Cyber Access and Security Control Policy

The Richards Bay Clean Air Association (RBCAA) protects the confidentiality, integrity, and availability of its information, air-quality monitoring data, systems, and technology resources.

This policy establishes the principles and responsibilities governing and controlling cybersecurity and access risks.

It applies to all MANCO members and to the service providers authorised to access RBCAA systems (the Project Management Service Provider and the IT Service Provider), and to all information and technology resources owned, operated, managed or used on behalf of the RBCAA, including cloud services, computers, servers, networks, mobile devices, and monitoring-station computers and dataloggers.

1. CYBER ACCESS

1.1. User 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.

1.2. Passwords

- Password resets require identity verification per the IT Service Provider.
- Passwords must be at least eight characters with a mix of uppercase and lowercase letters, 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

2. 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).

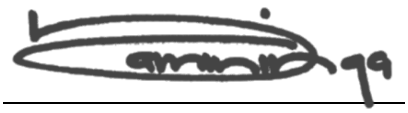
The IT Service Provider is responsible for ensuring that the above software is up to date and functioning correctly. Users must not attempt to resolve cybersecurity issues themselves; if a problem is detected, users must disconnect from the RBCAA network, stop using the infected resource immediately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

The following controls are also implemented and maintained:

- 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; and
- Active monitoring of the RBCAA server Microsoft 365 environment and personal computers by the IT Service Provider's Security Operations Centre.

Although ultimate responsibility for cyber access and security resides with the Directorate, MANCO members and service providers with access to RBCAA systems are responsible within their work areas for helping ensure that cyber access and security are embedded throughout the organisation.

This policy is communicated to MANCO members and to the service providers with access to RBCAA systems so that it is understood and applied in their work, is made available to members, stakeholders, and the public, and is reviewed at management review for continuing suitability.



Sandy Camminga

RBCAA MANCO Chairperson



Candice Webb

RBCAA Managing Director

Approved and effective from: 2026-10-23