsibility is outlined in section 7.

Responsibility for the production, implementation, maintenance, approval and communication of the individual supporting documents is specified within the list of underlying documents.

7 OPERATIONAL FRAMEWORK

What does the Framework look like?

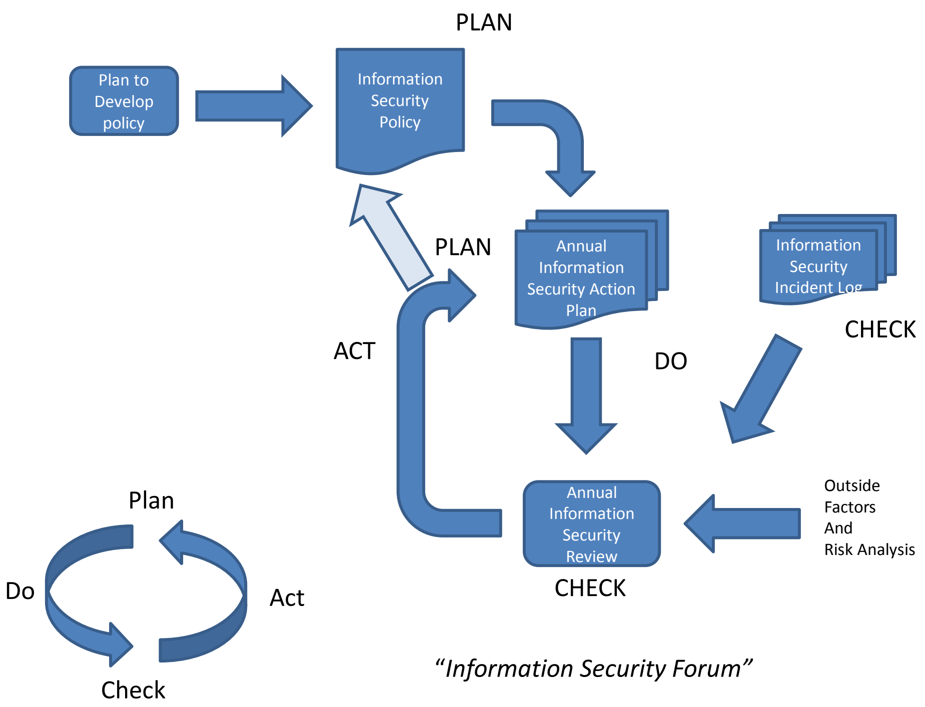
PLAN
Plan to Develop policy
Information Security Policy
PLAN
Annual Information Security Action Plan
Information Security Incident Log
CHECK
ACT
DO
Annual Information Security Review
Outside Factors And Risk Analysis
CHECK
Plan
Do
Act
Check
"Information Security Forum"

FIGURE 1: FRAMEWORK FOR THE MANAGEMENT OF INFORMATION SECURITY

The operational framework for the Management of Information Security (Figure 1) will allow the Digital Campus Sub Committee to operate as a virtual Information Security Forum for the University. The purpose of such a forum being to:

- Discuss, develop and approve the University's information security policies and associated underlying documents
- Ensure a consistent and effective approach to information security
- To monitor the effectiveness of the information security arrangements and practices of the University
- Improve information security in the light of lessons learned and changes to the organisation and its environment.

In order to do this a "Plan, Do, Check, Act" approach will be adopted as recommended by JANET within their training materials on Information Security.

- Plan – determine the actions to be taken to improve Information Security and record these within the ***Information Security Action Plan***.
- Do – carry those actions out
- Check – reviewing the completed Action Plan, the ***Information Security Log*** and the Information Security Risk Assessment
- Act – via an annual ***Information Security Review***

7.1 Information Security Action Plan

On an annual basis the Digital Campus Sub-Committee will produce an Information Security Action Plan for June each year. This Action Plan will be located at:

https://moss.strath.ac.uk/infostratportal/infosecurity/Lists/Policy%20Development%20Action%20Plan/AllItems.aspx

This plan will identify the particular tasks that should be completed in the following academic year relating to Information Security. Examples of tasks will include developing new policies, reviewing and updating existing policies, conducting staff training, policy dissemination activities, and tasks to mitigate or reduce risks associated with Information Security.

While the plan will initially be drawn up in June each year it is recognised that within the constantly changing University environment it will be necessary to make changes to the plan, in particular to add in some actions and remove/de-scope others during the year. The Action Plan must include assigning resources and responsibility for each task, must be prioritised and must take into account resource availability.

7.2 Information Security Incident Log

A log will be maintained within the ISD Help Desk software in which all Information Security Incidents will be recorded along with details of any action taken. All staff (from all Departments, Faculties, and Directorates of the University) will have a responsibility to log with the ISD Help Desk any incidents that occur and which impact or have a potential impact on Information Security. It should be noted that in an organisation as large and complex as the University there will be many Information Security Incidents each year.

The Assistant Director of Information Services responsible for IT is copied into each security incident logged. Should the incident have any financial impact or potential reputational impact on the University she will report this to the Director of Information Services. He will evaluate the situation and if he deems it necessary report this to the Chief Operating Officer. The Chief Operating Officer would make the decision of whether it was a serious incident that must be reported to the Executive Team and the Audit Committee.

Information Security Incidents can also be Data Protection Incidents and, thus, on occasions a potential Data Protection Incident will be reported via the ISD helpdesk. Such Data Protection Incidents will be referred onward by the Assistant Director immediately to the Information Governance Manager (within the Strategy and Planning Directorate) who will follow the agreed procedures within the Data Protection Policy.

7.3 Information Security Risk Management Process

The Digital Campus Sub Committee will be responsible for identifying and managing Information Security related risks. Where necessary, such risks will be escalated via the University's established risk management procedures for the Information Strategy Committee. Addressing and managing specific risks may be included in the annual Information Security Action Plan.

7.4 Information Security Annual Review

On an annual basis, the Digital Campus Sub Committee will produce an Information Security Annual Review for the Information Strategy Committee. This review will include:

- A report of the delivery of the Action Plan for the previous academic year
- A summary of the Information Security Incident Log for the previous year
- A summary of active Information Security related risks
- Identification of any new information management issues
- Any amendments being made to the Information Security Policy
- Presentation of the initial Action Plan for the following academic year.

7.5 Updating the Information Security Policy

The Digital Campus Sub Committee is responsible for identifying and enacting any changes required to the Information Security Policy. This committee should consider on an annual basis whether such changes are required, including making any such changes in the on-going Information Security Action Plan

APPENDIX 1 – LIST OF SUPPORTING DOCUMENTS AS OF THE 2ND OF MAY 2013

Title	Description	Document Types	Responsible Area or Dept	Document Status	Date Produce	Date to be produced by	Review Date	Review Cycle	Approver	Date Approved
Third party system access	Access to University services by third parties, usually for the purpose of support (not individual end user access)	Policy and Procedural	Information Services	Under development		26/07/2013		3 - years	ISD Change Management Group	
System Operating Procedures	Document outlining - System operations; systems Planning; Systems management; capacity Planning as per the document described in the UCISA Information Security Tool Kit	Procedural	Information Services	Required	01/04/2016			2 years	Manager for the relevant "IT Department"	
network Management	Document outlining the policies for connecting to the University network	Policy	Information Services - Infrastructure	Existing			28/02/2014	5 years	Digital Campus Sub Committee	
Software Asset Management	Management of software assets	Policy and Procedural	Digital Campus Sub Committee	Under development		27/12/2013		5 years	Digital Campus Sub Committee	
IT Incident Management	Management of IT Incidents	Policy and Procedural	Information Services	Existing	01/10/2011		01/10/2014	3 - years	ISD Change Management Group	01/10/2011
IT Change Management (ISD)	Managing the change control process for making changes to centrally managed IT systems or infrastructure.	Policy and Procedural	Information Services	Existing	01/10/2011		01/10/2014	3 - years	ISD Change Management Group	01/10/2011

Title	Description	Document Types	Responsible Area or Dept	Document Status	Date Produce	Date to be produced by	Review Date	Review Cycle	Approver	Date Approved
University Policy on the User of Computing Facilities and Responses	This policy covers the acceptable use of all computing facilities and resources administered by the University of Strathclyde, whether on- or off-site, including use by staff and students of the University and by any other person authorised to use these facilities.	Policy	Digital Campus Sub Committee	Existing	01/11/2012		01/11/2014	2 years	Digital Campus Sub Committee	01/11/2012
Data Protection Policy	University Data Protection Policy	Policy	Information Compliance	Existing	25/10/2012		25/10/2015	3 years	Digital Campus Sub Committee	25/10/2012
Records management Policy	University Records Management Policy	Policy	Information Compliance	Existing	11/05/2009		11/05/2014	5 years	Elaine Forbes	11/05/2009
Records Management Guidelines	Guideline document for complying with Records Management Policy and good information management practices	Guidelines	Information Compliance	Existing	01/04/2012		01/04/2017	5 years	Elaine Forbes	01/04/2012
ICT Legal Framework	Document outlining the ICT legal environment in which the University, its staff and students operate.	Guidelines	Information Compliance	Existing	01/11/2012		01/11/2013	Annual	Digital Campus Sub Committee	01/11/2012
End User Management	Document to outline how end user accounts are managed	Policy and Procedural	Digital Campus Sub Committee	Required		01/03/2015				
Disaster Recovery Framework	Framework for Disaster Recovery arrangements across the University	Policy and Procedural	Information Services	Under development	01/07/2013					
Good Information Management Guidelines	Guidance for good practice when managing information	Guidelines	Information Compliance	Not required as covered by a separate document						

Title	Description	Document Types	Responsible Area or Dept	Document Status	Date Produce	Date to be produced by	Review Date	Review Cycle	Approver	Date Approved
Guidance on Confidential and personal information	Guidance on how to identify if information is confidential or personal.	Guidelines	Information Compliance	Existing	01/11/2012		01/11/2017	5 years	Digital Campus Sub Committee	
Procedure for gaining access to allocated resources	A procedure document for dealing with requests to access information within the email or private storage (H:) of other people, usually for business continuity purposes when the original "owner" is unavailable.	Policy and Procedural	Information Services	Existing	01/11/2012		01/11/2015	3 years		
Protection of Information Held on Mobile Devices and Encryption Policy	A policy document outlining the University's policy on mobile information and encryption	Policy	Digital Campus Sub Committee	Existing	28/03/2013		28/03/2016	3 years	Digital Campus Sub Committee	28/03/2013
Use of Social media and Cloud services		Policy	HR	Required		20/12/2013				
Intellectual Property Policy		Code of Practice	RKES, HR	Not required as covered by a separate document						
PCI DSS Compliance	To ensure PCI DSS Compliance	Policy and Procedural	Finance	Required		31/7/2013	31/7/2014	Annual	Chief Financial Officer	
Paper files	Management Plan	Policy and Guidelines	To be identified	Required						

Title	Description	Document Types	Responsible Area or Dept	Document Status	Date Produce	Date to be produced by	Review Date	Review Cycle	Approver	Date Approved
Archiving Policy	Will point to digital preservations in addition to print preservation, institutional records for running the business and potentially research data material depending on final outcomes for the funding council mandates. We have statements for some of these areas (archives & special collections collection policy, brief record retention statements which require more working up,) but not all, and any final consolidated statement would depend on technology available to cope with the permanent digital preservation	Policy and Procedural	ISD	Required		29/05/2015		after 1 year and five years there after	University Librarian	
Management of Third Party Owned Data Sets	there are instances where a third party (e.g. a research funder) ‘loans’ a dataset to the university in order for the dataset to be used as the basis, or part of, a research project. These datasets may be confidential or commercially sensitive and will be loaned with strict terms and conditions.	Policy	RKES	Required		25/04/2014	25/04/2015	Annual		