4.1 Personal Data Security Breach Management Procedure and Guidelines

The purpose of these procedures and guidelines is to set out the processes that represent best practice in the event of a data security breach involving personal data or sensitive personal data (see Section 2 above for detailed definitions).

A Personal Data security breach ("data breach" in short) occurs when Personal Data is made available to one or more third parties without the consent of the data subject i.e. unauthorised access to, collection, use, disclosure or disposal of personal information.

If a staff member considers that a data security breach has occurred, this must be reported immediately to the Information Governance Officer at foi@dit.ie and your Line Manger by completing the form below.

Information Services via the DIT Support Desk (phone 01 402 3123 or email support@dit.ie) should also be advised of the potential breach.

There are statutory requirements on the Institute that all incidents in which personal data has been put at risk must be reported to the ODPC within 2 days of DIT becoming aware of the incident in particular circumstances.

Data breaches may occur in a variety of contexts, e.g.:

- Loss or theft of data or equipment on which data is stored (e.g. memory stick, laptop or paper records)
- Inappropriate access controls allowing unauthorised use (e.g. using unsecure passwords)
- Equipment failure
- Confidential information being left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account, leaving documents on top of shared photocopiers)
- Disclosing confidential data to unauthorised individuals
- Human error (e.g. emails being sent to the wrong recipient)
- Hacking, viruses or other security attacks on IT equipment systems or networks
- Breaches of physical security (e.g. forcing of doors/windows/filing cabinets).

As a Data Controller DIT processes significant amounts of personal data and appropriate measures require to be taken against the unauthorised or unlawful processing and accidental loss, destruction of or damage to personal data.

It is essential that in the event of a data security breach, appropriate action is taken by DIT to minimise any associated risks as soon as possible.

Responding to a Potential Data Security Breach

In line with best practice, these guidelines outline five stages to managing a response to a breach:

Stage 1: Identification and Classification

If a staff member considers that a data security breach has occurred, this must be reported immediately to the Information Governance Officer at foi@dit.ie and your Line Manger by completing the **Personal Data Security Breach Report Form** in Section 4.2 below.

Information Services via the DIT Support Desk (phone 01 402 3123 or email support@dit.ie) should also be advised of the potential breach.

The Information Governance Officer will initially review the incident, as reported, and if a data security breach has occurred involving personal data or sensitive personal data they will liaise with the President who will decide if a Breach Management Group of relevant DIT stakeholders and a Chair should be appointed to investigate.

The Breach Management Group may include, amongst others as appropriate, the relevant Director or Head of Function, the Person reporting the incident, Information Services, Public Affairs and the Information Governance Officer).

Any records relating directly to an investigation by the Breach Management Group will be retained by the Information Governance Officer.

Stage 2: Containment and Recovery

Containment involves limiting the scope and impact of a data security breach. If a breach has occurred, appropriate action will be taken by the relevant DIT stakeholders to minimise any associated risks which may include:

- Establishing who within DIT needs to be made aware of the breach and ensuring relevant staff are informed what is required to assist in the containment exercise;
- Establishing whether there are any actions which may recover losses and limit the damage the breach can cause;
- Where appropriate, informing the Gardaí.

Stage 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant DIT stakeholders require to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be.

The information provided at Stage 1 by the individual reporting the breach can assist with this stage.

Stage 4: Notification of Breaches

In accordance with the Office of the Data Protection Commissioner's (ODPC) "Personal Data Security Code of Practice", all incidents in which personal data has been put at risk must be **reported to the ODPC within 2 days of DIT becoming aware of the incident.**

Incidents do not have to be reported to the ODPC only when:

- The personal data concerned is protected by a DIT Information Services Department approved encryption solution1 and the password is not stored with the device

Or

- The full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and**
- It affects no more than 100 data subjects **and**
- It does not include sensitive personal data or personal data of a financial nature2.

The decision to report a breach to the ODPC will be made by the group of relevant DIT stakeholders investigating the incident.

However, if issues are raised relating to the adequacy of technological risk-mitigation measures, DIT will automatically report the incident to the ODPC.

If a decision is made by the group not to report a breach, a brief summary record of the incident with an explanation of the basis for not informing the ODPC will be retained by the Information Governance Officer.

Stage 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the relevant DIT stakeholders will occur to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Subsequent to each data security breach a log will also be maintained by the Information Governance Officer of the agreed steps arising from each incident and this will be presented by way of an overall annual report to the President or his nominated Committee.

[1] Further information on encryption is available in DIT's Information Services IT Security Policy P: Cryptography

[2] Personal data of a financial nature means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.