iQuda information security policy

1. Introduction

This policy is concerned with:

- the management and security of iQuda Ltd (iQuda)'s information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to iQuda)*; and
- the use made of these assets by iQuda's staff and others who may legitimately process information on behalf of iQuda.

*Information assets include but are not limited to: company data, client data, employee data, records, servers, workstations, client servers, client workstations, databases etc.

This overarching policy document provides an overview of information security.

2. Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

Furthermore, iQuda is committed to compliance with the General Data Protection Regulations 2016 (the GDPR). In line with the regulations, we are committed to practising the highest standards of data protection, in order to safeguard any and all personal information in our care or processed by the company.

3. Scope

The documents in the Information Security Policy set apply to all information assets which are owned by iQuda, used by iQuda for business purposes or which are connected to any networks managed by iQuda.

The documents in the Information Security Policy set apply to all information which iQuda processes, irrespective of ownership or form.

The documents in the Information Security Policy set apply to all staff at iQuda and any others who may process information on behalf of iQuda.

4. Definitions

Personal information is defined as

The General Data Protection Regulations 2016 defines personal information or data as any information that relates to an identifiable person who can be identified, directly or indirectly, from that information (the data subject).

Personal data can include:

- Names
- Dates of birth
- Location data
- Email addresses
- Addresses
- Identification numbers
- IP addresses
- Pseudonymous data
- Online identifiers

iQuda is committed to protecting all personal information that is processed by the organisation or in our care. Regardless of whether it pertains to our staff, our clients, or any other stakeholders.

5. Information Security Principles

The following principles underpin this policy:

1. Information will be protected in line with all of iQuda's relevant policies and legislation, including those relating to data protection.
2. All iQuda databases, or those managed on behalf of our clients, will be accessible only to individuals who have been given a password, and trained in the use of the database. All databases will be managed by a database manager / administrator, who will define access rights and maintain information quality.
3. Information should be accessed solely by those who have a legitimate need for access.
4. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification and our confidentiality policy.
5. It is the responsibility of all individuals who have been granted access to iQuda information or that of our clients, to maintain security over that information, whether it is on paper, verbal, or electronic. This means taking steps to ensure that the information is not viewed or accessed by people who have no need to access it.
6. Information will be protected against unauthorised access through the password policy and through the requirements of this policy.
7. Compliance with the Information Security policy is mandatory and may be enforced.
8. Any data including backups must be encrypted to at least AES256.
9. Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment. This should be done on a secure separate network and virtual environment where applicable, with no direct access to the live environment i.e. the iQuda workshop.
10. Passwords must be changed at least once every 365 days, in order to protect the integrity of our information assets and those of our clients. Line of business applications will be protected through the use of passwords & 2-factor authentication. Passwords must follow the guidelines of the iQuda Password Policy.

11. If you are unsure about how to handle information, treat it as top secret until you have sought clarification from a member of the management team.
12. iQuda reserves the right to revoke access rights, without warning, if an employee is found to be noncompliant with this policy. Noncompliance may result in disciplinary proceedings being carried out against the member of staff responsible.

6. Print Policy

iQuda has a variety of printers, including multi-function-devices, (network printer, copier, scanner), network printers for workgroups and USB printers for individual print users.

No documents containing PID relating to our clients or their stakeholders are to printed under any circumstances.

Any documents containing sensitive information or confidential data that pertains to iQuda must be collected as soon as possible after the print job is sent from the workstation.

Physical copies of sensitive information or confidential data pertaining to our clients or their stakeholders should not be used under any circumstances. Physical copies of sensitive information or confidential data pertaining to iQuda or its staff must be kept secure at all times. Do not store any records, which contain personal or sensitive data relating to iQuda unnecessarily or for longer than necessary. Files containing such information should be kept in the dedicated locked filing cabinets or locked desk drawers with access strictly on a “need to know” basis by the authorized persons.

Once the physical copy of data is no longer required it must be properly disposed of. This means being placed into a cross paper shredder and shredded.

7. Information handling and transmission principles

The following principles underpin this policy:

1. Online privacy policies are clearly displayed on all emails sent by iQuda and it’s staff.

2. Confidential data or sensitive information relating to iQuda or it’s staff should only be printed, communicated verbally or copied electronically when necessary for the following reasons:
    a. When authorized by upper management;
    b. Communications with other professionals where consent has been given;
    c. Data back ups. Data backups are encrypted to at least AES256;
    d. Work schedules to facilitate effective working practices.
    e. Where data is copied to electronic media (Encrypted Media Only), or printed it should be stored securely, and securely destroyed when no longer required. Any electronic files or copies are encrypted to at least AES256. Please also see note 6 below.
3. Staff working remotely will only access data by using the iQuda Remote Terminal Server, which is a secure connection, restricted by two factor and active directory authentication. Any remote access devices are fully encrypted to at least AES256 and have remote wiping implemented.

4. If staff do not have access to the iQuda remote access Terminal Server, and need to access iQuda or client data away from the head office, they will need to speak to their direct manager who will decide whether access is required.
5. No confidential information is sent by fax.
6. Confidential information should be sent only from a iQuda verified, secure email account registered to the iQuda.co.uk domain wherever possible.
7. Where confidential information is communicated verbally, staff should ensure that iQuda procedures are followed.
8. No PID data should be printed or distributed under any circumstances.
9. Any remote access devices are fully encrypted to at least AES256 and have remote wiping implemented.
10. Devices containing information and data must be wiped to at least HMG S5 standards after use. Retired computers/devices are overwritten with 7 passes before being physically destroyed. At end of life all electronic files must be multi pass patterns wiped to HMG S5 on site prior to disposal and degaussed or physically destroyed.

8. Enforcement

This policy will be enforced by the Executive Team and Data Protection Officer. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. In the event of a policy breach that leads to a data breach in violation of the GDPR, the Data Protection Officer may need to report the breach to the Information Commissioners Office (the ICO). Please refer to the QGDPR iQuda GDPR Policy and the QDBRP iQuda Data Breach Response Policy for more information.

9. Policy review

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

10. Practical guidelines

Do:	Don't
• Seek advice from your line manager or a iQuda director if you are unclear about any aspect of information security.	• Disclose your password to anyone or ever share passwords.
• Report any loss or suspected loss of data to your line manager or a iQuda Director.	• Use a personal email account for conducting iQuda business.
• Change your password if you have any	• Use a iQuda email account for conducting

Do:	Don't
suspicion that it may have been compromised.	personal business, or use iQuda email distribution lists for personal emails.
• If you use iQuda supplied portable media to store or process data pertaining to iQuda or its clients, destroy the data securely when you have finished using it. At end of life all electronic files must be multi pass patterns wiped to HMG S5 onsite prior to disposal and degaussed or physically destroyed.	• Make copies of restricted iQuda information without permission.
• Mobile devices are encrypted to at least AES25.	• Provide access to iQuda information or systems to those who are not entitled to access.
• Password protect your personally owned devices.	• Undermine or seek to undermine the security of computer systems, for example, by installing unauthorized software..
• Keep all of the software on your personally owned devices up to date, and install anti-virus protection.	• Leave your computers unlocked when left unattended.
• Comply with the law and iQuda policies.	• Leave hard copies of confidential information unattended or unsecured.
• Be mindful of the risks of using open (unsecured) WiFi hotspots or computers in internet cafes, public libraries etc.	• Assume that Information Security is someone else's responsibility. **It is the responsibility of all iQuda staff.**
• All data including backups are encrypted to at least AES256.	• Access websites known to be infected with viruses or suspicious materials. • Access websites that are unacceptable at work (e.g. containing pornographic, explicit or illegal content).
• Report any suspicious occurrences, such as the appearance of viruses, Ransomware, Trojans or other malicious computer threats.	• Fail to report suspicious occurrences, even if you aren't sure of their severity.