Cyber Access and Security Control Policy

Applicable to	Users
Person responsible	Communications Officer

1. PURPOSE

This policy:

- Establishes guidelines for managing access to the RBCAA's controlled cyber resources.
- Aims to ensure adequate cybersecurity for the RBCAA.

2. SCOPE

This policy applies to all users of RBCAA's controlled cyber resources.

3. CYBER ACCESS

3.1. Use Accounts

- Creating admin user accounts on the RBCAA network requires approval from the Communications Officer.
- RBCAA's IT Service Provider manages user accounts, maintaining audit records for processed and denied requests.
- Admin accounts must be unique and traceable; group accounts are not allowed unless approved by Directors.
- Users receive minimum access based on the principle of least privilege.
- Inactive accounts may be deactivated after 30 days.
- Temporary accounts must have an expiration date approved by the Communications Officer and implemented by the IT Service Provider.
- Individuals must not share account access information.
- The IT Service Provider will immediately cancel account access for users whose relationship with RBCAA has concluded.

3.2. Passwords

- Password resets require identity verification per the IT Service Provider.
- Passwords must be at least eight characters with a mix of upper and lower case, numbers, and special characters.
- Automatic login software is restricted, except with specific approval for tasks like automated backups.
- Remote access points follow identification and authentication technologies for security.

Cyber Access and Security Control Policy

4. CYBER SECURITY

All computers that access the RBCAA cyber resources, excluding the station PC dataloggers, must have the following standard software installed:

- Anti-virus, anti-exploit, and anti-ransomware software (Malwarebytes);
- Communication protection software (Mimecast), and
- Anti-spoofing software (Sendmarc).

The IT service provider is responsible for ensuring the above software is up-to-date and functioning correctly. Users must not attempt to resolve cybersecurity issues themselves; if a problem is detected, users must disconnect from the RBCAA network, stop using the infected resource immediately and notify the IT service provider.

The following must also be implemented:

- Security awareness training;
- Daily backups of all Microsoft 365 accounts;
- Dark web monitoring of the rbcaa.org.za and rbcaa.co.za domains;
- Monthly verification of DMARC compliance for both domains.
- Active monitoring of the RBCAA server Microsoft 365 environment, and personal computers by the IT Service Providers' Security Operations Centre

Sandy Camminga

RBCAA MANCO Chairperson /
Communications Officer

Candice Webb

RBCAA Managing Director

Richards Bay, 2025-08-21