University of Sunderland – Business Assurance

Information Risk Policy

Document Classification: **Public**

Policy Reference – Central Register	IG006_______________________________
Policy Reference – Faculty / Service	**IG 006**
Policy Owner	**Director of Business Assurance**
Date Policy Written	**July 2014**
Date Policy Last Updated	
Author	**Assurance Manager, Business Assurance**
Date to Information Governance Group	
Date to Executive	
Date for next Review	**December 2016**
Comments	

1. Introduction

The University recognises the value and importance of the information it holds and places high importance on minimising information risk and safeguarding the interest of students, staff and the organisation.
Information risk is inherent in all organisational activities and everyone working for, or on behalf of the University, has a responsibility to continuously manage information risk. The aim of information risk management is to provide the means to identify, prioritise and manage the risks involved in all of the organisation's activities whilst supporting the University's aims and objectives.

2. Purpose and Scope

This policy applies to all University staff and independent contractors, and to all information, in all formats.

This high-level information risk policy is a key component of the University's overall information governance framework and should be considered alongside other information governance documentation including policies set out in the Overarching Information Governance Policy and other guidance, protocols and procedures.

3. Definitions

Information Risk:	the chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.
Information Risk Management:	defines the areas of an organisation's information infrastructure and identifies what information to protect and the degree of protection needed to align with the University's tolerance for risk. It identifies the business value, business impact, compliance requirements and overall alignment to the organization's business strategy.
Information Asset:	come in many shapes and forms and include: • personal information e.g. content within databases, archive and back up data, audit data, paper records (health, social care and staff records) • software e.g. application and system software, data encryption utilities, development and maintenance tools • hardware e.g. PCs, laptops, USB sticks, PDA • system/process documentation e.g. system information and • documentation, manual and training materials, contracts, business continuity plans
Information Asset Register:	a record of all information assets along with the associated Information Asset Owner
Consequence	the outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Likelihood	a qualitative description or synonym for probability or frequency
Risk Assessment	the overall process of risk analysis and risk evaluation.
Risk Management	the culture, processes and structures that are directed towards the

	effective management of potential opportunities and adverse effects.
Risk Treatment	Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies: • Avoid the risk • Reduce the likelihood of occurrence • Reduce the consequences of occurrence • Transfer the risk • Retain/accept the risk
Privacy Impact Assessment	Privacy Impact Assessment is usefully defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a search is undertaken for ways to avoid or minimise privacy concerns.

4. Roles and Responsibilities

All individual employees and contractors have responsibility for ensuring that they comply with this policy and any related policies and guidance. Staff should attend training and awareness sessions provided by the University. Employees also have a duty to report any incidents or 'near misses' in relation to information security.

The University has identified the following roles specific to the management of information risk:-

Role	Responsibility
Senior Information Risk Owner (SIRO) **Director of Business Assurance**	• ensuring that an overall culture exists that values and protects information within the University • owning the University's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used • owning the University's information incident management framework
Information Asset Owners (IAO)	• maintaining a register of information assets under their ownership and associated risks • supporting the SIRO in ensuring that information risk assessments are performed on all information assets to which they have been assigned 'ownership' • submitting risk assessment results and associated mitigation plans to the SIRO for review • reviewing and authorising requests for access to information assets • ensuring information risk assessments are carried out prior to any new or change to a system, electronic or manual, which impact their information assets • reporting data breaches and assisting in the management of incidents in relation to their information assets • ensuring all information flows from information assets are appropriate, documented and secure in transit • ensuring information assets are included in Business Continuity Plans

Information Asset Administrators (IAAs)	• providing administrative support to assist the IAO

Additionally the information risk management process will be supported by:

Information Governance Group (IGG)	• accountable to the University's Business Assurance Board, the Information Governance Group will act as a programme board for direction of the University's overall approach to Information Governance, including information risk management • review the University's information asset register and information risk register to provide assurance that risks are being captured and effectively managed
Deans of Faculty and Directors of Support Services	• ensuring that appropriate members of staff, in each Faculty and Service, take on the role of IAO for information assets within their area • ensuring compliance with the University's Information Governance policies • ensuring any issues of non-compliance are addressed
Assurance Manager (Business Assurance - Information Governance)	• drawing up information governance policy, process and guidance and ensuring compliance with this policy • overseeing the Information Governance Framework and ensure its successful operation • developing and implementing an information risk training programme • collating and maintaining a central information asset register and information risk register • facilitating incident investigation • supporting the SIRO
The **IT Security Manager (ITS)**	• developing IT Security Policy, standards and guidelines • ensuring that effective IT Security systems, controls and training programs are operationally implemented, fit for purpose and available across the University.
Legal Support and Data Protection Officer	• developing policy, process and guidance relating to Data Protection • advising on collecting, using and protecting personal information
Assurance Manager (Business Continuity/ Insurance)	• providing advice and guidance with regards to business continuity planning and insurance

5. Policy Detail

Information Risk Management Assurance Framework

The Information Risk Management Assurance Framework aims to:

- Protect students, staff, the University and partner organisations from information risks.
- Ensure the University meets its legal and statutory requirements
- Support the strategic Assurance Framework by identifying and assessing risks in the approval, review and control processes.
- Encourage pro-active rather than re-active information risk management.
- Contribute to the quality of decision making throughout the organisation by facilitating the timely retrieval of robust information.

Assessment of Information Risk

Information risk management is the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding

what countermeasures, if any, to take based on the value of the information resource to the organisation.

Identification and a threat assessment of risks related to the University's information assets will be carried out in line with the University approved processes and procedures.

The University will assess information risk in a number of ways, which will include the following:

- Regular review of routine and adhoc flows of information to ensure any risks identified with these flows are mitigated, including ensuring appropriate controls are in place.
- Undertaking of Privacy Impact Assessments (PIAs) and Supplier Information Security Assessments as appropriate when introducing new systems or processes.
- Maintaining and regularly reviewing information assets, taking into consideration an ever changing threat landscape and business impact
- Considering and recording information risks when reviewing proposed changes to existing / live systems through the Change Approval Board and project lifecycle.
- Considering new and existing risks when dealing with incidents, ensuring lessons are learnt

A template to assist in assessing information risk is provided in Appendix A.

6. Training and Education

Information is the lifeblood of the University. It is essential that a culture is developed whereby information management is part of everyday activities and becomes part of the culture of the organisation. Increasing staff awareness is key to successfully implementing a University-wide approach to Information Governance. Training and awareness will be available to all staff:

Induction

All newly employed staff will receive basic guidance in organisational policy in relation to information governance as part of the University's induction.

Information Governance Training

All staff will receive basic Information Governance training, at least 3 yearly. Additionally service specific and subject specific training will be provided as appropriate and necessary to inform staff of policy and process.

Information Risk Management Training

Information Risk Management training will providing to all staff who have involvement in the information risk management process. Training will be relevant to the role to be performed.

Training will be deployed using a variety of techniques including:-

- e-learning
- face to face training sessions
- facilitated workshops

7. Related Policies

This policy should be read in conjunction with the policies listed in Appendix A of the Overarching Information Governance Policy.