iQuda password policy

Overview

Passwords are the key to any network. Just one insecure password could enable anyone to log on to iQuda's network. Bad passwords are just as bad as no passwords at all. Passwords traverse networks on an almost constant basis, and all it takes is a well-placed eavesdropping program to gather most passwords in a matter of minutes.

All Internet related equipment, including but not limited to computer equipment, software, storage media, electronic mail, and Internet connections remain the property of iQuda. These systems are to be used for business purposes and in the course of normal daily operations. It is in iQuda's best interest to make sure that these resources are protected and used appropriately. Where appropriate it is in iQuda's best interest that access is restricted to those individuals whose job function relies upon access. Where possible, access is restricted only to the relevant persons.

Purpose

The purpose of this policy is to outline the password policy at iQuda. These rules are in place to protect the user, our clients and iQuda as a whole. Inappropriate use exposes iQuda to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, visitors, contractors, consultants, temporaries and other workers at iQuda, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by iQuda. This policy applies to all equipment that has access to iQuda's network either locally or via remote connections.

Policy

Every individual should have a unique logon ID and a strong password associated with each logon ID. This is so that any action on the network can be attributed to an individual and appropriate resources can be made available to the individual. There will be very exceptional circumstances where a group shares a logon ID (please see the section on group passwords). Each person should have a strong password in order to keep unauthorised users from guessing their password and accessing the network in their name.

A strong password will follow these guidelines:

- Passwords should not be easily guessable or be found in a dictionary.
- Use a nonsensical combination of letters: The best passwords will be nonsensical. For example, if you use a memorable phrase such as a statement e.g. "Daisy is my favourite pet dog in the world", the result could produce: "dimfpditw". This is a good

Classification: PUBLIC. iQuda Password Policy. Ref: Q204.
Version Number: 6. Approved by: Anthony Jones. Created by: Garth Macintosh.
Date created: 01.09.2015. Date of this version: 12.06.2019. Date of next review: 08.05.2020.

password (and the phrase is easy is remember), but see the next bullet to make it even more difficult.

- Include a mix of UPPER and lower case letters: You should include an uppercase letter somewhere other than at the beginning. The result could produce: “DiMFPDitw”
- Include numbers and/or special characters such as!”£$%^&*()_+@’: Because the letter l looks like a number one, you could use a one instead of that letter. Because the special characters ^^ look like the letter M, you could use that instead. Your password then becomes: D1^^FPD17w.
- Numbers and special characters are best used towards the beginning of the password.
- Longer passwords are better: Your password **must** be at least 8 characters in length but the longer it is, the better.
- Your line of business application passwords **will be** changed automatically every 365 days.
- You are required to update any other passwords at least every 365 days.
- Your password **must** be new; you can’t reuse old ones.
- Don’t use a set of characters straight off the keyboard: You should never use qwerty, 12345678, or asdfghj for passwords. Even though they look nonsensical, they follow a distinct pattern of consecutive keys on the keyboard and password crackers will break them in seconds.
- **Treat your passwords as top secret information**: All passwords should be protected and not shared! If they must be written down (and this is only in very exceptional circumstances) they must be locked away.
- **Never** let anyone know your password (including system administrators). A system administrator can reset your password if work needs to be done on your account.
- **Password hints should not be used.**
- **If you accidentally share your password with anyone else, you should notify your line manager immediately.**

Password Changes

iQuda operates a self-service password reset service. This tool allows users to change their Active Director password without requiring authorisation from a manager. For more information, please speak to the Service Delivery Director Vincent de Beer.

2-Factor Authentication

iQuda uses 2-factor authentication for line of business applications. 2-factor authentication (2FA) adds an additional layer of authentication to the logon process by generating a unique code via an application, call or text message that must be used in conjuction with a password in order to gain access to our systems. Without the code **and** your password, you will not be able to logon to iQuda line of business applications. **All staff are required to use 2-factor authentication.** The technical department will assist with the setup of your 2-factor authentication on your personal or work mobile phone. It is because of 2-factor authentication that we have extended our password change frequency from 60 days to 365 days.

Group Passwords

In very exceptional cases a group of users will share a logon ID and password. In these cases iQuda will set and change the password (based on the guidelines above). A nominated list of individuals will be informed of the new password. It will be the responsibility of the nominated individuals to inform authorised members of the group of any password changes. These passwords must still be treated as top secret.

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 a breach of policy leads to an incident that has the potential to affect the rights and freedoms of individuals, the Data Protection Officer may report the incident to the Information Commissioners Office (ICO). This will take place if the breach is in violation of the General Data Protection Regulations 2016 (the GDPR).

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.