2

Site Security

- ACCESSING YOUR SITE
- SECURITY GUIDELINES

Section 2 Contents

Accessing your Site

To access your Corporate Republic*Online* site you will need the following:

Username

You can set your own username at registration. Your username is not case sensitive, but it must be unique and alphanumeric (i.e. comprise letters and/or numbers). Special characters (e.g. @ _ “) are not permitted.

Password

You will set your password during your first login process. *(See Section 2 - Site Security, pg. 20 for Password Guidelines)*

Security image

- At your first login to your Corporate Republic*Online* site, you must select one security image from the options provided.
- The image will be used as an anti-phishing device. Thereafter, each time you log on to your Corporate Republic*Online* site, the selected image will be displayed. This helps you to differentiate between your authentic Corporate Republic*Online* site and a phishing site.

Accessing your Site

Second authentication method device

As a user you must register a mobile device, which will be used for authentication when logging on.

You will be required to select your preferred channel from the following options:

Option 1. SMS

If this option is selected, each time an attempt is made to access the application, a unique SMS code will be generated and sent to your registered mobile number. You will then be prompted to enter the unique SMS code.

Option 2. Republic*Mobile* App

The Republic*Mobile* App offers you 2 options:

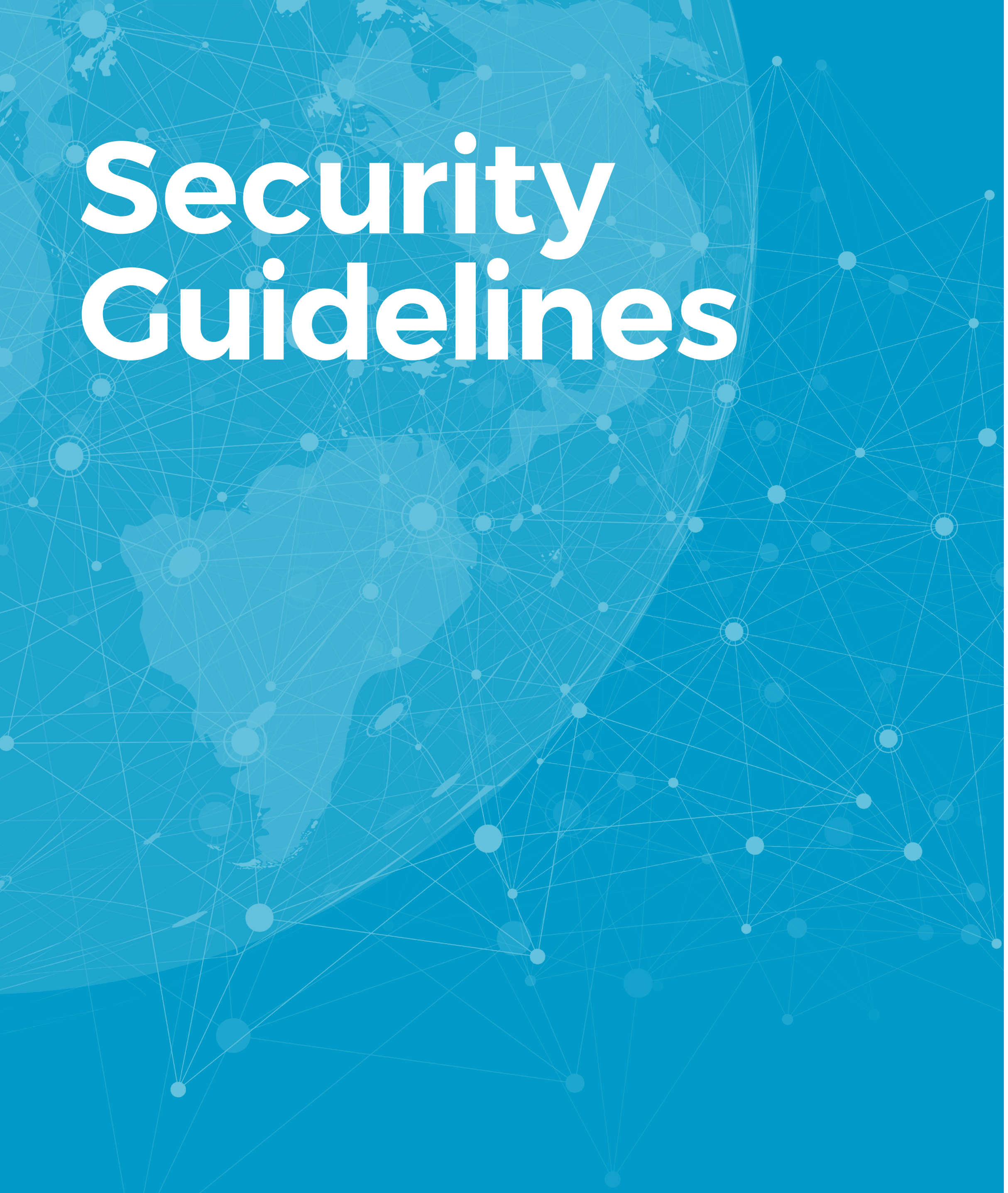
Selecting OTP (One Time Password)

Each time you log on to your Corporate Republic*Online* corporate site, an OTP will be generated by the Republic*Mobile* App. That OTP must be entered at login.

Selecting SYNC

When you attempt to log on to your Corporate Republic*Online* site, the system will attempt to connect or sync with your registered mobile device. You will then be required to either ACCEPT or REJECT this connection, before proceeding.

All security features are set up at your first login except for your username which is set up during registration.



Security Guidelines

Security Restrictions

The following constraints have been deliberately imposed in the application to enhance the security and integrity of the system and the transactions conducted online:

Session timeout duration

To enhance security, the system is equipped with a session timeout feature which enables the application to log off after 20 minutes of inactivity on the web and 5 minutes of inactivity on the Mobile App. The system will advise that the session has expired and prompt you to log in again.

Unique session control

The system will only allow you to access one session at a time. In instances where you attempt to log in to the system and there is already an active session using the same credentials, a warning message will appear advising that you must cancel one of the active sessions before proceeding.

Password Guidelines

Consider the following guidelines when creating your Corporate Republic*Online* password:

- Use a **minimum of 8** and a **maximum of 12** characters.
- Include at least **1 capital letter** and **1 number**.
- **Spaces** and other **special characters** are **not allowed** in the password.
- **Avoid using names** of pets, parents or friends and relatives for your passwords.
- Refrain from using passwords **containing all the characters in your login ID**. For example, if your login ID is ‘jSmith’, then your password should not be ‘jSmithOne’.
- The password fields will **not allow any information to be copied from the clipboard**.
- **Change your password** at regular intervals.
- **Avoid the use of the ‘saved password’** feature offered by any mailing application or software.
- Ensure you **always log out** of the application, terminating transactions and all possible activities.

Second Authentication Method Device Guidelines

Use the following guidelines for the second authentication method device:

- The **device selected** should belong to one of your company's **Corporate Republic*Online* site users**.
- **Avoid leaving the device unattended**.
- Always ensure that you use the **screen lock** option.
- **Connect to secure WIFI** to conduct internet banking transactions, as public WIFI hotspots may be susceptible to hackers.
- Keep your device's **operating system up-to-date**, to ensure you have the most secure and efficient experience.