Information Security Incident Management

Data Breach Procedure

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document control

Version history

Version	Date	Comments
0.1	28 Aug 2020	First draft
1.0	02 Sept 2020	Minor amendments and issue

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 26 Jan 2018
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A16 – Information security incident management
ISO 27001:2013 Conformance Control	Information Classification Objective A.16.1 - Management of information security incidents and improvements

Data Breach Procedure

1. Purpose and Scope

1.1 The University is obliged under Data Protection legislation to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

1.2 This procedure sets out the action to be followed to ensure a consistent and effective approach is in place for managing data breaches and is aligned to the BUL ISMS information security incident management policy and procedure across the University.

1.3 This procedure relates to all personal and special categories (sensitive) data held by the University regardless of format.

1.4 This procedure applies to all staff and students at the University. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the University.

1.5 The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

2. Types of Data Breach

2.1 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

2.2 An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the University's information assets and / or reputation.

2.3 An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record).
- equipment theft or failure.
- system failure.

- unauthorised use of access to, or modification of data or information systems.
- attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- unauthorised disclosure of sensitive / confidential data.
- website defacement.
- hacking attack.
- unforeseen circumstances such as a fire or flood.
- human error.
- 'Scam' offences where information is obtained by deceiving the organisation who holds it.

3. Reporting an incident

3.1 Any individual who accesses, uses or manages the University's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer and IT customer Services. data-protection@brunel.ac.uk and computing-support@brunel.ac.uk.

3.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

3.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).

3.4 All staff should be aware that any breach of Data Protection legislation may result in the University's Disciplinary Procedures being instigated.

4. Actions for Containment and recovery

4.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

4.2 An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and who within InfoSec will take the lead investigating the breach, as the Investigation Officer. This will depend on the nature of the breach and in some cases, it could be the CISO.

4.3 The Investigation Officer (IO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

4.4 The IO will establish who may need to be notified as part of the initial containment and will inform the ICO and police, where appropriate.

4.5 Advice from experts across the University may be sought in resolving the incident promptly.

4.6 The IO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

5. Investigation and risk assessment

5.1 An investigation will be undertaken by the IO immediately and wherever possible, within 24 hours of the breach being discovered.

5.2 The IO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6. Notification

6.1 The IO and / or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

6.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

6.2.1 whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation;

6.2.2 whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);

6.2.3 whether notification would help prevent the unauthorised or unlawful use of personal data;

6.2.4 whether there are any legal / contractual notification requirements;

6.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the University for further information or to ask questions on what has occurred.

6.4 The CISO and DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

6.5 The CISO and the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

6.6 A record will be kept of any personal data breach, regardless of whether notification was required.

8 Evaluation and response

8.1 Once the initial incident is contained, InfoSec in liaison with the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3 The review will consider:

8.3.1 where and how personal data is held and where and how it is stored.

8.3.2 where the biggest risks lie including identifying potential weak points within existing security measures.

8.3.3 whether methods of transmission are secure; sharing minimum amount of data necessary.

8.3.4 staff awareness.

8.3.5 implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by University Executive Board.

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Information Asset Owner / Head of Department immediately, complete Section 1 of this form and email it to the Data Protection Officer and computer support Helpdesk where appropriate

Section 1: Notification of Data Security Breach	**To be completed by person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Investigation Officer in consultation with the CISO and DPO and if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to vulnerable adults and children;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	

Data Protection Officer and/or Investigation Officer to consider whether it should be escalated to the appropriate University Executive Committee member	