DATA BREACH MANAGEMENT POLICY

**1 INTRODUCTION**

* 1. The purpose of this policy is to set out the process to follow when a potential information security incident has been identified. An information security incident may lead to a data breach.

* 1. The UK General Data Protection Regulation requires all organisations to report certain types of *personal* data breach to the affected individuals (as soon as possible) and also the Information Commissioner’s Office (ICO) within **72 hours** of becoming aware of the breach. Failure to report within this timescale can lead to a monetary penalty (up to a maximum of £8.7m).
	2. It is therefore essential that you adhere to the process within this policy. This will facilitate decision-making about whether or not we need to notify the ICO and any individuals affected by a breach.
	3. A flow chart detailing the incident management process is included at [**Annex A**](#AnnexA).

## 2 SCOPE

2.1 All employees of Invest NI, temporary staff and external contractors with access to Invest NI information and/or systems are subject to this policy.

2.2 If Invest NI data held by an external contractor is subject to a breach, this should be reported through their Invest NI contract manager.

## 3 IDENTIFYING AN INCIDENT OR A DATA BREACH

3.1 An Information Security Incident is a failure to follow Invest NI information security policies (and therefore place corporate information at risk). Whilst all data breaches are incidents, all incidents may not be data breaches.

3.2 A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal or business sensitive data. This includes breaches that are the result of both accidental and deliberate causes.

3.3 Some examples of data breaches are as follows:

* Theft or loss of IT equipment containing personal or business sensitive data
* Inappropriately accessing personal data about customers/staff
* Inadequate disposal of confidential material
* Unauthorised disclosure of sensitive client data (e.g. Sending a sensitive email to the wrong recipient by mistake)
* Accidental or unauthorised loss of access to, or destruction of, personal data (e.g. clicking on a link within a phishing email)

3.4 An adverse impact of these can be defined for example as:

* Threat to personal safety or privacy
* Legal challenge or regulatory penalty
* Financial Loss / Commercial Detriment
* Disruption to business
* Inability of individuals to access their data
* Reputational loss

These are not exhaustive lists but are representative of the circumstances which this policy seeks to cover.

3.5 A data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal or business sensitive data.

4 REPORTING AN INCIDENT

4.1 All potential information security incidents **must** **be reported immediately on being identified** to minimise any potential risk and impact that may occur as a result of it. **Failure to report a known incident has the potential to result in disciplinary action**.

4.2 Individuals must notify their appropriate line management (see 5.2 below) and all potential incidents must be reported to the Information Governance Team via mailbox privacy.officer@investni.com. Lost IT equipment should also be reported immediately to the ICT service desk at extension 140.

4.3 All potential incidents will need to be investigated as a matter of urgency by the team involved in the incident (See Incident Response Plan at 5 below).

4.4 A **summary report** ([**Annex C**](#AnnexC)) should be sent to privacy.officer@investni.com within **24 hours**. This will allow the Data Breach Review Group to initially assess the incident.

4.5 Within **48 hours** of the incident being identified the investigation must be formally recorded on an **incident report** form ([**Annex D**](#AnnexD)), signed off by the Head of Division / Group and returned to privacy.officer@investni.com.

4.6 Please Note: If the incident relates to the loss of any Invest NI equipment, the equipment will not be replaced until a fully complete and signed form has been sent to privacy.officer@investni.com.

5 PROCEDURE FOR DEALING WITH INFORMATION SECURITY INCIDENTS

**Incident Response Plan**

5.1 Should an incident occur, it is vital to ensure it is dealt with **immediately and appropriately** to minimise any impact and prevent a recurrence.

5.2 As soon as a member of staff becomes aware of a potential incident, they should immediately report it to their line manager and the relevant Head of team. Ensure that the DPO has been advised via privacy.officer@investni.com.

5.3 The Head of Team will appoint an Investigating Officer to carry out an immediate investigation as set out below and inform the Director / Head of Division to keep them informed. Except for major incidents, the Investigating Officer will usually be the line manager of the incident originator. In the case of a major incident, the Data Breach Review Group will advise on who should be assigned as Investigating Officer.

5.4 Once it has been confirmed that a breach has occurred, the Investigating Officer will be responsible for instigating an immediate investigation covering four key elements:

* Containment and recovery
* Assessment of risks
* Informing individuals / customers of breach
* Evaluation and response

These four key elements are reflected in the Incident Report Form ([Annex D](#AnnexD)) which should be completed by the Investigating Officer and can be used as a guide in their investigation.

5.5 The Investigating Officer should complete the **summary report** ([Annex C](#AnnexC)) and send to privacy.officer@investni.com within 24 hours of the incident being identified.

5.6 See [**Annex B**](#AnnexB) for guidelines on the key elements of an investigation as noted in 5.3 above.

**6 Organisational Management of Information Security Incidents**

6.1 The Information Governance team will keep a log of all incidents reported and will produce a regular report on the number, type and originator of information security incidents for review by the Information Governance Group (IGG) to allow any trends to be identified and addressed.

6.2 The Data Breach Review Group (comprising of the DPO , the Risk Manager, the DSO, the ITSO, Information Governance Officer and when necessary the PR Media Relations Manager) will conduct a risk assessment for each incident, to gauge the impact and likelihood of realisation, in relation to data subjects, customers and also Invest NI.

6.3 The Data Breach Review Group will decide if the incident is a breach and also if it should be reported to the individuals impacted by the breach and the ICO. The DPO will report the breach to the ICO if required.

6.3 All incidents will be reported to the relevant Director / Head of Division after the risk assessment is complete to address with the employee(s) involved and also, when the mitigated risk is rated at medium or above, to Human Resources.

6.4 Human Resources will assist with consideration as to whether disciplinary action needs to be taken in respect of employees who have not complied with information security policies and guidance.

**A significant security breach, or repeated security breaches, by the same individual will result in disciplinary action. Where appropriate, breaches of a criminal or illegal nature will be reported to the relevant authorities.**

6.5All incidents are reported as internal control issues within the quarterly Assurance Statement checklists which require approval by ELT members. Any significant risks related to Information Security Incidents are reported to Board through the corporate risk management process.

6.6 The DPO will report all data breaches to the Board Audit & Risk Committee as part of the reporting duties of this post.

**7. Further Guidance**

7.1 Guidance on information security issues, and related policies, can be found in the **Information Security Handbook**.

7.2 Guidance on data protection can be found in the Invest N **Data Protection Policy**.

7.2 Any queries on this policy should be raised with the Information Governance team via privacy.officer@investni.com. Any specific ICT security queries should be raised with the IT Security Officer via itso@investni.com.

**ANNEX A** Incident Management Response Plan

***Within 24 Hours***

* Identify Incident
* Report Incident to Line Manager and Head of Team
* Report to Privacy Officer via privacy.officer@investni.com
* Begin Investigation:
	+ Contain the incident (Can it be stopped?)
	+ Assess the risks – complete the summary report and send to privacy.officer@investni.com
	+ Assess whether Individuals / customers need to be informed?

***Within 48 Hours***

* Evaluation & Response: complete incident report
* Sign off from Director / Head of Division
* Return to privacy.officer@investni.com

***Within 72 Hours***

* Data Breach Review Group review incident report:
	+ Risk assessment completed
	+ Plan to contact customers (if needed)
	+ Decision on ICO reporting
	+ Report to ICO if necessary

***Beyond 72 Hours***

* Customer Relationship Management in respect of the incident
* Consideration of disciplinary action (HR & Management)
* Report to the Information Governance Group (IGG)
* Report to the Board (ARC)

ANNEX B – Guidance on the investigation

Once it has been confirmed that an incident has occurred, the Investigating Officer will be responsible for instigating an immediate investigation covering four key elements:

* Containment and recovery
* Assessment of risks
* Informing individuals / clients of breach
* Evaluation and response

These four key elements are reflected in the **Incident Report** form (Annex D) which should be completed by the Investigating Officer and can be used as a guide in their investigation.

The investigation should begin immediately and be reported on twice, firstly within 24 hours via the Summary Report and then within the Incident Report within 48 hours of the incident being identified.

**Containment and Recovery**

Information Security Incidents / Data breaches will require not just an initial response to investigate (how did it happen?) and contain the situation (stop it happening) but also a recovery plan including, where necessary, damage limitation.

The following actions should be carried out by the Investigating Officer:

* If the incident is ongoing (for example unauthorised disclosure on a website) ensure that it is stopped immediately. You may need to contact colleagues from ICT to assist.
* Establish whether anything can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment or papers, this could involve the deletion of data uploaded to mimecast or the use of back-up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
* Establish who needs to be made aware of the incident and inform them what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of work, finding a lost piece of equipment or item of post, or simply changing access codes or passwords.
* Where appropriate, inform the police.

**Assessing the Risks**

Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the incident. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. Risk should be evaluated on the basis of an objective assessment (view the incident from the individual’s perspective).

The following points may also be helpful in making this assessment:

* Know what type of data is involved?
* How sensitive is it? Some information is sensitive because of its personal nature (health records) while other types are sensitive because of what might happen if it is misused (bank account details).
* Is it special category data? The potential damage to individuals that could result can be especially severe, in particular where the breach could result in physical harm, psychological distress, humiliation or damage to reputation.
* If information has been lost or stolen, are there any protections in place such as encryption?
* What has happened to the information? If it has been stolen, it could be used for purposes which are harmful to the individuals to whom it relates. If it has been damaged, this poses a different type and level of risk.
* What could the information tell a third party about the individual? Breaches involving identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft or fraud. A combination of personal data is typically more sensitive than a single piece of personal data.
* How many individuals are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but it is an important factor in the overall risk assessment.
* Who are the individuals whose data has been breached? Whether they are staff, customers, stakeholders or suppliers, for example, will to some extent determine the level of risk posed by the breach and therefore, your actions in attempting to mitigate those risks.
* What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
* Are there wider consequences to consider such as a loss of public confidence in Invest NI as a trusted business partner?
* If individuals’ bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

**Informing individuals and other parties of incidents / breaches**

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. These will have been assessed under the step above.

Where there is a likely high risk of adverse effects occurring, the GDPR requires us to communicate the breach to the affected individuals as soon as is reasonably feasible.

The GDPR explains that adverse effects where a breach must be reported to the individuals can include:

* Loss of control over their personal data
* Limitation of their rights
* Discrimination
* Identity theft or fraud
* Financial loss
* Unauthorised reversal of pseudonymisation,
* Damage to reputation
* Loss of confidentiality of personal data protected by professional secrecy
* Any other significant economic or social disadvantage to those individuals

Even where it is not necessarily dictated by the GDPR; informing people and organisations that there has been a data security breach is a recommended element of the Invest NI breach management strategy. For instance, being transparent about a breach can be important for building a relationship with a customer and as a consequence protecting the reputation of Invest NI as a trusted business partner. If we failed to notify a customer of a breach involving their data and they later discovered it through other means it would reflect poorly on Invest NI.

Nonetheless, informing people about a breach is not an end in itself. Notification should have a clear purpose, such as enabling individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. As noted this purpose can also simply be as a courtesy to the customer and thus a means to protect Invest NI’s reputation.

Consideration should be given to who should be notified (a customer or their individual employees), what they should be told and how you are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to your decision:

Notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach.

When notifying individuals, give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

**Evaluation and Response**

It is important not only to investigate the causes of the incident / breach but also to evaluate the effectiveness of your response to it and to mitigate against any future recurrences of the same breach.

Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing ‘business as usual’ is not acceptable. You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made. Lessons learnt from the breach should be documented and circulated to staff for the purpose of preventing a similar incident. The following points will assist you:

Consider what lessons have been learnt and circulate these to relevant staff. Any recommendations for improvements should be implemented as quickly as possible and recorded as evidence that all reasonable steps have been taken to prevent recurrence at that time.

ANNEX C – Information Security Incident Summary Report

[To be completed & returned ASAP but no later than **24 hours** of incident being identified][*Complete electronically*]

|  |  |  |  |
| --- | --- | --- | --- |
| Investigating Officer | Team & Division | Phone ext | Date & time Identified |
|  |  |  |  |

|  |
| --- |
| Please describe the **incident** (what has happened?): |
|       |

|  |
| --- |
| Categories of the individuals impacted by the incident (e.g. customers, staff, members of public): |
|       |
| Approximate number of individuals impacted: |
|       |

|  |
| --- |
| Categories of Personal Data Records and/or Business Sensitive data and number of records |
|       |

|  |
| --- |
| Steps taken to date to contain breach & recover the data? |
|       |

ANNEX D – Information Security Incident Report

[To be completed & returned ASAP but no later than 48 hours of incident being identified] [*Complete electronically*]

|  |  |
| --- | --- |
| **Report Number** |       |

1. Notification

|  |  |  |  |
| --- | --- | --- | --- |
| Investigating Officer | Team & Division | Phone ext |  |
|  |  |  |  |

2. Incident Details

|  |
| --- |
| **Type of Incident [Tick All That Apply]:** |
| Equipment Loss |  |
| Data Loss |  |
| Unauthorised Disclosure |  |
| Unauthorised Access |  |
| Breach of Policy |  |
| Other (expand): |  |

|  |  |
| --- | --- |
| Date Incident occurred |  |
| Date & time Incident detected |  |
| Incident Location |  |
| Person(s) responsible for incident (Originator) |  |

|  |  |
| --- | --- |
| Media / Device Type (if relevant) |  |
| If portable storage device was this password protected in line with Invest NI policy? |  |
| If portable storage device was this encrypted? *[Please note that all Invest NI issued mobile phones & laptops are encrypted]* |  |
| Did the device have network connectivity? |  |
| Was any personal or business information stored on the device? |  |
| If answer to above was ‘No’ explain why: |

|  |
| --- |
| Please describe the **incident** in as much detail as possible: |
|       |

|  |
| --- |
| Please describe the **data**. For example: is it personal information (give specific examples). Is it business sensitive (give specific examples) – consider if the information is in the public domain / would it be disclosed under FOI / would the owner/individual be concerned at its disclosure (put yourself in their place). Please attach a copy of the information unless there is a reason this is not possible.  |
|       |

|  |
| --- |
| What remedial action has been taken to **contain** the incident? For example has the data been retrieved? Has it been returned or destroyed (include evidence of this)? When were the individuals/owner informed of the incident and what was their response? |
|       |

|  |
| --- |
| Identify potential **risks** to the subject /owner of the data? E.G potential for identity theft / Phishing aid / Commercial detriment / Reputational damage  |
|       |

|  |
| --- |
| What remedial action has been taken to **mitigate** against future similar incidents occurring at an individual / team / divisional level? |
|       |

|  |
| --- |
| Identify any potential impact this incident may have on Invest NI’s **reputation** or relationship with Customer / Stakeholder. |
|       |

I confirm that the above is a complete and accurate account of the incident, information involved & potential impact:

|  |  |  |
| --- | --- | --- |
| ***Title*** | ***NAME*** | ***Date*** |
| Originator |  |  |
| Investigating Officer |  |  |
| Head of Division |  |  |

Please return completed form to privacy.officer@investni.com ASAP but no later than **48 hours** of incident being identified.

**Version Control**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Author / Reviewer | Approver | Review Date | Reason for change |
| 3.0 | Danny Smyth | Steve Chambers | 25 May 2018 | Name change, revised process to reflect GDPR requirements |
| 4.0 | Mark Hutchinson | Danny Smyth | 20 May 2020 | Scheduled review |
| 5.0 | Mark Hutchinson | Danny Smyth | 09 Feb 2022 | Scheduled Review, reintroduce ‘incidents’ |