Northern Ireland Policing Board – Security / Data Incident Reporting Policy

Introduction

1. Security Incident Management is a critical activity for the Northern Ireland Policing Board (the Board). Its Members and all staff, at whatever grade, have responsibilities and roles to play. This policy's objective is to provide the Board with standard and clear incident reporting guidance along with supporting roles and responsibilities. It includes guidance for those who have specific responsibilities within the Board. However, it is also intended for all staff to enhance their understanding and awareness of incident reporting and its management. Staff must also ensure appropriate arrangements are in place for those who process information on the Board's behalf.

2. **This policy reflects the new responsibilities and reporting roles introduced by GDPR. Particularly, it highlights the mandatory requirement to notify the ICO of certain incidents within 72 hours and the introduction of fines up to €10m for not doing so**. A major objective of this policy is to enable the Board to identify an incident and notify the ICO as required. **It is essential that incidents are reported to the Information Security Team (IS Team) immediately to allow notification to the ICO if required. If an incident is not reported immediately it could result in the Board incurring very substantial fines.**

3. **The Information Security Team[1] comprises the Information Asset Owner, the IT Security Officer, the Communications Manager and the Compliance Officer.**

Scope

4. This document covers paper information, computer systems, networks, the physical environment and staff who support those business functions. This policy does not cover the outworking of any incident investigation.

[1] The Premises Officer and the Security Manager may be co-opted onto the IS Team as required

5. While the Board is responsible for handling and reporting its own incidents it must keep the Department of Justice's Information Security Team and DOJ Accounting officer updated regarding any major incidents.

Incident Definition

6. A security incident can be defined as any untoward event that has an adverse impact on the Board or its business. It may or may not result in an information breach. An information security breach is defined as any compromise of confidentiality (loss or unauthorised disclosure); integrity (unauthorised modification or corruption); or availability (denial or destruction) of information/data that is likely to lead to an adverse impact on the Board or its business, or in the case of personal data, on the data subjects. The underlying cause/nature may fall into one or more of the categories below:-

Physical (Physical Access)	**Technical** (ICT system or service failure)	**Personnel** (Unauthorised use of information or equipment etc.)	**Information** (Compromise of confidentiality, Integrity or availability of information)
• Physical buildings, doors, perimeter fences	• ICT system access	• Illegal activity	• Physical or electronic file
• Access to unauthorised areas, breach of access controls	• Electronic data or information including Email, EDRMS, Line of Business application and Internet	• Failure to act within the Code of Conduct for Board Staff and Members.	• Data Protection breach

• Environmental security e.g. accommodation, water, heating, electricity, transportation, location etc.	• Computer Environment operating conditions • Significant downtime	• Security risk to staff/ others	• Risk to staff or others
N.B. Any of the above could also result in a Data Protection incident – the vast majority of Board incidents fall into the Information category.			

7. **Information asset**

As stated in the Information Asset Owner (IAO) Guidance issued by the Department of Justice (HPRM ref 346809) "An information asset can be defined as an identifiable collection of information or data stored in any manner, at any location, and recognised as having value to the Board for the purposes of performing its business functions and activities". Therefore the term information asset covers both electronic and paper records. Most incidents involve the mishandling or loss of data and in particular personal data.

Some examples of information assets are:-

- A store of paper files or local store e.g. filing cabinet;
- A line of business system with large amounts of business data;
- A collection of files e.g. associated with a specific project or programme;
- A single casework file;
- A database or spreadsheet;
- A corporate system such as HR or Finance;
- Removable media with large amounts of information;
- Collections of information gathered from one or more external source which may be managed or administered by the Board ; and
- Policy or strategy information still under consideration i.e. prepublication.

8. Incidents should be considered against the protective marking of the information, the impact to the business and the risk to personal data. Further advice on these areas can be obtained from the Information Asset Owner (IAO). Reference to your Information Asset Register (IAR), which contains descriptions, protective markings and details of any personal data held, should also be helpful.

Incident Reporting – Staff / Board Member Responsibility

9. It is the responsibility of all Board staff to report any perceived incidents, breaches or threats (whether observed or suspected) to business activities, systems or services to their line manager **immediately**. Line managers must then report these suspected incidents or breaches to their IAO (Director) **immediately**.
10. It is the responsibility of all Board Members and researchers appointed to support Members, to report any perceived incidents, losses, breaches or threats to the Board's Chief Executive **immediately**.
11. The following pages set out the Board's Security / Data Incident Management Policy with guidance on how an incident will be handled, the various roles and responsibilities involved, procedures to be followed and various critical decision points.

1. Assessing an Incident

Start – Significant incidents must be notified to the ICO within 72 hours. The ICO can issue fines up to €10m solely for not notifying in time. It is essential therefore that the Board has arrangements in place to ensure that staff and Members and anyone else who is processing information on the Board's behalf (Contractors, other Departments, etc) can recognise an incident and report it **immediately** to their line manager, who will in turn **immediately** notify their IAO. The IAO should then ensure that the incident is reported **immediately** to all the members of the IS Team to allow an initial discussion to take place. **This is the most crucial part of the process.**

Initial Discussion – The purpose of the initial discussion is to identify quickly whether it is a major incident which requires immediate action (mitigation, containment, protection, escalation, etc.) and whether it involves a breach of personal data and therefore may require to be notified to the ICO or whether it can be dealt with in slower time with the Initial Incident Report Form (IIRF) being forwarded to the IS Team within 3 days. At this stage minimal details should be sufficient to allow a decision to be made or to highlight what other information is required urgently:

- Branch and location of incident
- What information / data is involved?
- Who are the data subject(s) – how many are there?
- Brief summary of incident
- Potential consequences / risks and likelihood of them being realised

Incident Administration – Once an incident has been notified to the IS Team the incident will be recorded and allocated an incident number. This incident number must be inserted into all further related emails / correspondence. The Compliance Officer will save into HPRM all records of each incident including when an incident was reported and when the related incident report is received. They will automatically send a request for an IIRF to be completed to the relevant IAO. This report must be returned promptly and not later than 24 hours after becoming aware of the incident. This is to allow the Board to meet the 72 hour deadline to report to the ICO if required.

2. Not a Major Incident

Historical evidence shows that most incidents will not be major incidents and can be dealt with in slower time, but it is essential the 'Not a Major Incident" process is followed as this process will identify learning points, allow these to be shared across the Board , and will agree actions to reduce the likelihood of a recurrence. **Typically an incident will not be 'major' if it does not create a risk / potential risk to personnel or physical assets, does not involve personal data, risk damaging the reputation of the Board, or create a potential financial loss.** If the incident is thought to be 'major', immediate actions must be carried out and branches should expect to prioritise this work to provide any information requested by the IS Team and to complete the IIRF immediately (see Section 3 – Pages 8 – 9).

Investigation (IAO) – If the incident is deemed not to be 'major' following the initial discussion, the IAO will carry out an investigation to establish and confirm the facts to enable him/her to complete the IIRF. **It is possible that the investigation will uncover new detail that leads to the incident correctly being deemed as 'major'.**

IIRF (IAO) – The IIRF, with guidance, will be issued automatically to the IAO when the incident is recorded. The IIRF must be sent to the IS Team within three days.

Agree Actions – The IIRF includes your immediate actions but also recommended / follow up actions. These are designed to reduce the likelihood of a recurrence and might include: focused or generic staff guidance and/or staff training, a review of the processes and procedures etc.

Review Actions – The IS Team might request, on behalf of the SIRO (Chief Executive), that further actions be carried out. The incident will be held open on a BF system until all actions have been carried out and until the IS Team have physical proof of the actions having been carried out. It is essential that the IS Team is provided with this proof (copy of staff notice that issued, copy of minutes of a staff meeting which refers to staff training etc.) as we must be able to make these available to the ICO, when requested.

Recommendations to SIRO – Once all the actions have been carried out and proof provided the IS Team will forward your IIRF to the SIRO with a written recommendation that the incident be closed.

Close Incident – If the SIRO is content to close the incident the register will be updated and the IAO will be advised accordingly.

3. Dealing with a Major Incident and Identifying if there is a Data Protection Issue

If the incident is deemed to be 'major' the SIRO must be informed immediately. The SIRO in turn will further inform and advise the Board, the Chair of the Audit Committee, the Departmental Accounting Officer and the Departmental Chief Information Officer.

Initial Mitigation – Correct and effective actions taken quickly at this stage can negate even a major incident, completely reduce its detrimental impact (both financial and reputational), support and reassure data subjects and remove the requirement to notify the ICO. **Should the incident be notified to the ICO, we must always provide details of the Board's immediate and mitigating actions. The extent and effectiveness of these actions will be considered closely and commented on by the ICO and will likely impact on their final decision.** It is important that discussion between the branch and the IS Team allows for a full understanding of the incident, effects, consequences and risks, to allow all appropriate mitigating actions to be carried out. Mitigating actions might include:

- Notifying Data Subjects - If an incident involves a breach of personal data which is likely to result in a high risk to the rights and freedoms of natural persons the Controller shall communicate the personal data breach to the data subject without undue delay. The threshold for reporting to data subjects is higher than for reporting to the ICO. Not all breaches will be reported to data subjects, thus protecting them from unnecessary concern. If, however for example, the name and address of a PSNI Officer was inadvertently disclosed and there were fears for their personal safety or Article 2 concerns, advising the individuals involved could obviously allow them to take actions to consider the position and protect themselves.

Other possible mitigating actions are:

- Visiting a location to retrieve physical data.
- Arranging for IT experts to delete, purge, remove electronic data.
- Informing or getting a data subject to inform the local PSNI.

- Obtaining confirmation from unintended recipients that data has been deleted and has not been shared.
- Arranging for data held on a phone or laptop to be made inaccessible remotely.

Investigation – Most investigations will be carried out by the IAO but in some circumstances the SIRO may lead or support the investigation. **If it has not already been established whether personal data is involved this must be done now and urgently.** If it is, and if the incident is notifiable to the ICO, we only have 72 hours to notify, after which the Board can be subject to significant fines. If notification is not made with 72 hours, it must be accompanied with reasons for the delay.

4. Major incident - Not a Data Protection Issue

Note - GDPR only applies to a breach of personal data. **If there is personal data involved Section 5 sets out the process which must be followed to decide whether the ICO must be notified.**

IIRF (IAO) – Having already investigated the incident and having discussed it with the IS Team the IAO will complete, or update, the IIRF and send it to the IS Team within three days.

Agree Actions – The IIRF includes your immediate actions but also recommended / follow up actions. These are designed to reduce the likelihood of a recurrence and might include: focused or generic staff guidance and/or staff training, a review of the processes and procedures etc.

Review Actions – The IS Team might request on behalf of the SIRO that further actions be carried out. The incident will be held open on a BF system until all actions have been carried out and until the IS Team have physical proof of the actions having been carried out. It is essential that the IS Team is provided with this proof (copy of staff notice that issued, copy of minutes of a staff meeting which refers to staff training etc.) as we must be able to make these available to the ICO, when requested.

Recommendations to SIRO – Once all the actions have been carried out and proof provided the IS Team will forward your IIRF to the SIRO with a written recommendation the incident be closed.

Close Incident – If the SIRO is content to close the incident the register will be updated and the IAO will be advised accordingly.

5. Major Issue - Process to decide whether ICO must be notified

The Article 29 Data Protection Working Party has published guidelines on personal data breach notification by Controllers. For the Board the Controller is the Northern Ireland Policing Board. For the purposes of this policy the decision whether to notify will be delegated to the SIRO. It is the Controller who is responsible for the final decision on whether the ICO is notified but the Controller must receive advice from the IAO and the Data Protection Officer (DPO) before making the decision. If the ICO decides to impose fines in relation to the incident, it is the Data Controller who will be liable, not the IAO or the DPO.

Advice – notify ICO (DPO) – For all major incidents which involve personal data the DPO will provide 'independent expert advice' to the SIRO on data protection law. The DPO is to be free to disagree with the IAO and / or Data Controller and must not 'take instructions' in relation to his/her independent role or about his/her tasks. The DPO's advice must be recorded and made available to the ICO if necessary.

Advice – notify ICO (IAO) – The Controller will also receive advice from the IAO on whether the ICO requires to be notified. This advice will be set out in the IIRF, along with reasons why the ICO should not be notified, if appropriate.

Notify ICO? (SIRO) – The SIRO, having the benefit of advice from the IAO and the DPO, makes the final decision on whether to notify the ICO. The SIRO will arrange notification.

Breaches must be notified when they are likely to result in a risk to the rights and freedoms of individuals. Some examples of when a breach does not need notified are: if data is shared with a 'trusted' recipient (with someone within the DOJ/PSNI family or an appropriately national security vetted person), or if the data has been encrypted and cannot be accessed by anyone. But note that if no backups are available there might be a notifiable availability breach i.e. if rights and freedoms are at risk.

6. Major Issue - Process when Data Protection Issue does not need notified to ICO

Note - GDPR only applies to a breach of personal data. **If no personal data is involved the incident should be handled under Section 4 'Not a Data Protection Issue'** (see page 10).

Investigation (IAO) – Having already investigated the incident and having discussed it with the IS Team the IAO will complete, or update, the IIRF and send it to the IS Team within three days.

Agree Actions – The IIRF includes your immediate actions but also recommended / follow up actions. These are designed to reduce the likelihood of a recurrence and might include: focused or generic staff guidance and/or staff training, a review of the processes and procedures etc.

Review Actions – The IS Team might request on behalf of the SIRO that further actions be carried out. The incident will be held open on a BF system until all actions have been carried out and until the IS Team have physical proof of the actions having been carried out. It is essential that the IS Team is provided with this proof (copy of staff notice that issued, copy of minutes of a staff meeting which refers to staff training etc.) as we must be able to make these available to the ICO, when requested.

Recommendations to SIRO Once all the actions have been carried out and proof provided the IS Team will forward your IIRF to the SIRO with a written recommendation the incident be closed.

Close Incident – If the SIRO is content to close the incident the register will be updated and the IAO will be advised accordingly.

7. Major Incident - Process when Data Protection Issue does need notified to the ICO

Notifying ICO (Initial) (CIO) – **If the SIRO on behalf of the Data Controller decides that the incident should be notified to the ICO, this must be done within 72 hours of the Controller 'having a reasonable degree of certainty' that a notifiable breach has occurred. If the Controller is not certain, he/she can start a prompt investigation to establish if a breach has occurred. This investigation should not take more than 24 hours.** Fines of up to €10m can be imposed solely for a failure to notify (irrespective of the nature or severity of the breach) so it is essential that at least initial notification takes place within 72 hours. **There is no penalty for reporting an incident that ultimately transpires not to be a breach.**

Even if the incident is not reportable to the ICO "any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken" must be documented by the Controller. Failure to properly document a breach can lead to the ICO imposing a fine.

Phased Notification – Where it is not possible to notify all the details of the incident to the ICO at the same time, an initial notification of what is known should be made, with further phased notifications being made as the investigation continues.

ICO Liaison – The ICO will consider the details notified and will very often liaise with the Board and request further information and answers to specific questions. Branches must make themselves available to assist in this process.

ICO Decision – When the ICO has had time to consider all the facts it will write to the Board to confirm its decision. These can include: no further action, a fine, and/or a direction to carry out specific actions. After each breach, which results in an ICO decision, the DPO must carry out a review of the breach to ensure that all appropriate actions have been identified and rolled out throughout the Board as necessary.

Alongside notification to the ICO the same process set out in section 6 must be carried out.

Annex A – Initial Incident Reporting Form (IIRF) – use appropriate protective marking when completed

You must report the incident to the Information Security Team immediately by telephone to establish if the ICO must be notified within 72 hours. If the ICO must be notified you must provide the Initial Incident Report Form immediately to allow sufficient time to draft the notification. If you delay reporting the incident you must provide reasons for the delay.

Even if you do not have the full details of the incident, complete as much of the form as possible, and send it without delay to the members of the IS Team and the Data.Protection@nipolicingboard.x.gsi.gov.uk mailbox.

Part 1 – Incident Details (Can be completed by Reporting Officer but must be signed off by the IAO)	
Branch area:	
Date of incident:	
Time of incident:	
Location of incident:	
Date and time you became aware of the incident	
Reporting Officer details:	
IAO details:	
Has the incident resulted in a breach of personal data?	
Description of Incident/ Cause/ Nature (see Paragraph 6 on Page 2) – Which category does the incident fall into? • Physical • Personnel • ICT • Information	

Description of Incident/ Cause/ Nature (see Paragraph 6 on Page 2) – If the incident was an information security breach what was compromised? • Confidentiality, • Integrity • Availability		
Impact of incident: (Provide a brief outline) likely consequences, severity, likelihood of risk materialising, numbers of data subjects, detail of records and number of records involved?		
Do you anticipate media interest? (Yes/No)		
Immediate actions taken by branch:		
Further actions planned/ recommendations:		
Date and time the relevant Director (IAO) and IS Team were advised of the incident?	IAO: Name:	Information Security Team:
Is a fuller investigation required? If yes provide investigation lead details and target deadline:		
Has the DPO been notified?		
Date notified:		
Necessary to inform the Department of Justice?	Y/N	Date notified
Do you believe the incident should be reported to the ICO? Yes / No (Give details)		
Reminder: All related emails must be emailed to as soon as possible to the members of the IS Team and the Data.Protection@nipolicingboard.x.gsi.gov.uk mailbox.		

Part 2 – Reporting and Closure Actions (To be completed by the Information Security Team and signed off by the SIRO (Chief Executive)	
Date and time initial incident report form (IIRF) received:	
Date and time IIRF recorded:	
Incident record number:	
Has the Senior Information Risk Owner (SIRO) been notified? (Yes/No)	
Date SIRO notified:	
Appropriate actions taken: (Yes/No)	
Further action required: (Yes/No) If Yes provide details	
Dates incident closed by SIRO	

Incident Reporting Contacts	
Senior Information Risk Owner (SIRO) (Chief Executive)	**Amanda Stewart**
Data Protection Officer (DPO)	**William Magee**
Security Manager	**Jenny Passmore**
Information Security Team	**Information Asset Owner ie the Relevant Director (IAO)**
Information Security Team	**Finance Manager / ITSO**
Information Security Team	**Communications Manager**
Information Security Team	**Compliance Officer**
Information Security Team*	**The Premises Officer and the Security Manager co-opted as required**
Incident Reporting Mailbox	**Data.Protection@nipolicingboard.x.gsi.gov.uk**
Department of Justice (if appropriate)	