iQuda access control policy

Introduction

The purpose of this Policy is to establish and control User Access Management by imposing procedures, and governance to ensure the appropriate protection of iQuda's information assets and to ensure that information assets are handled, processed, stored, and communicated by systems and networks in a secure manner.

Scope

This Policy applies to all Employees, Contractors, Consultants, Temporary Staff, Third Parties, and other associates who have access to iQuda's information assets, and systems.

General Policy

All information assets being processed and communicated by iQuda's systems that have not been *specifically* identified as the property of other parties will be treated as though they are iQuda's assets. It is the Policy of iQuda to prohibit unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information assets. In addition, it is the Policy to protect information belonging to Third Parties that has been entrusted to iQuda.

Management Responsibilities

iQuda's Systems Administrators (Anthony Jones, Vincent de Beer and James Watson) (SA) are responsible for information assets and system security coordination. The incumbent individual(s) are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer.

Anthony Jones maintains a register of all current user access to respective elements of iQudas systems. Please refer to the QUAM iQuda User Access Management Spreadsheet. This document is kept on SharePoint.

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed by management. Logging facilities and log information shall be protected against tampering and unauthorized access.

Reporting of Suspicious Events:

Administrators and Staff are responsible for reporting all suspicious computer and network-security-related activities to the iQuda Systems Administrators as soon as is practicable.

iQuda System Administrator(s) also serve as the system information security liaisons, implementing the requirements of this, and other Information Systems Security Policies, Standards, Guidelines, and Procedures.

iQuda System Administrator(s) are responsible for ensuring that appropriate user management and access are exercised for management of computer and communication system security measures, to assure they are observed aligned to this and other Security Policies.

User Responsibilities

All iQuda users, and associates are responsible for complying with this and all other approved Policies defining Computer, and Network Security Measures.

System Access Control

Users must choose passwords which are difficult-to-guess. This means that passwords should not be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address should not be used. This also means passwords must not be a word found in the dictionary, or some other part of speech. For example, proper names, places, technical terms, and slang should not be used. Where such systems software facilities are available, users should be prevented from selecting easily-guessed passwords.

Users can choose easily-remembered passwords that are at the same time difficult for unauthorised parties to guess if they:

a) String several words together (the resulting passwords are also known as "passphrases")
b) Shift a word up, down, left or right one row on the keyboard
c) Shift characters by a certain number of letters up or down the alphabet
d) Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word
e) Combine punctuation or numbers with a regular word
f) Create acronyms from words in a song, a poem, or another known sequence of words
g) Combine a number of personal facts like birth dates and favourite colour

iQuda users should not construct passwords that are identical, or substantially similar to passwords they have previously employed. Where systems software facilities are available, users should be prevented from reusing previous passwords.

Users should not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users should not employ passwords like "P28MAR" in March, "P15JUNE" in June, etc.

Hard Coding:

Passwords should not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover them.

Passwords should not be written down and left in a place where they could be compromised by unauthorised person. Aside from initial password assignment and password reset situations, on occasions where there are suspicions that a password has been disclosed to, or accessed by authorised person(s), the password must be immediately changed.

Password System Set-Up

All computers permanently or intermittently connected to iQuda networks must have robust password access controls implemented. All multi-user systems must employ User-IDs and passwords unique to each user, as well as agreed, appropriate user privilege restriction mechanisms.
Computer and communication system access control must be achieved via passwords which are unique to each individual user. Access control to files, applications, databases, computers, networks, and other system resources via shared passwords (e.g. "group passwords") should be prohibited.
Wherever systems software permits, the display and on-screen printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorised parties will not be able to observe, or subsequently recover them.

Wherever systems software permits, the initial passwords issued to a new user by a System(s) Administrator must be valid only for the new user's first on-line session. At that time, the user must be forced to choose another password. This same process applies to the resetting of passwords in the event that a user forgets a password.

All vendor-supplied default passwords must be changed before any computer or communications system is used for iQuda business. This Policy applies to passwords associated with end-user User-IDs, as well as passwords associated with System(s) Administrator and other privileged User-IDs.
To prevent password guessing or Brute Force attacks, where systems software permits, the number of consecutive attempts to enter an incorrect password must be strictly limited. After, for example, three (3) unsuccessful attempts to enter a password, the involved User-ID should be either suspended until reset by a system administrator, or temporarily disabled for no less than say five (5) minutes. If dial-up or other external network connections are involved, the session should be disconnected.

Whenever it is known, or suspected that system security may have, or has been subject to compromise, the incumbent System Administrator(s) must immediately:

a) Reassign all relevant passwords
b) Force every password on the involved system to be changed at the time of the next log-in

If systems software does not provide the latter capability, a broadcast message should be sent to all users instructing them to change their passwords.

Whenever system security has been compromised, or even if there is a convincing reason to believe that it has been compromised, a trusted version of the operating system and all security-related software should be reloaded from trusted storage media such as CD-ROMs, magnetic tapes, or original source code. The involved system(s) should then be rebooted. Similarly, all changes to user privileges taking effect since the time of suspected system compromise should be immediately reviewed by the System(s) Administrator for unauthorised modifications.

Log-In/Log-Off Process

All users should be positively identified prior to being able to use any iQuda computer or communications system resource. Positive identification for internal iQuda environments involves both a User-ID and a fixed password, both of which are unique to an individual user.

Remote Access:

Positive identification for remote access, dial-up lines where possible should involve the use of hand-held tokens, cryptographic challenge/response, or other approved extended user authentication techniques. The combination of a User-ID and a fixed password does not provide sufficient security for remote access dial-up connections to iQuda information assets, systems and/or networks.

Modems attached to network-connected workstations situated within the iQuda estate should be forbidden as they do not provide adequate positive user identification. The same rules apply to any other form of communications, such as Wireless Protocols, including both 802.11x, and Bluetooth. Modems connected to isolated computers (such as portable computers and home computers) may be permissible so long as their anti-malware and security patches are-up-to-date with the most recently known release.
Positive identification for all users originating from external real-time connections to iQuda systems, networks, and assets via an external, off premise networks, public networks, or any other external communications system should also require extended user authentication techniques.

Where systems software permits, the log-in banner on multi-user computers should include a log-on notification which is aligned to the iQuda Acceptable Use Policy (AUP). This notification should state:

a) That the system is to be used only by authorised iQuda users
b) By continuing to use the iQuda system, the user agrees that he/she is an authorised user

The log-in process for network-connected iQuda computer systems must simply ask the user to log-in, providing prompts as required. Specific information about the organization, the computer operating system, the network configuration, or other internal matters should not be provided until such time the user has successfully provided both a valid User-ID and a valid password.

If there has been no activity on a computer system for a certain period of time, the system should automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period of time is (as deemed adequate by iQuda Security).

An exception to this policy could be applicable in cases where the immediate area surrounding a system is physically secured via secured-room badge readers, or similar technology (e.g. a Datacentre). With the exception of electronic bulletin boards or other systems where all regular users are anonymous, users are prohibited from logging into any iQuda system or network anonymously (for example, by using "Guest" User-IDs). If users employ systems facilities which allow them to change the active User-ID to gain certain privileges, they should have initially logged-in employing a User-ID that clearly indicates their identity.

Note 1:
On a UNIX system, this means that users must be prevented from initially logging-in as "root," but must instead first log-in employing their own user-ID. If such users have been granted the ability to achieve Superuser Privileges, they may then "set userid" ("su") to gain "root" access. Whatever the operating system, logs must record all such changes of current User-IDs.

External Access Controls

Any users initiating sessions via dial-up lines connected to iQuda networks/systems must pass through an additional access control point (Firewall/IDS/IPS) prior to users establishing connectivity. Unless approved in advance by the iQuda Systems Administrator(s), external connections that do not go through approved iQuda firewalls to connect to internal-network and systems are prohibited. This Policy applies to all inbound connections.

Remote maintenance ports for iQuda systems should be disabled until the specific time as they are needed by the vendor to perform an approved activity. These ports should then be again disabled immediately after use.

System Privileges

Limiting System Access: Computer and communications system privileges of all users, systems, and independently-operating programs (such as "agents") must be restricted based on the need-to-know, and need-to-access. This requires that privileges must not be extended unless a legitimate business-oriented need for such privileges exists which have been authorised by the iQuda System Administrator(s).

Default user file permissions should not automatically allow anyone on the system (e.g. on a UNIX system) to read, write, or execute a file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions should be prohibited. Nonetheless, default file permissions granted to limited groups of people who have a bona fide need-to-know and need-to-access may be supported.

On occasions where Users work away from the iQuda site, processing, storing, and communicating business information assets, they are responsible for administering a screen saver program securing access to their system(s), and should ensure their systems, and localized information assets are secure against compromise, manipulation, or loss.

iQuda systems should restrict access to other systems that users can reach over the enterprise network(s). These restrictions should be implemented and enforced via firewalls, routers, gateways, and other network components (e.g. IDS/IPS).

Privileged User Access and Management:

Where users are enrolled with access to Privileged Accounts (Administrator), on Unix or on Windows Systems (e.g. “root” on Unix), such privileged access should not be used for routine Business-as-Usual (BAU) activities like sending an e-mail, or originating a word document.
On such occasions Privileged users should either log out of their Administrator account, or utilize an account associated with an Ordinary User Profile; or in the case of UNIX, log out from “su”, again, to an account with reduced privileges.

Procedure

Process:

The following is the process to be adopted to assure that user privileges are current, and appropriate for all users with access to iQuda assets.

Table 1 – Allocation of System Accounts & Privileges

User Type	O/S	Privileges	RAS	Token	Review	Comment
Ordinary	Wintel	System Admin agreed	As required	As required	Every 12 months	Basic access aligned to JD
Admin	All	MD/System Admin Agreed	Yes	Yes	Every 3 months	Privileged Access aligned to Systems under JD

						(Local/Server) as required.
Power	Wintel	System Admin agreed	As required	As required	Every 6 months	Enhanced access aligned to JD
Contract and Temp	All	System Admin agreed	As required	As required	Every 3 months	Basic access aligned to JD & Contract
External Third Party	All	MD + System Admin agreed	Yes	Yes	Every 2 months	

Redeployment:
Upon any iQuda users being redeployed into new roles, it is important that their assigned privileges are revoked (*as necessary*) to assure that arrogation of user rights is not achieved, only supporting access to systems to which no *need-to-know*, or *need-to-access* exists. *This is of particular importance in relation to Privileged accounts.*

Table 2 - Revocation/Change of Rights

User Type	Leaver	Termination	Internal Move	LAN	RAS	Mobile Device
Ordinary	•			**Within 24 hours**	**Within 24 hours**	**Immediate**
Ordinary		•		**Within 8 hours**	**Immediate**	**Immediate**
Ordinary			•	**Within 48 hours**	**N/A**	**N/A**
Admin/root	•			**Within 8 hours**	**Immediate**	**Immediate**
Admin/root		•		**Immediate**	**Immediate**	**Immediate**
Admin/root			•	**Within 24 hours**	**N/A**	**N/A**
Contractor	•			**Within 24 hours**	**Immediate**	**N/A**
Contractor		•		**Within 8 hours**	**Immediate**	**N/A**
Contractor			•	**Within 48 hours**	**N/A**	**N/A**
Third Party	•			**Within 8 hours**	**Immediate**	**N/A**
Third Party		•		**Immediate**	**Immediate**	**N/A**
Third Party			•	**Within 8 hours**	**Within 8 hours**	**N/A**

Process for Granting System Privileges:
Requests for new User-IDs and changes to privileges should be applied for in writing, and approved by the System Administrator(s) prior to any changes being applied. In support of

accountability for events relating to escalation, or demotion of user privileges, all changes should be documented.

Individuals who are not iQuda employees should not be granted a User-ID or otherwise be given privileges to use iQuda assets unless the advance written approval the System Administrator(s) has first been granted.

All system privileges granted to users should be reevaluated against AD/LDAP *as applicable* by the relevant System Administrator(s) at six (6) month intervals to assure they are correct, and aligned to their iQuda user role. Where excessive, or incorrect privileges are identified they should promptly revoked. Again, such actions should be fully documented.

iQuda System Administrator(s) should assure that all user access, and privileges are maintained to reflect the *current* business access, and *need-to-know*, and *need-to-access*, and should promptly notify all significant changes in staff roles. For all terminations, the responsible Human Resources (HR) function at iQuda (process) should issue a notice of status change to the System Administrator(s) requesting immediate revocation of all user rights and systems access for *internal*, and *external* (remote access) privileges.

Special System Privileges:
Special system privileges-such as the default ability to write to the files any other user or system should be restricted to those directly responsible for systems administration and/or any other related systems security activity. On occasions, an exception to this policy can be made only with approval from the Manging Director – this must be documented for audit purpose.

Third Party Dial-In/Access:
Third Party vendors and associates should not be granted dial-up privileges to any iQuda system(s) or asset(s) unless the System Administrator(s) has agreed that such Third Parties have bona fide need, and that their access privileges are appropriate to the task in hand. Such privileges should be enabled only for the time period required to accomplish the approved tasks (such as remote maintenance).

If a perpetual, or long-term connection is required, then the connection should be established by approved iQuda authentication method(s) (hand-held tokens, software-based challenge/response process, etc.), along with audit, log, and accountability of usage. It is further required that such enabled extended Third Party access will be subject to periodic reviews, and will be terminated as soon as no longer required to support an operational task.

All users, (including third parties and associates) wishing to connect to iQuda's systems, assets, and the internal network(s) should sign a Compliance Statement prior to being issued a User-ID. If a nominated user already has a User-ID, a signature must be obtained prior to receiving a renewed User-ID. The latter process should be performed periodically.

Process for Revoking System Access

All User-IDs must automatically have the associated privileges revoked after a certain period of inactivity.

Fail Safe:

If a computer or communication system or asset access control subsystem is not functioning properly, it should default to denial-of-privileges to users. If access control subsystems are malfunctioning, the systems they support should remain unavailable until such time as the problem has been rectified.

Third Party Assurance

All Third Party Suppliers must be subject to a security inspection and service review by iQuda prior to the establishment of a contacted obligation, and thereafter at 12 month intervals, as required to assure their service meet the expectation of iQuda, and is, as far as it practicable, assured to be robust and secure.

Security Testing

Users should not security test, or attempt to compromise computer, communication, or system assets security measures unless specifically approved in advance and in writing by the iQuda System Administrator(s). Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, unapproved software copying, or similar unauthorised attempts to compromise security measures may be unlawful, and will be considered serious violations of iQuda policies.

Laptops and Portable Devices

Staff in possession of portables, laptop, notebook, palmtop, and other such transportable computers containing iQuda business information should not leave such assets unattended at any time in public places. Furthermore, where practicable, all such devices should employ encryption to protect the stored information from unauthorised access, and compromise. Please refer to the Q202 iQuda Portable Media Policy.

Security Tools and First Responder Forensic Capabilities

System assets, including computers and or communications systems should be provisioned with tools and applications to support iQuda System Administrator(s) to investigate events, and to verify a systems' security status. Tools should also be provided to support any Incident Responder Capability where erroneous or adverse user misuse has taken place, or is suspected to have taken place.

Note 2:

All such specialty, and potentially intrusive tools and applications can pose a security threat to network security, and thus the associated access rights and privileges should be only enabled for responsible, trained System Administrator(s).

Users must be put on notice about the specific acts that constitute computer and network security violations. Users must also be informed that such violations will be logged.

Incident Response:

To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information should be securely stored off-line until such time as it is determined that iQuda, in conjunction with any other function (Legal, or HR process) function, will not pursue legal action or otherwise use the information. The information to be immediately collected includes local and remote logs:

a) System logs
b) Application logs
c) Security Logs

To allow proper remedial action to be taken in a timely manner, records reflecting security relevant events should be periodically reviewed in a timely manner by the iQuda System Administrator(s).

Management of User Access

All access will be logged and controlled through the QUAM iQuda User Access Management Spreadsheet. Management of User Access Rights is controlled by the Service Delivery Director Vincent de Beer. All access rights will be reviewed at regular intervals, and may be revoked at any time under management discretion.

Exception Process

iQuda acknowledges that under rare circumstances, it may be necessary to enable systems, facilities, and operations which are not compliant with this, or other iQuda Security Policies. In these cases, they will be managed by the iQuda Exception Process. All such instances must be approved in writing and in advance by the MD, and System Administrator(s), and fully documented in the Exception Log.

Enforcement

The Executive Team will enforce this policy. 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 the organisations property (physical or intellectual) are suspected, iQuda 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.