Incident management procedure policy

1. Introduction

Ensuring personal information remains confidential and secure is everyone's responsibility and therefore, it is important to ensure that when incidents do occur, the damage from them is minimised and lessons learnt from them.

2. Purpose

The Incident Management Procedures set out how iQuda Ltd will investigate and manage information incidents; and provide staff with guidelines on identifying and reporting information incidents including near-misses. Where relevant they should be read in conjunction with the organisations Emergency and Business Continuity Plan.

3. Scope

The procedures apply to incidents that impact on the security and confidentiality of personal information. These information incidents can be categorised by their effect on our clients and their information:

- Confidentiality e.g. unauthorised access, data loss or theft causing an actual or potential breach of confidentiality – **the company operates a separate policy for handling Data Breaches, please refer to the QDBRP iQuda Data Breach Response Policy;**
- Integrity, e.g. records have been altered without authorisation and are therefore no longer a reliable source of information;
- Availability, e.g. records are missing, misfiled, or have been stolen which causes a delay.

These procedures apply to all staff including permanent, temporary, and locum members of staff.

4. Responsibilities

Every member of staff, whether permanent or temporary, is responsible for reporting information security incidents if they are the person to discover an incident has occurred. All staff play a part in identifying and reporting information security incidents.

5. Managing incidents

The organisation has assigned the role of incident manager to the information governance lead, Anthony Jones.

Any actual or potential information incident in the organisation will be assigned to one of the following categories, and investigated and managed accordingly.

A) Report that confidentiality has been breached or put at risk

Please note: the company operates a separate policy for handling Data Breaches; please refer to the QDBRP iQuda Data Breach Response Policy.

This could be reported by an affected client, a member of the public or other staff:

- Interview the complainant to establish the reason for the complaint and why the organisation is considered to be responsible;
- Investigate according to the information given by the complainant;
- Record findings, e.g. unsubstantiated concern, suspected/potential breach, actual breach, etc;
- Where necessary, provide written explanation to the client with formal apology if warranted;
- Take and document appropriate action, e.g. no further action as there is no evidence that information was put at risk, advice/training, disciplinary measures, etc.

B) Inadequate disposal of confidential material

Please note: the company operates a separate policy for handling Data Breaches; please refer to the QDBRP iQuda Data Breach Response Policy.

This type of incident may lead to a breach of confidentiality and is likely to be reported by an affected client, a member of the public, or a member of staff and could be paper, hard drive, disks/tapes, etc:

- Investigate how the information left the organisation by interviewing staff and contractors as appropriate;
- Consider the sensitivity of the data and the risk to which the client(s) have been exposed, e.g. breach of confidentiality, misuse of data;
- Consider whether the client(s) should be informed and where it is judged necessary, provide written explanation to the client(s) with formal apology;
- Record findings, e.g. potential breach, actual breach, evidence of misuse, etc;
- Take and document appropriate action, e.g. advice/training, disciplinary or contractual measures, etc.

C) Attempted or actual theft of equipment and/or access by an unauthorised person

Please note: the company operates a separate policy for handling Data Breaches; please refer to the QDBRP iQuda Data Breach Response Policy.

This type of incident may lead to a breach of confidentiality, the risk that information has been tampered with, or information not being available when needed:

- Check the asset register to find out whether equipment is missing;
- Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual base);
- If the cause is external inform the police, ask them to investigate and keep them updated with your findings;
- Interview staff and check the asset register to establish what data was being held and how sensitive it is;
- Establish the reason for the theft/unauthorised access, such as:
    - Items to sell;
    - Access to material to embarrass the organisation;
    - Access to material to threaten clients (e.g. blackmail, stigmatization).

- Consider whether there is a future threat to system security;
- Inform insurers;
- Review the physical security of the organisation;

- If there has been unauthorised access to the organisation computer system:
  - Ask the system supplier to conduct an audit to determine whether unauthorised changes have been made to client records;
  - Consider whether any has been delivered to clients whose records have been tampered with;
  - Check compliance with access control procedures, e.g. ensure passwords haven't been written down, staff members are properly logging out, etc.
- Consider the sensitivity of the data and the risk that it has been tampered with or will be misused, in order to assess whether further action is appropriate (e.g. warning clients);
- If computer hardware or the core software has been stolen, inform system suppliers to enable restoration of system data to new equipment;
- Record findings, e.g. potential breach, actual breach, evidence of tampering, compromised or delayed service delivery, etc;
- Take and document appropriate action, e.g. physical security improvements, advice/training, disciplinary measures, etc.

D) Computer misuse by an authorised user

This includes browsing client records when there is no requirement to do so; accessing unauthorised Internet sites; excessive/unauthorised personal use, tampering with files, etc.

- Interview the person reporting the incident to establish the cause for concern;
- Establish the facts by:
  - Asking the system supplier to conduct an audit on activities by the user concerned;
  - Interviewing the user concerned.
- Establish whether there is a justified reason for the alleged computer misuse;
- Consider the sensitivity of the data and the risk to which the client(s) have been exposed, e.g. breach of confidentiality; the risk information may have been tampered with; and consider whether the client(s) should be informed;
- Record findings, e.g. breach of confidentiality, evidence of tampering, fraud, carrying on a business, accessing pornography, etc;
- Take and document appropriate action, e.g. no action as allegation unfounded, training/advice, disciplinary measures, etc.

E) Lost or mis-filed records

Please note: the company operates a separate policy for handling Data Breaches; please refer to the QDBRP iQuda Data Breach Response Policy.

This type of incident could have a possibly severe impact on the business as the information is incorrect or is not available when required:

- Investigate who last used/had the paper record by interviewing staff and contractors as appropriate;
- Consider whether any services have been provided based on incorrect information within a client record;
- Consider whether service delivery has been delayed due to information not being available;

- Establish whether missing information can be reconstituted, e.g. from electronic records;
- If information within records has been misfiled, ensure it is restored to correct filing order/returned to the correct record;
- Where necessary, (i.e. if service delivery is affected) provide a written explanation to the client with formal apology;
- Record findings, e.g. compromised or delayed service delivery, etc;
- Take and document appropriate action, e.g. advice/training, disciplinary or contractual measures, etc.

F) Breach of policy leading to Information Security Risk

Please note: the company operates a separate policy for handling Data Breaches; please refer to the QDBRP iQuda Data Breach Response Policy.

- Interview the offending staff member to establish why policy was potentially breached;
- Investigate according to the information given by the complainant;
- Record findings, e.g. unsubstantiated concern, suspected/potential breach, actual breach, etc;
- Fill in Incident Report Form
- Where necessary, provide written explanation to any affected clients with formal apology if warranted;
- Take and document appropriate action, e.g. no further action as there is no evidence that information was put at risk, advice/training, disciplinary measures, etc.

6. Collecting, identifying and preserving evidence

When an incident occurs, information which can serve as evidence should be identified, collected and preserved accordingly. The main reason for the collection of evidence is to resolve the incident, however in some cases this evidence may be used in relevant legal proceedings. It is important to correctly document evidence collected.

Indentifying evidence

Evidence can be identified as information that provides proof of an incident occurring.

Types of evidence you may wish to collect:

- Identifying information that pertains to where to incident occured (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer).
- Telephone recordings (if the breach or incident took place over the phone)
- Computer Screenshots – if the incident was discovered to have taken place on a computer, for example a malware attack.
- CCTV records (the ISM can assist with accessing the CCTV records)
- An attacking hosts IP address
- Copies of an email containing information that proves an incident has occurred
- Date and time the incident occurred

- Any witness statements

How to collect evidence:

- If evidence can be collected easily (e.g. a confidential document left by the printer), this can be passed directly to the ISM Anthony Jones. In cases where you are aware an incident has occurred, but you cannot provide evidence directly, report the incident to your manager who will collect appropriate evidence if it is available. This may be achieved for example by accessing CCTV records, telephone recordings, or event logs.

Preserving evidence:

Evidence should be passed to the Information Governance Lead and Information Security Manager Anthony Jones who will log and preserve the evidence in the iQuda Incident Report Form Log.

7. Lessons learned

The organisation maintains a register of all incidents occurring within the organisation. This register of incidents and the resulting actions taken will inform the other policies and procedures within the organisation. Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

All registered incidents are re-evaluated after a 6 month period to assess the effectiveness of the implemented actions in ensuring that either the type of incident is no longer being reported or the volume of those types of incidents has reduced. If there is no change in the volume of each type of incident the Senior Management Team is alerted and appropriate action taken. The incident will also be reported to the business owners for review during Management Review Meetings.

To provide staff with an example of what could occur, how to respond to such events and how to avoid them, previous incidents may be used in security and confidentiality training sessions.

8. Approval

These procedures have been approved by Anthony Jones, and they will be reviewed on at least an annual basis and in particular in the event of an incident.

Information Asset Incident Management Procedure

GUIDELINES ON IDENTIFYING AND REPORTING INFORMATION INCIDENTS

These procedures apply to all staff including permanent, temporary, and locum members of staff. All incidents must be reported to your line manager and/or the organisation's information governance lead [Anthony Jones] as soon as possible after the event. The QIRF iQuda Incident Report Form must be used. This can be found on SharePoint.

What should you report and how can you indentify information incidents?

Here are some examples of information incidents that should be reported:

- Finding a computer printout of client data where it is not relevant to the work being carried out;
- Finding a document containing client data, the back of which is used for a shopping list, in the supermarket;
- Finding a sensitive document in the staff toilet within the organisation;
- Identifying that a fax that was thought to have been sent to someone else had been received by the wrong person;
- Losing an unencrypted laptop computer or other portable device with personal information on it;
- Giving information to someone who should not have access to it – verbally, in writing or electronically;
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password;
- Trying to access a secure area when not authorised to access that area;
- Finding your PC and/or programmes aren't working correctly – potentially because you may have a virus;
- Sending a sensitive e-mail to 'all staff' by mistake;
- Finding a colleague's password written down on a 'post-it' note;
- Discovering a 'break in' to the organisation.
- Finding confidential waste in a 'normal' waste bin.

How should you report an incident?

If you discover something that could be considered as an incident you should report it directly to the information governance lead, Anthony Jones and complete a QIRF iQuda Incident Report Form. This can be found on SharePoint.

If an incident involves personal data, it may need to be reported to the Information Commissioners Office (ICO). In this event, the Data Protection Officer Garth Macintosh will advise you further.

Ensure you enter the following information on the form:

- Your name;
- The date you discovered the incident;
- Where the incident occurred;
- Details of the incident;
- Any initial actions that you took - including who the incident has been or will be reported to and the date the report is made.
- Any evidence you have collected

What happens next?

Your information governance lead Anthony Jones or Data Protection Officer Garth Macintosh will investigate the incident and may wish to speak to you directly as things progress.