iQuda remote access policy

Introduction

Remote Access refers to any technology that enables iQuda to connect users in geographically dispersed locations. Technologies currently used by iQuda for remote users to connect to iQuda networks are:

1. Terminal services. Used by staff to connect to iQuda files and systems remotely if specifically authorised to do so.
2. Remote email access. Used by any individual with a iQuda email account to check emails and calendars remotely.
3. VPN. Used by iQuda staff to connect to the shared networks.
4. Teamviewer, Ncentral and similar. Used by iQuda and potentially other remote suppliers to resolve specific maintenance issues for ourselves or our clients. This access is for limited periods only and requires authentication before use.

Purpose of Policy

This document sets out the policy for remote access to iQuda systems or networks via **any means.**

Scope

This policy covers all types of 'roving' remote access using Terminal Services, including potentially:

- Travelling users (e.g. Staff working off-site or temporarily based at other locations)
- Home workers
- Non iQuda staff (e.g. Contractors and other 3rd party organisations)

Responsibilities

- The Managing Director at iQuda is ultimately responsible for IT security.
- The Manager Director will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.
- The Managing Director is responsible for providing authorisation for all remote access users and the level of access provided, and is responsible for ensuring that remote access by staff is managed securely.
- The Service Desk Manager will ensure that user profiles and access controls are implemented in accordance with iQuda policy.
- The Technical Team will ensure that appropriate systems are in place to uphold the integrity of the security employed at iQuda.
- All **remote access users** are responsible for complying with this policy and associated standards. They **must** safeguard corporate equipment and information resources and notify iQuda immediately of any security incidents and breaches.
- All remote connections must have 2-factor authentication enabled.

Applying for remote access

- The member of staff will request remote access from their direct manager.
- The Direct Manager will email and ask the Managing Director for approval.
- The Managing Director will approve by return email.

- The Service Desk Manager will input the individual's phone details into the system, and send the individual a message with details of how to access the two-factor authentication system.

All applications for remote access must be done through the QRF iQuda Change Request Form. This can be found on the shared company server.

The member of staff is now able to access the iQuda network remotely. The level of access that they have will depend on their existing IT profile & user access privileges.

Please see appendix one to this policy for more detail on connecting to iQuda's systems remotely.

Security

1. User Identity

All remote users must be registered and authorised as described above. User identity will be confirmed by:

a. user ID and password authentication
b. two-factor authentication

The Service Desk Manager (Vincent de Beer) is responsible for ensuring a log is kept of all users of remote access.

2. Perimeter Security

The Technical Team (led by James Watson) will be responsible for ensuring perimeter security devices are in place and operating properly. These comprise:

a. Perimeter security solutions to control access to critical network applications, data, and services so that only legitimate users and information can pass through the network.
b. Routers and switches to handle this access control lists and by dedicated firewall appliances.
c. A firewall to provide a barrier to traffic crossing a network's "perimeter" and permitting only authorised traffic to pass, according to a predefined security policy.
d. Complementary tools, including virus scanners and content filters, to help control network perimeters.

3. Security Monitoring

The Technical team are responsible for monitoring the effectiveness of the network's security.

4. User Responsibilities, Awareness & Training

iQuda will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action(s).

Reporting Security Incidents & Weaknesses

All security weaknesses and incidents must be reported to the Managing Director (Anthony Jones) and the Technical Team. Incidents will be reviewed by the Data Protection Officer (Garth Macintosh) who will

establish whether the incident must be reported to the Information Commissioners Office (ICO). This will apply in the event that the event poses a risk to the rights and individuals of individuals, as governed by the General Data Protection Regulations 2016 (the GDPR).

Guidelines and training

All remote users will be provided with training on remote access procedures.

Day to day considerations

Security

- Remote access to iQuda IT networks is covered by the same security policies as access within the iQuda office building.
- At no time should any iQuda employee provide their login or password to anyone, not even family members.
- The employee with remote access privileges must also ensure that that the remote link is not used for illegal activities, or in the pursuit of outside business interests. Each employee bears responsibility for the consequences should the access be misused.
- All staff working on iQuda data at home must have constant regard to the need for security over confidential data. All staff must log off the network when they have finished working on it, to reduce the risk of unauthorised access.
- Line of business applications may only be used within a Terminal Server environment when outside the iQuda Office.

Practicalities

- Any staff planning to work from home on days when they would normally be present in the office must request prior approval from their line managers. Staff should be aware of pressures on other staff members which may arise if the office is inadequately staffed.
- Remote working is dependent on a reliable Broadband connection. iQuda will not pay for this connection, or for the running costs of the connection.
- It is the responsibility of each member of staff to ensure that the equipment to be used when working at home is suitable. Home computer equipment should be adequate for the accessing of the iQuda network, and chairs and desks should be safe and suitable for extended periods of work. iQuda will not pay for additional equipment to be used when working at home.
- The remote working facility is offered to allow staff members to work according to their contracts of employment. Therefore, the facility should not be used for activities which are unrelated to the individual's contractual obligations.
- Remote access is provided to allow staff to choose where they can best work as contractually obliged to do so. It is not provided to allow or enforce working additional hours over and above contracted or pre-agreed overtime hours.

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. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

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.

Appendix One: Objectives, Principles and Risks of Remote Access

Objectives

The objectives of iQuda's policy on remote access by staff are:

- To provide secure and resilient remote access to iQuda's information systems.
- To preserve the integrity, availability and confidentiality of the iQuda's information and information systems.
- To manage the risk of data loss, serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.
- To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that iQuda is adequately protected under computer misuse legislation.

Principles

In providing remote access to staff, the following high-level principles will be applied:

- A senior manager of iQuda will have overall responsibility for each remote access connection to ensure that iQuda's policy and standards are applied.
- Managers will have authority to approve flexible working with their teams, so long as iQuda's business needs always overrule other considerations.
- Remote users will be restricted to the services and functions necessary to carry out their role.

Risks

iQuda recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

- Unavailability of network, systems or target information
- Degraded performance of remote connections
- Loss or corruption of sensitive data
- Breach of confidentiality
- Loss of or damage to equipment
- Breach of legislation or non-compliance with regulatory or ethical standards.