BC|MQI
BC Medical Quality Initiative

Password Security and Confidentiality in AppCentral
Tips and best practices

Your account security

BC MQI is committed to keeping your information private and secure. However, you play an important role in maintaining the security of your AppCentral/CACTUS account.

Keeping your password secure and confidential

1. The first key is to create a strong password.

   New passwords in AppCentral must meet these requirements:

   - Be 10-15 characters long
   - Have at least one number and one letter
   - Have at least one special character (except the <)

   And also be sure to avoid passwords that are easy to guess.

   - Don't use your user name, your real name, family names, birthdays, pet names, house or phone numbers, or common words like "password."

2. To maintain a secure account, be sure to keep your password confidential.

Best practices to keep your password confidential:

1. **Do not re-use previous passwords.**
   - **Ideally, create unique passwords for each health authority application and each system log in.**
2. **Never share your password with anyone.**
   - **This includes administrative support staff, co-workers, colleagues or others in the workplace.**
3. **Do not write your password down or store it electronically on your computer.**

Act quickly if your password confidentiality is compromised.

Reset it immediately through the process within AppCentral, or contact medical affairs for assistance.

Need to reset your password? Learn how in the AppCentral Practitioners User Guide.

*A note on mobile devices

Please note that AppCentral and other CACTUS modules (such as iCommittee) are not supported for use on mobile devices, such as smartphones and tablet computers or iPads.