iQuda acceptable use of assets policy

Introduction

This is the iQuda Ltd Acceptable Use Policy (AUP) and encompasses IT, Telecommunications equipment and services provided by iQuda Ltd, and applies to all user (including third parties, associates, temporary staff, and contractors) who have access to, and use iQuda Ltd assets, including, but not limited to:

- The network
- Personal computers (PC)
- Servers
- Laptops
- Internet connections
- Printers
- Telecommunications facilities (all forms)

All users of iQuda Ltd assets are required to comply with this policy and to be aware of the applicable associated Security Polices.

What is Unacceptable Use?

Unacceptable use is any act, or operation which is against iQuda Ltd Security Policies, which is considered to be detrimental to the stability, and security of its assets, and operations. iQuda Ltd users must not misuse system, assets, or upload, download, use, retain, distribute, create or access any electronic materials including emails, documents, images, text or software which:

- Might overload, damage, affect, or have adverse impact on the performance of systems, networks and/or external communications in any way
- May be a breach of copyright and/or licence provisions
- May be a breach of relevant law or legislation, including but not limited to the General Data Protection Regulations 2016 (the GDPR).
- Might gain access to restricted or unauthorised areas of the network, websites which the users is not authorised to access
- Partake in and activities which are considered to be hacking, unless this has been pre-authorized as a “network infiltration service” performed with the explicit consent of a iQuda Ltd client and our Managing Director, Anthony Jones.
- Initiating threats, slanderous, abusive, indecent, obscene, racist, illegal or offensive communications
- Communicating what may be considered Spam to other users of the iQuda Ltd Network; or any other remote users (not iQuda Ltd)

- Making unauthorised configuration changes to any iQuda Ltd asset. All changes must be requested via the QCRF iQuda Change Request form, and submitted to Information Security Manager Anthony Jones for review and approval.

Preventative Measures

iQuda Ltd automatically denies access to specific categories of websites that may impose a threat to their operational assets. This is achieved by firewalls, and other associated physical and logical security controls.

Management Responsibilities

iQuda Ltd denies any direct connection to their Network or equipment, or assets not supplied by the company. This includes, but is not limited to personally owned Thumb Drives, U3 Keys, PCs Laptops, IPods, IPads, Blackberries, PDA, Cameras, and Smart Cell Phones, unless previously authorized by a manager or iQuda Ltd's Managing Director.

Note 1: If there is a iQuda Ltd business reason for connecting a personally owned device to the Network, or other iQuda Ltd asset, an Exception must be sought from the System Administrator prior to such an attachment being made.

Personally Owned Software

iQuda Ltd users must not introduce, install or download any software from personally owned media, shares, or the internet with the intention of introducing it to iQuda Ltd assets. iQuda Ltd reserve the right to remove any personally owned, added software, or equipment from their assets. All installation requests must be requested via the QCRF iQuda Change Request form, and submitted to Information Security Manager Anthony Jones for review and approval.

Personally Owned Devices

Personally devices are not to be brought into the iQuda building, with the exception of personal mobile phones. Mobile devices may not be used for work purposes, except for access to email & for 2-factor authentication. If you wish to use your phone for workplace email, this must be requested and authorised by Anthony Jones. If your phone is misplaced or lost, you must make Anthony Jones aware immediately. If you access work email through your mobile phone, a secure screen lock with password must be enabled.

The General Data Protection Regulations 2016

iQuda Ltd adheres to the General Data Protection Regulations (2016). All users of iQuda Ltd IT assets, including information, must be adhere to the GDPR, and appropriate controls must be excursed around data assets which are classified as Personal under the Act. For further clarification on our approach, please refer to the QGDPR iQuda GDPR Policy.