Security Incident Handling Procedure

This procedure is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

Procedure Statement

This procedure sets out a process for handling data security incidents where confidentiality, integrity or availability has been, or may have been, breached. There are several ways this may happen including, but not restricted to, personal data breaches, theft, break-ins, and poor disposal of confidential waste. All breaches should be assessed, investigated, and reported accordingly.

The majority of data security breaches are innocent and unintentional such as the user not 'logging out' of their desktop personal computer (PC) at the end of the day. However, 'near misses' where no actual harm results from the incident but could have had the incident come to fruition, should still be reported and will be analysed by the ISO to look for possible ways of preventing an actual incident occurring in the future.

North Yorkshire Police (NYP) has a responsibility to monitor all data security incidents that occur within the organisation that may breach security and/or confidentiality of business information. NYP also needs to ensure that not only are all incidents identified, assessed, reported, and monitored but also are investigated to a sufficient level, in line with the risk posed to the organisation.

The scope of this procedure includes the handling of ALL potential or actual security incidents and/or weaknesses reported to the ICT Service Desk, Data Protection Officer (DPO), Information Security Officer (ISO), Professional Standards Department (PSD) or any other member of NYP staff.

Overarching Policies:
Information Security Policy

Procedures:
Clear Desk and Clear Screen Procedure
Internet and E-mail Procedure
Protective Marking Procedure
Working with Portable Technology and Documents Procedure
Security Incident Reporting Procedure
Physical Security Procedure

Other Documents:
Information assurance (college.police.uk)
HMG Security Policy Framework (SPF)

Process

Incident Definition and Reporting Mechanism:

For greater detail on the types of Security Incidents that need to be reported, as well as when and how to report such an incident, please seek guidance from the Security Incident Reporting Procedure.

Incident Sources:

There are various sources for a Security Incident to be uncovered and subsequently reported. The most common of these would be as follows:

- incident reported to, or uncovered by, PSD
- incident reported to, or uncovered by, the ISO
- incident reported to, or uncovered by, ICT staff member
- incident reported to, or uncovered by, ICT Service Desk
- incident reported to, or uncovered by, the Force Control Room (FCR)
- incident observed and reported by a staff member

In any of the above instances, the incident must be reported to the DPO and ISO using the Information Security Incident e-form. Where this is not immediately possible, the incident should be raised via email with the incident report submitted at the earliest opportunity thereafter.

Out of hours: where a personal data breach of information held within systems is discovered out of hours, the FCR Deployment Manager should be contacted and provided with detail to assist in making the decision whether to call ICT on-call staff to handle system breaches. The person reporting such a breach must submit a Security Incident Report even though FCR may have been contacted. This is to allow the DPO to assess the breach and report to the Information Commissioner's Office within the statutory 72 hours.

Initial Assessment

When a security incident has occurred the initial action is the responsibility of the staff member who discovered the security incident, regardless of whether they have had any involvement in the cause of the incident. The following actions must be taken immediately:

- initial containment action such as asking incorrect recipients to delete all traces of emails not intended for them and asking for written assurances that they will not further share or use the information, must be undertaken where possible;
- line supervision to be notified;
- reporting procedure carried out;
- ISO and DPO notified;

- ISO and DPO to make initial assessment of incident severity made;
- where appropriate, ensure the information received from the data subject or reporting person and how they can assist the breach handling process are considered.

Following initial identification of an incident, a severity level will be applied, in line with the incident gradings listed below, which will account for the potential harm and detriment of those involved and any impact the incident may have on the organisation. This assessment will be made by the ISO, DPO, or appropriate representative and the decision to escalate the process will be made depending on the perceived severity level.

It should be noted that the ongoing nature of the incident and any further information gathered may require the re-evaluation of severity. If convened, it will be responsibility of the incident Management Team (IMT) to endorse the severity level that has been applied or to amend as appropriate.

DPO, ISO, or representative

The DPO, ISO or other, in conjunction with the line manager if appropriate, will seek further required detail surrounding the breach of security in order to further define the incident and aid the Initial Assessment.

The DPO, ISO, or appropriate representative will, where appropriate, seek clarification on any technical issues that may be created due to the incident. This may involve:

- assessing the technical options to reduce the impact of the incident;
- assessing the damage to technical systems; and/or
- assessing the source and cause of technical incident.

Incident Grading

Grade - Explanation

Severe

Those incidents that will usually cause the degradation of vital service(s) for a large number of users, involve a serious breach of network security affecting a very large number of users, and affecting business critical equipment and/or services or significantly damage public confidence in the organisation.

Examples of such incidents include;

- a significant malware infection affecting service delivery;
- compromise of cryptographic material;
- loss or theft of equipment; and
- carrying material in an unprotected state i.e. unencrypted or loss of paper based, removable media or email.

Significant

Those incidents of a less serious nature having a greater impact or affecting a significant number of users or non-essential systems.

Examples of such incidents include;

- a virus attack on a single server or PC;
- use of non NYP-issued IT equipment or similar event;
- loss of laptop containing NON-sensitive information; or
- loss or compromise of non-sensitive OFFICIAL material.

Minor

Those incidents of limited impact or affecting a small number of users.

Examples of such incidents include;

- the loss of a warrant/ID card;
- a contained instance of an unauthorised disclosure; or
- an unauthorised persons on premises for a short period of time and who has not gleaned any policing information or access to secure working areas.

Incident Management Team (IMT)

Following the initial assessment and grading of the incident, an appropriate IMT is convened, based upon the severity of the incident and the professional areas upon which the incident resides.

The core members of the IMT are listed below and should attend in all cases where the initial assessment has concluded the incident is Significant or higher.

In the case of a SEVERE incident, the Gold Command process will be invoked in order to co-ordinate resources and activities until the incident has been resolved, or the impact has been reduced to a lower level (SIGNIFICANT or MINOR) when it can be devolved to the Head of PSD, DPO or ISO respectively.

In a case of a SIGNIFICANT incident, the DPO or ISO will co-ordinate the activities of the IMT.

Core Members Responsibility

Gold Commander

- In the event of a severe incident, the Gold Commander should take charge and co-ordinate the relevant resources/activities.

Data Protection Officer

- Determining whether this constitutes a personal data breach;
- Maintaining an audit log of activity and actions;
- Assessing impact on data subjects; and
- Advising on referral to ICO and data subject notification.

Information Asset Owner and/or SPOC/Business Lead

In the event of a personal data breach:

- Co-operate with the questions asked by the DPO and ISO;
- Co-ordinate the identification of affected individuals as soon as is reasonably possible;
- Assist in assessing the impact on data subjects;
- Where necessary, review local processes, procedures and security controls around the handling of the data at risk and implement any improved security controls, instruction, training etc.

Head of PSD and/or Head of Information Management Team (IT and non-IT incidents)

- Chair IMT meetings in respect of all incidents;
- Directing Information Management, ICT and PSD resources as required;
- Ensuring that all external agencies are adequately informed as required;
- Determining formal meeting schedules; and
- Involving the Head of ICT or representative.

(IT specific incidents)

- Approving ICT resources for Technical Response Team(s);
- Authorising urgent or immediate purchase of technical tools or physical accessories;
- Determining formal meeting schedules; and
- Approval for implementation of Business Continuity/Disaster Recovery procedures.

ISO (IT and non-IT incidents)

- Initial impact assessment and determination of severity;
- Representing the Information Management Team and providing updates to the IMT;
- Representing the Technical Response Teams progress and providing updates to the IMT;
- General research, including technical information, regarding the nature of incident;
- Alerting external agencies such as GovcertUK/PolWarp, as appropriate;
- Communication to NYP users via email, intranet etc.; and
- Creation and updating of incident record.

Out of Hours Incident Handling

If a security breach is reported outside of normal office hours, then it is the responsibility of the individual who became aware of the incident and who is reporting the incident to make contact with

the Force Control Room (FCR).

The FCR Inspector will:

- take details of the incident;
- conduct an initial assessment;
- categorise as above (minor, significant or severe);
- determine whether to call the ICT out of hours support; and
- remind the incident reporter to complete the Security Incident Report immediately.

If the incident fits the category of significant or above, the 'on-call' Gold Commander must be informed. The Gold Commander will make a decision as to whether or not the situation requires immediate treatment.

If it does, the Gold Command structure is to be called upon, if not, details shall be passed to the relevant person(s) as detailed in this procedure and will be dealt with accordingly at the commencement of the next working day.

Partnership Organisation Security Incidents Affecting NYP

Where NYP information and/or equipment resides within partnership organisations there is the possibility that breaches of security will occur.

There should be appropriate wording within any Information Sharing Agreements, Data Processing Contracts and/or Memorandum of Understandings in place to instruct such partners as to what to do in the event of any security incident.

Partners should contact their NYP contact in the first instance who will, in turn, contact the DPO, ISO or ICT Service Desk in order to report such incidents. If this is not possible, partners should be directed to email in all notifications of security incidents to the Information Security mailbox.

It is also important to note that such incidents will be recorded and reported upon, and where it is discovered that any partnership is posing a threat to NYP through repeated incident occurrences, the continuance of such partnerships will be reviewed. Partners will be advised of the outcome of any evaluation.

Incident Closure

Once an incident has been declared as resolved by the IMT, all relevant feedback will be collated and it will be the responsibility of the DPO, ISO or suitable representative to report to the Senior Information Risk Owner (SIRO) and other senior individuals at the Information Assurance Board (IAB). The briefing to the IAB will include;

- a summary of the events leading to the incident, where known;
- the incident itself;
- the immediate impact assessment and severity;
- the assessment by the IMT, where appropriate;

- the steps taken to recover from the incident;
- any residual impact following resolution;
- any qualitative or quantitative costs, if any, in relation to the incident including direct costs in respect of equipment or additional services, additional manpower hours accrued to include overtime working, any measurable loss of business services, and any impact to reputation; and any identified preventative or remedial action that should be undertaken to prevent reoccurrence.

Police Warning, Advice and Reporting Point (PolWarp), Computer Emergency Response Team for UK Government (GovCert) and National Management Centre (NMC)

NYP is a member of both the PolWARP and GovCert schemes, as well as being signed up to the NMC. This allows the sharing of information between member organisations relating to incidents, attacks or recently discovered vulnerabilities. It will be the responsibility of the ISO, and ICT in the case of Threat Intelligence received from the NMC, to monitor notifications from these sources and take appropriate action. Where applicable the DPO, ISO or appropriate representative, will call a meeting of the IMT to discuss and agree action resulting from such notifications.

It will be the responsibility of the DPO, ISO or representative, to ensure that all necessary communication with partner organisations or required bodies is undertaken; examples of such bodies would include PolWARP or GovCertUK. To facilitate this process the DPO and ISO will retain a list of all appropriate organisations and the communication methods and it will be the responsibility of the DPO and ISO to ensure that the accuracy of this list is maintained.

Internal Communications

Communication details in respect of all core and non-core IMT members will be conducted by the IMT Chair and will not be released for general circulation. It will be the responsibility of each individual IMT member to ensure that the IMT Chair is made aware of any changes in a timely manner.

It will be the responsibility of the IMT Chair to provide timely briefings to the SIRO and other senior staff members as appropriate. It will be the responsibility of the ISO to ensure relevant and timely communications with internal staff.

External Communication with Media Bodies

Should it be necessary to issue any form of statement or comment to the media in the event of an incident it will be the responsibility of the IMT Chair to liaise with the Force SIRO and, where applicable, the Heads of PSD and Joint Corporate Legal Services to develop a form of words appropriate to the incident and the action being undertaken. All media statements must be issued with the endorsement and assistance of Corporate Communications Department.

Responsibilities

Operational Officers/Police Staff

Are to be familiar with the Security Incident Handling Procedure and should act accordingly to report any identified incidents. All members should use the Security Incident Report e-form to report the incident, regardless of in hours/out of hours.

First Line Supervision

Are to ensure all staff are aware of, and adhere to, the Security Incident Handling Procedure. In addition, supervisors must report any incidents arising from the non-adherence to this procedure i.e. procedural incident.

Heads of Functions/Safer Neighbourhood Commanders

In addition to the above, Heads of Functions and Safer Neighbourhood Commanders may be required to attend and contribute to IMT meetings and provide resources and/or funding where appropriate.

Chief Officer Team

Overall responsibility for the security of all information assets.

Definition of Special Terms

ACPO -Association of Chief of Police Officers
ICT – Information Communication Technology
DPO - Data Protection Officer
GovCertUK - Computer Emergency Response Team (CERT) for UK Government
IAB - Information Assurance Board
IMT - Incident Management Team
ISO - Information Security Officer
MoPI - Management of Police Information
NMC – National Management Centre
NYP - North Yorkshire Police
PolWarp - Police Warning, Advice and Reporting Point
SIRO - Senior Information Risk Owner