Academic Services

Data Security Breach Management Procedure

Document Reference:	*Data Breach Procedure 1.1*
Document Type:	Procedure
Document Status:	v1.0 Approved by ISSG v1.1 Issued
Document Owner:	Caroline Dominey
Review Period:	Annual
Next Review Date:	August 2015

Last Reviewed:	July 2014 – minor changes only

1 TABLE OF CONTENTS

2 DOCUMENT HISTORY

2.1 DOCUMENT LOCATION

This document can be accessed from the following location:

N:\ITGovernanceCompliance\Records Management\Policy & Procedures\20130322_Data Breach Procedure_1.0.docx

2.2 REVISION HISTORY

The latest revision can be found at the top of the list:

Revision Date	Author	Version	Summary of Changes
February 2013	Caroline Dominey	0.1	First Draft
March 2013	Caroline Dominey	0.2	Incorporated comments from Paul Sandy
March 2013	Caroline Dominey	1.0	Incorporated final amendments from ISSG

2.3 APPROVALS

This document requires the following approvals:

Name	Version	Date of approval
Information Security Steering Group	1.0	22 March 2013 (Approved v0.2 to become approved v1.0)

3 WHAT IS A DATA SECURITY BREACH?

A data security breach is considered to be any loss of, or unauthorized access to, University data, normally involving University Personal or Confidential information[1] including intellectual property. Data security breaches include the loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, human error (e.g information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.

4 MANAGING A DATA SECURITY BREACH

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. Breaches can result in fines of up to £500,000 for loss of personal information and significant reputational damage, and may require substantial time and resources to rectify the breach. The following procedure outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently.

This procedure outlines the four stages (4.2 to 4.6 below) which should be completed following the initial containment of the breach. The individual stages may run concurrently.

4.1 RECORD KEEPING

Throughout the breach management process records should be kept of what action has been taken and by whom. Appendix C provides an activity log template to record this information, in addition copies of any correspondence relating to the breach should be retained.

4.2 SECURITY BREACH PROCEDURE

4.2.1 Containment & recovery

As soon as a data security breach has been detected or is suspected the following steps should be taken:

a) Identify who should lead on investigating and managing the breach
b) Establish who (within the University) should be aware of the breach – you must contact the IT Governance & Compliance Team via the helpdesk
c) Identify and implement any steps required to contain the breach

[1] Personal and Confidential Information have the same definition as in the University Policy for Information on laptops and portable media: **Personal information** is defined as any information relating to a living individual who can be identified either from the data, or from that information used in conjunction with other information that may be available. **Confidential information** is privileged or proprietary information that could cause harm (including reputational damage) to the University or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure.

d) Identify and implement any steps required to recover any losses and limit the damage of the breach
e) If appropriate inform the police/insurance office

4.2.2 Assessment of risk

All data security breaches must be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach should be assessed in order to identify an appropriate response. The checklist in Appendix A should be used to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

4.2.3 Notification of breach

Consideration is required as to whether any individuals, third parties or other stakeholders should be notified of the breach. This will depend on the nature of the breach, any notification must be carefully managed. Don't be too quick to disclose information before the full extent of the breach is understood; when disclosure is required ensure that it is clear, complete and serves a purpose. The checklist in Appendix B: Notification of breach checklist should be used to identify potential stakeholders who should be notified and to establish what information should be disclosed.

The Director of Communications or other senior manager must be involved in the notification process and no message sent without approval. The Information Commissioner's Office may be notified only after liaison with the University Data Protection Officer.

4.2.4 Evaluation and response

It is important to investigate the causes of the breach and evaluate the University's response to the breach. A brief report on the breach, how it was dealt with and recommendations on how to prevent the breach reoccurring and similar risks should be written. All significant breaches must be reported in the Information Security Steering Group.

Finally if there are recommended changes to this procedure, such as additional information that would have been helpful or further explanation required these should be communicated to IT Governance and Compliance.

5 FURTHER RESOURCES AND CONTACT DETAILS

5.1 RESOURCES

- ICO guidance on Data Security Breach Management
- Notification of Data Security Breaches to the ICO

5.2 CONTACTS

- To report an urgent security breach please contact the helpdesk immediately

- Other useful contacts[2]:
  - Helpdesk (ext: 3934 or 4724)
  - University Records Manager, dataprotection@exeter.ac.uk
  - Information Security Team, infosecurity@exeter.ac.uk
  - Allan Edgcumbe, Head of Security/Estate Patrol
  - Jane Chafer, Director of Communications and Corporate Affairs
  - University Insurance Services, insurance@exeter.ac.uk, (ext: 3087)

[2] Once the Procedure is approved all contacts will be notified and provided with details of expected input.

APPENDIX A: SECURITY BREACH RISK ASSESSMENT CHECKLIST

a) What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)

b) How did the breach occur?

c) What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)

d) How many individuals or records are involved?

e) If the breach involved personal data, who are the individuals? (Students, staff, research participants etc)?

f) What has happened to the data?

g) Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)

h) Were there any protections in place? (e.g. Encryption)

i) What are the potential adverse consequences for individuals or the University? How serious or substantial are they and how likely are they to occur?

j) What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?

k) What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted)

APPENDIX B: NOTIFICATION OF BREACH CHECKLIST

WHO TO NOTIFY

There should be a purpose to notifying individuals of a breach, it may be that there are steps they need to take to protect themselves, we may be legally or contractually obliged to report breaches to stakeholders or we may need to manage potential reputational damage. The following (non exhaustive) list identifies key external stakeholders who may require notification.

- Police – in the case of criminal activity
- Individuals whose data has been compromised
- Information Commissioner's Office (ICO) - There is no legal obligation to inform the ICO, but serious breaches should be reported.
- Regulatory bodies, Funders, Research Partners
- Others – e.g. banks where steps may be required to protect accounts, press

WHAT TO SAY

Communication and Marketing Services will be able to advise on the content of any message sent. Any notification message should not be sent too quickly, it is important that we understand the extent of the breach and are able to provide useful information, whilst at the same time if there are important steps that individuals need to take this should be communicated promptly.

You should consider including the following:

- Details of the what happened and when the breach occurred
- What data was involved
- What steps have been taken to contain the breach and prevent reoccurrence
- Advice on what steps they should take e.g. contact banks
- How will you help and keep them informed (if necessary)
- Provide a way to be contacted

APPENDIX C - ACTIVITY LOG[3]

DATE/TIME	ACTIVITY Activity, Decision, Instruction or Briefing (A, D, I or B)	ACTION	OWNER	COMPLETED
e.g.25/10/11 12:20	*B - received notification of personal data available on website*	*Informed Web Team and request immediate page take down*	*F Smith*	*13:00*

Completed by .....

[3] Taken from template for University Business Continuity Plan