# iQuda supplier security policy

## Purpose

The purpose of this policy is to identify the process necessary to establish the technological means and perquisite level of trust between iQuda and their approved Third Parties (including suppliers), to facilitate all involved entities with a clear understanding of the purpose of the relationship, and the connection type, and agree the responsibilities assumed by establishing the contract. In addition, iQuda need to adhere to the General Data Protection Regulations 2016. This policy therefore sets out our approach towards compliance in relation to supplier security agreements.

This iQuda Policy must be agreed, by all commercial entities external to their operational estate where remote access to assets is required. Furthermore, all Third Parties connected to the iQuda network must comply with the following policy statements:

Third Party access to the iQuda network potentially exposes their internal applications, systems, and infrastructure to risk, and therefore an established agreement must be in place that assures the contracted service is supplied aligned to the iQuda expectations of security.

## Access must be disabled by Default

Third Parties, including suppliers of systems, must have their access to iQuda's applications, systems and infrastructure denied by default. Thereafter, access to any such asset must only be enabled for *specific*, *agreed* and *documented* tasks which has been subject to approved by the iQuda System Administrator.

## All Third Parties Apply iQuda's Security Policies

To provision a level of assurance, all iQuda Third Parties must agree to the relevant areas of iQuda's Security Policies as applicable. The relevant policies will be supplied for agreement by all Third Party Providers prior to them establishing any connection to any iQuda asset.

## Supplier Contracts

In line with the GDPR, supplier contracts will cover the following:

*NB: in the event that iQuda engages the supplier, they will be considered the 'processor' and iQuda the 'controller'.*

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

**Third Parties – Managing Change**

All Third Party connections *must* have a clearly defined Change Management Process. This control is applied to provide iQuda with a level of governance to ensure the agreed connection is maintained in an agreed condition, and profile, and that any required change(s) will be communicated, and agreed prior to them being promoted to an operational state.

iQuda operates a change request procedure. Please refer to the QRF iQuda Change Request Form for further information.

**Incident Response**

An IT Security Incident is an adverse event or condition that can impose the potential to adversely impact iQuda, their partners, and their associate's assets; or which can impose complete or part denial-of-service to their operations. For this reason any *actual*, *inferred*, or *suspected* incident imposing treat to *any* iQuda asset, or service being provided, or supported by a Third Party, must be reported to the iQuda system administrator as soon as is practicable.
An information Security Incident includes, but is not restricted to the following examples:

- The loss or theft of data or information
- Accidental, or illicit transfer of data, or information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data, information storage, computer systems, or infrastructure
- Unauthorised changes to information, data, system hardware, firmware, or software characteristics
- Unwanted disruption or Denial-of-Service (DoS) against any iQuda asset
- The unauthorised use of a system for the processing or storage of data by any person

**Incident logging**

A log is kept of all supplier incidents that occur. This process allows us to continually review the suitability of the suppliers that work with iQuda. The logic behind this process is that if multiple negative incidents occur frequently, iQuda will look to change the suppliers we use. We also use incident logs to make informed decisions, and for incorporation into our lessons learned process. The name of this log is the QATPL iQuda Approved Third Parties List, Review Process and Supplier Incident Log. This document can be found on SharePoint. It is controlled by the Data Protection Officer.

## Definition of Third Parties

Third parties are defined as any entity not employed directly by iQuda that require access to their premises (physical), or assets (logical).

Third Parties are individuals and organisations which fall into the following categories. These will include, but not be limited to:

- Hardware and software maintenance and support staff
- Cleaning, catering, security guards and other outsourced support services
- Temps and agency staff
- Staff working on Contractual basis
- External IT support staff
- Suppliers (including Suppliers of IT goods, systems or services)

## Third Party Service Level Agreement (SLA)

iQuda requires suppliers to adhere to specific service level agreements in order to maintain their status as a suitable provider. We use the following service level agreement table as a framework for categorizing supplier outages according to their variety. This SLA feeds into the supplier incident response process, which is in turned used by the iQuda management team in making an informed decision about whether or not a supplier is still a suitable service provider to iQuda. To illustrate, if a supplier has frequent critical or high priority service issues, management will be required to look for an alternative supplier to ensure business continuity.

Supplier incidents are logged via the QIRF iQuda Incident Report Form and the QATPL iQuda Approved Third Parties List, Review Process and Supplier Incident Log. Located: smb://kcs-dc/Managers/ISO 27001:2013 Standards Documents

| Problem | Priority | Response Required | Resolution Time |
|---|---|---|---|
| A business critical service is not available resulting in all users and functions being unable to work. | 1 Critical | 30 minutes | ASAP — Best Effort |
| Significant degradation of service where a large number of users or business critical functions are affected. | 2 High | 1 hour | ASAP — Best Effort |
| Limited degradation of service (limited number of users or functions affected, with business processes till able to continue). | 3 Normal | 4 hours | ASAP — Best Effort |
| Small service degradation (business process can continue, one user affected). | 4 Low | 4 hours | ASAP — Best Effort |
| Regular but minor issues, for example password resets (although Customer | 4 Low | 8 hours | ASAP — Best Effort |

| | | | |
|---|---|---|---|
| agrees to use reasonable endeavours to resolve such issues internally where practicable) | | | |

### Supplier Review Policy

iQuda regularly reviews our suppliers and the services they provide in order to ensure their suitability and competency. Because services change over time, it is important that they are regularly reviewed to ensure their suitability and to provide the best possible business continuity for iQuda. Performance of suppliers is monitored through this process, in line with supplier SLAs in order to hold suppliers responsible. The QATPL document is used for our supplier review process. This document is located on SharePoint & is controlled by the Data Protection Officer.

### Process Agreement

This part of the Third Party Access Policy defines the process that will be followed to be completed for authorised access to iQuda assets:

- The initial requirements shall normally be captured during the initial contract negotiation
- Initiate a dialogue between iQuda and the Third Party to include a detailed definition of the requirements of the connection (i.e. which systems the Third Party will have authorised access to, and as to the privileges, and profile of access to application/systems which are in scope
- Ensure a Non-Disclosure Agreement is agreed and signed by the Third Party. See QNDA.
- A successful *on-site*, or *off-site* Security Review will have been conducted to assure that the security requirements of iQuda have been satisfied
- Extended periods of access are subject to periodic reviews.
- Access will be terminated as soon as no longer required to support an operational task.

### Appendix A – Third Party Network Access Agreement

Agreement between iQuda and their contracted Third Parties is considered a formal agreement for access to any specified asset, application, system, infrastructure, data, and information as is appropriate under the terms of the established contract, and/or any other related SLA's.

| **General Information (completed by iQuda)** | | |
|---|---|---|
| **Date of Security Review** | | |
| **Name of Third Party requesting Remote Access** | | |
| **Non-Disclosure Completed and signed** | **Yes** q | **No** q |
| **Contract or non-disclosure contains relevant GDPR clause** | **Yes** q | **No** q |

| | |
|---|---|
| **Agreed hours of support/access** | |
| **Purpose of Connection** | |
| **Is there sufficient technical understanding of requirements between iQuda and the Third Party to proceed with the request?** | **Yes** q **No** q |
| **If No above – explanation** | |
| **Proposed technical method of connection (as agreed by the iQuda System Administrator)** | SSL, VPN, Token, X509 etc |
| **Description of the iQuda assets to be accessed (server names, IP addresses)** | |
| **Will the Third Party have any *direct*, or *indirect* access to *any* sensitive business related data (information) belonging to iQuda; or any business partner data (information) in the custodianship of iQuda?** | **Yes** q **No** q |
| **Will the Third Party have any *direct*, or *indirect* access to *any* personal data subject to the provisions of the Data Protection Act?** | **Yes** q **No** q |
| **3rd Party Name:**<br><br>**Sign:**<br><br>**Print**<br><br>**Date** | **iQuda:**<br><br>**Sign:**<br><br>**Print**<br><br>**Date** |