Document Control Sheet

Document Control			
Document Title	Policy for Information Security Incident Management		
Version Number	Final_1.1		
Author(s) (name, job title, department)	Gareth Pritchard, Business Manager, Corporate		
Authored Date:	13/03/2018	Date Approved:	13/06/2018
Approval Committee:	ICT Committee	Date of Next Review:	13/02/2021
Superseded Version:	Policy for Information Security Incident Management_final_v1.0		

Version Control			
Version	Author	Date	Changes/Purpose
Draft_v1.0	Gareth Pritchard	13/02/2018	Initial Draft
Final_v1.0	Gareth Pritchard	13/06/2018	Policy Approved
Final_v1.1	Gareth Pritchard	23/08/2018	Reformatting

Policy for Information Security Incident Management

Institute for Optimum Nutrition

1. Introduction and scope

1.1 The Institute holds a large amount of information in a variety of media, physical and otherwise (including photos and videos). This includes personal and sensitive personal data, and also non-personal information which may be sensitive or commercially confidential (e.g. financial data) and may be subject to legal obligations of confidence, whether contractual or otherwise).

1.2 The Institute has legal responsibilities both under the Data Protection Act and in respect of its own business (for example, under the common law of confidence) to safeguard information in its control. Care should be taken to protect information, to ensure its integrity and to protect it from loss, theft or unauthorised access.

1.3 In the event of an information security incident (also referred to as a 'data breach'), it is vital that appropriate action is taken to minimise associated risks. A risk analysis should be performed, factors which need to be considered are:

- The number of individuals affected
- Type of data involved
- Impact (on individuals, the Institute or its contractors)

1.4 Any member of staff, student, contractor or pseudo-employee discovering or suspecting an information security incident must report it in accordance with this policy.

2. What is an information security incident?

2.1 An information security incident in an event whereby data held by the Institute, in any format, is compromised by being lost, destroyed, altered, copied, transmitted, stolen, used or accessed unlawfully or by unauthorised individuals whether accidentally or on purpose. Some examples:

- Loss, or theft of equipment on which data is stored, e.g. laptop or mobile phone
- Unauthorised access to data
- Human error, e.g. emails to wrong recipient; public posting of confidential material online; incorrect sharing of Google documents
- Failure of equipment or power leading to loss of data
- Hacking attack

- Data maliciously obtained by way of social engineering (an attack in which a user is 'tricked' into giving a third-party access, often by purporting to be someone other than they actually are)

2.2 Information security incident reporting also includes instances of 'near misses' and identification of vulnerabilities where IT Services considers there is a high likelihood of an actual incident occurring.

3. Reporting of the breach

3.1 All Information security incidents should be reported immediately to Business Manager on 020 8614 7809, as the primary point of contact.

3.2 The report should include full and accurate details of the incident, including who is reporting the incident; what type of data is involved (not the data itself unless specifically requested); if the data relates to people and if so, how many people are involved.

3.3 The Business Manager is responsible for maintaining a confidential log of all information security events.

4. Investigation and response

4.1 The Business Manager will consider the report, and where appropriate, instigate a Response Team. Membership will depend on the type and severity of the incident. The response team will be responsible for investigating the circumstances and effect of the information security incident. An investigation will be started into material breaches within 24 hours of the breach being discovered, where practicable.

4.2 The investigation will establish the nature of the incident, the type of data involved, whether the data is personal data relating to individuals or otherwise confidential or valuable. If personal data is involved, associated individuals must be identified and, if confidential/valuable data is concerned, what the legal and commercial consequences of the breach may be.

4.3 The investigation will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss. This will include risk of damage and/or distress to individuals and the institution.

4.4 The response team is responsible for formally documenting the incident and associated response. This information will (as a minimum) be subject to review by the ICT Committee with serious incidents reviewed by the CEO and other senior managers.

5. Containment and recovery

5.1 The Response Team and IT Services will determine the appropriate course of action and the required resources needed to limit the impact of the breach. For instance, this may require isolating a compromised section of the network; alerting relevant staff or contractors; changing access codes/locks or shutting down critical equipment.

5.2 Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

5.3 For incidents that involve a suspected or actual criminal offence all efforts will be made to preserve evidence integrity.

6. Escalation and notification

6.1 The head of department in which the incident occurred is responsible for initial assessment of an incidents severity based on the scope, scale and risk of the incident.

6.2 This preliminary decision is then reviewed by the Business Manager.

6.3 If at this stage the incident is deemed serious then the CEO will be notified and a report submitted to the ICT Committee.

6.4 If a personal data breach has occurred of sufficient scale the Business Manager after consulting with the CEO will notify the Information Commissioner's Office (ICO) within the prescribed statutory time limits and manage all communications between the Institute and the ICO.

6.5 If the breach is deemed of sufficient seriousness (in line with ICO guidance), and concerns personal data, notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks, and will be undertaken by the Response Team. Liaison with the Police or other authorities may be required for serious events.

7. Review

7.1 Once the incident is contained a thorough review of the event will be undertaken by the Response Team, to establish the cause of the incident, the effectiveness of the response and to identify areas that require improvement.

7.2 Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter. Targeted training may be offered to the department affected.