iQuda portable devices policy

1. Introduction

iQuda's information security policy is intended to provide a pragmatic, workable policy that provides an optimum level of security while remaining compatible with our day to day activities and workload.

The security of information on laptops and portable media is seen as a high-risk area. This policy provides guidance to cover security in this area.

2. Purpose

iQuda is concerned with ensuring that all sensitive information and confidential data is used in a secure manner. Portable electronic storage devices are widely used, and iQuda needs to ensure that their use does not compromise data security.

3. Scope

All staff working for or on behalf of iQuda who have access to our information and that of our clients, and specifically those users who have access to any Personally Identifiable Data (PID) need to read and comply with this policy.

4. Definitions

Portable device means any of:

- Laptop computer, notebook computer, netbook etc, typically running windows, MacOS, Unix or Linux
- PDA (Personal digital assistant)
- Tablet
- Phone, smartphone, MP3 player or any other device with data storage or data access capacity

Portable medium means any of:

- CD or DVD
- External hard disc
- USB memory stick
- Storage card

Personal information is defined as

The General Data Protection Regulations 2016 (GDPR) 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:

1. Names
2. Dates of birth
3. Location data
4. Email addresses
5. Addresses

6. Identification numbers
7. IP addresses
8. Pseudonymous data
9. 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.

Confidential information is privileged or proprietary information that could cause harm, including reputational damage, to iQuda, our clients or to individuals.

5. Policy

Portable devices

All iQuda laptops that are used both inside and outside of the office are encrypted to at least AES256. Staff must ensure that a laptop without encryption is never used outside our office for work involving personal or confidential information. All laptops and portable media must be kept secure at all times by the employee responsible for them. If a device contains any PID, it will have remote wiping implemented.

Personal Mobile Devices

Personal mobile devices may not be used for work purposes, except for email (by approval) & for 2-factor authentication.. Email may be accessed through your personal mobile phone, however approval must first be sought by requesting access through the QRF iQuda Change Request Form process. If you access work email, a secure screen lock with password must be enabled. It would be best to also encrypt your mobile device, if possible.

In the event that a personal mobile phone is lost, you must report this to Anthony Jones as soon as possible.

Cryptographic Keys

All cryptographic keys, resulting from the encryption of portable devices, must be protected during their lifetime. Cryptographic keys may be used for the lifetime of a machine only. After a machine is retired, the cryptographic key must be destroyed. This applies to the entire lifecycle of each encrypted device.

Portable devices Register

All devices are to be signed for in the portable devices register. This is controlled by Vince de Beer. Please speak to Vince if you require a portable device.

Transportation

iQuda policies apply to all iQuda owned devices and media. This includes devices and media that are in transportation. All devices and media transported are the ultimate responsibility of the user transporting it - this is detailed in the staff handbook. Devices and media containing information shall be protected

against unauthorized access, misuse or corruption during transportation. All portable devices are to be signed for in the portable devices register. No personal devices are permitted for transportation of data. The staff member(s) transporting a device or media storage device are responsible for it's adequate protection during transportation. Staff are expected to apply due diligence while transporting devices.

Portable media

iQuda will issue encrypted portable USB storage devices to authorised staff. iQuda owned PC's and portable devices will only allow the copying of iQuda data or that of our clients to a iQuda encrypted USB device. This policy has been established to protect the data held by iQuda in its secure data files.

- Authorised staff will be entitled to use USB devices to transport data. Encrypted USB memory sticks and external hard drives, which meet the minimum security standard are issued to authorised users. The minimum security standard is: 256 bit Advanced Encryption System (AES). If a device contains any PID, it will have remote wiping implemented.
- A record will be kept of USB sticks, external hard drives and passwords issued so that they can be traced and the information retrieved if the storage devices are lost or the user forgets the password.
- No staff will be authorised to use their own pre-encrypted USB sticks or external hard drives.
- Staff cannot bring their own USB sticks into iQuda.

Sending data in an email attachment

Staff must ensure that they comply with iQuda data protection policies when sending information in an email attachment.

Destruction of data

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.

6. Responsibilities

All staff with access to iQuda information are responsible for adhering to this policy. If a USB stick or external hard drive is issued, and lost, please inform Anthony Jones or Vincent de Beer immediately.

7. Information handling and transmission principles

The following principles underpin this policy:

- Confidential client information containing PID must never be printed under any circumstances. Confidential staff or client information and data must only be printed, communicated verbally or copied electronically when necessary for the following reasons:
    - Communications with clients, management and other pre-authorized persons;
    - Communications with other professionals where consent has been given;
    - Data back ups (these will comply with iQuda encryption and remote wiping policies);

    - Work schedules to facilitate effective working practices.
    - Where data is copied to electronic media, or printed it will be stored securely, and securely destroyed when no longer required.
    - 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.
- Staff working remotely must access data by using the iQuda remote access Terminal Server, which is a secure connection, restricted by two factor and active directory authentication.

- If staff do not have access to the iQuda Remote Access Terminal Server, and need to access company or client data away from the office, they must follow process and contact their direct manager requesting the required access.

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.