St Georges University of London

Information Risk Procedure

1 Introduction

1.1 This document sets out St Georges University of London's (SGUL) commitment to the management of information risk and also sets out what SGUL, their 'delivery partners' and third party suppliers should do to manage information risk. In doing so, this procedure supports the SGUL strategic risk management aims and objectives and should enable employees throughout the organisation to identify an acceptable level of information risk and, when required, use the correct risk escalation process.

2 Responsibility

2.1 To provide evidence that information risks within SGUL have been identified and that there are plans in place for managing them the Data Protection Officer (DPO) is responsible for compiling and maintaining an Information Risk Register.

2.2 All Directors in their capacity as Information Asset Owners (IAOs) are responsible for reviewing information risks on a regular basis and reporting on these at Information Governance Steering Group meetings. The review must also consider forthcoming potential changes in services, technology and threats. Any major risks that arise between these meetings must be immediately escalated to the Senior Information Risk Owner (SIRO) and if these have arisen during an Data Breach then the DPO must be informed.

2.3 The Director Information Services is to assure all IAOs that any IT systems that hold protectively marked information are accredited according to government standards.

3 Controls

3.1 An Information Risk Register, maintained by the DPO, will be updated regularly by the IAOs with information explaining identified risks and the risk management decisions they that have been taken.

3.2 The Information Risk Register should contain, as a minimum, the following information:

- a description of each risk expressed in terms of the potential or actual compromise associated with the risk and the cause (threat and vulnerability),

- an indication of the Information Assurance (IA) controls already in place to remediate each risk,
- a rating that reflects the likelihood of the risk being realised and is typically expressed in terms of the ‘score’ assigned by the risk assessment method used,
- a rating that reflects the business impact associated with the threat being realised is typically expressed in terms of the ‘score’ assigned by the risk assessment process,
- a description of the controls that the business group has or plans to implement to further control the risk (together with any additional actions or contingency arrangements that lessen the business impact if the risk is realised), and
- a target date for implementing proposed controls or other plans to reduce the risk further.
- A target rating that reflects the score following the implementation of the further controls
- In support of the Information Risk Register SGUL will have an Information Asset Register in place, this can be used to help to identify the different types of information assets held and provide direction on the risk to the organisation that a loss / compromise or lack of availability of that asset would have.

3.3 **Assurance**

3.3.1 The DPO will inform the IGSG, chaired by the SIRO, of all information risks and make recommendations on those which should be notified to the Executive Board.