Information Management and Policy Services (IMPS)

Information Security Incident Response Procedures

To be read in conjunction with the Information Security Incident Response Policy.

1 Introduction

1.1 The purpose of this document is to provide instruction and guidance on reporting and managing information security incidents. Information security incidents are defined as those involving actual or potential compromise or disclosure of, and/or unauthorised access to, University data to include:

- Sensitive nonpersonal data including information of an operational and/or confidential nature, research data, data given in confidence by third parties or data of any kind which is given or the University is required to hold under a contractual confidentiality obligation;
- Personal data (data that identifiki

- Data Protection Officer
- Director and/or Assistant Director (s) of DTS
- Director of Legal Services (or alternate)

3.4 The ISIT will then establish if further assistance or notifications are required in line with the Information Security Incident Team: Incident Response (Appendix C). Where necessary, the following Lead Officers will be notified and included in the ISIT:

- DTS staff and specialists
- Business Continuity Officer
- Director of Internal Audit Services (or alternate
- Head of News – Corporate Communications (or alternate)
- Director of HR (or alternate)
- Heads of School, Department or Function
- A relevant member of University Executive Board

3.5 Where the incident involves any suspected criminal activities, the ISIT will designate a Lead Officer to ensure the matter is reported to the Police.

3.6 Where the incident involves personal data, the Lead Officer for IMPS will assess the volume and sensitivity of the data involved and advise the ISIT on whether it is necessary to:

- Inform any affected individuals
- Notify the Information Commissioner's Office

3.7 Where theWheissioner'

4.2 Information Security Incident Reports analysis and data will be reported into the ISG by the IMPS Officer.

4.3 The ISG will review incidents reported on a quarterly basis to establish if:

- Changes to existing policy is required to improve information management practices;
- additional or improved communications, training or resources for University data users are required to prevent similar occurrences;
-

APPENDIX A: SECURITY INCIDENT REPORTING FORM

INFORMATION SECURITY INCIDENT REPORTING FORM

This form should be completed in the event of an actual, suspected or potential Information Security Incident.

This form should be completed