Data Breach Policy

iQuda Ltd is hereinafter referred to as iQuda and "the company".

1.0 Introduction

iQuda holds and processes a large of personal data. The company recognizes its obligation to protect this asset to prevent it from being disclosed or damaged while in our care. Every care is taken to protect personal data from accidental or intentional incidents in order to avoid a data protection that could compromise data in our care.

Compromise to the confidentiality, integrity or availability of information in the company's care may result in harm to individual(s), reputational damage, detrimental effects on service provision, legislative non- compliance, and/or financial costs. It is therefore important that there are measures in place to report breaches as soon as they are detected.

2.0 Purpose

iQuda is obliged under the Data Protection Act 2018 and the General Data Protection Regulations 2016 (the GDPR) to have a framework in place to ensure the security of all personal data. The company is obliged to assign clear lines of responsibility in relation to data protection.

This Policy sets out the process the company has designed to effectively handle data breaches and ensure we comply with the above regulations.

3.0 Scope

This Policy relates to all personal and sensitive data held by iQuda in any format. Personal data means information that relates to an identifiable individual. In short, if a living individual can be identified from a piece of information it is classified as personal data.

This Policy applies to all staff working at iQuda, whether permanent or temporary and includes work experience placements, business owners, consultants, contractors and suppliers.

The objective of this Policy is to contain any breaches, to report breaches effectively, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4.0 Definition / Types of Breach

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents. Suspected incidents will be treated as data breaches where there is substantial evidence to suggest that a breach has occurred.

An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of data, either accidentally or deliberately, and has caused or has the potential to cause damage to data in the company's care, whether that data belongs to the company or to our employees, clients or other stakeholders.

and/or reputation.

A data breach incident includes but is not restricted to, the following:

- The loss or theft of personal or sensitive data or a system that contains personal or sensitive information (for example, a laptop, a tablet device, a Smartphone, a USB drive or paper records).
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data

5.0 Reporting an incident

Any individual who accesses, uses or manages the company's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer. The Data Protection Officer can be reached by phone on 01442 251 514 or by email on info@iquda.co.uk

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (document reference: QIRF iQuda Incident Report Form).

All staff should be aware that any breach of the Data Protection Act may result in iQuda's Disciplinary Procedures being instigated.

The Data Protection Officer will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then they will notify the Information Commissioners Office (ICO). If the risk is unlikely to have an adverse effect to people's rights and freedoms, the breach will not be reported. In these circumstances case, the Data Protection Officer will document their decision not to report a breach.

6.0 Containment and Recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform relevant parties such as the police, where appropriate.

Advice from experts across the company may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and Risk Assessment

An investigation will be undertaken by the LIO immediately and wherever possible within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved, especially whether it contains personal or sensitive data
- its sensitivity
- any protections in place (e.g. encryptions)
- what's happened to the data, has it been lost or stolen
  whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

8.0 Notification

The LIO and / or the DPO will determine who needs to be notified of the breach.

Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

- Whether the ICO should be notified of the breach.
- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals must be notified if there data has been breached if there is a high risk to their rights and freedoms as a result of the breach. Notification to the individuals whose personal data has been affected by the incident will include the name and contact details of the data protection officer, a description of the likely consequences of the personal data breach and a description of the measures taken or proposed to deal with the personal data breach including the measures taken to mitigate any possible adverse effects.

Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact iQuda for further information or to ask questions on what has occurred. If an individual will be notified, they must be notified without undue delay (as soon as possible).

The LIO and or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

All actions will be recorded by the DPO.

9.0 Timeframes

Where a breach must be reported to the ICO, it must not be reported any later than 72 hours after the breach is first detected. If there is a delay, the ICO must be informed of the reasons for the delay.

10.0 Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum the amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the Executive Management Team.

11.0 Policy Review

This policy will be reviewed at least annually. The policy will be reviewed before this timeframe if new legislation or guidance is released by the relevant supervisory authority.