CommBiz User Guide

Keeping your business secure

CommBiz combines the convenience of internet banking with state-of-the-art security features to keep your business and your financial information safe.

This guide describes how the security features of **Comm**Biz protect you, and sets out some additional steps you can take to protect yourself.

How we protect you	
Login security for users	Everyone who logs on to **Comm**Biz is authenticated by a unique login ID and password. Each password must be between eight and 16 characters in length and must be different to the last five passwords chosen by the same user.
Security tokens for authorisers and administrators	Users with the permissions required to authorise transactions or administer your **Comm**Biz Service must also enter a second password, generated by a personal electronic security token. The token updates the password every 32 seconds, and each password can only be used once. If you wish, you can set up **Comm**Biz so that all users need security tokens. If you use the Express Registration method, by default all users will have administrator permissions and, as a result, will automatically receive security tokens.
Netlock device	NetLock is designed to be used along with existing **Comm**Biz tokens to give extra protection against even the most sophisticated security threats. The NetLock USB security device provides access to **Comm**Biz through a secured Mozilla Firefox internet browser. It also uses an encrypted digital certificate (like a long mathematical algorithm) to authenticate the internet connection to **Comm**Biz which considerably reduces the risks of known internet threats.
Encryption	When you log on to **Comm**Biz, all of the data sent to and from your computer is encrypted using industry-standard 128-bit Secure Socket Layer (SSL) encryption technology.
User roles	You can use **Comm**Biz to create different user Roles for different people within your business. For each Role, you can determine: • which accounts users can view; • which transactions they can create, if any; • which transactions they can authorise, if any; and • whether they can administer your **Comm**Biz account. For example, you could create a role for an accounts payable clerk with the permission to authorise direct credits of up to $1,000.
User permissions	As well as user roles, you can set personalised permissions for individual users.
Authority to operate	As an added security measure, your **Comm**Biz administrator can only create user roles and permissions that are consistent with the signed Electronic Account Authority you have lodged with the Bank. The authority sets out who can authorise transactions and how many authorisers are required for each account.

Commonwealth Bank

Automatic timeout	When a user logs into **Comm**Biz, their session has an automatic inactivity time limit of 15 minutes. If you are logged in for 15 minutes without doing anything, your **Comm**Biz session will be locked until you re-enter your login ID and password. When you do so, you will be immediately returned to the **Comm**Biz page that you were on when your session timed out.
Lockout	To protect against unauthorised users trying to guess a password, a user's account will be locked after a number of unsuccessful attempts to log on. A locked account can be unlocked by an administrator.
Auditing and activity tracking	Every action a user takes in **Comm**Biz is recorded with a date and time stamp, so your **Comm**Biz administrator can view and print detailed audit reports, including audit logs for individual users.
Independent audits	**Comm**Biz is regularly reviewed by independent security experts to guarantee the integrity of our system architecture, firewall configuration, network device security, web server security and web application security.

How you can protect yourself

Keep your CommBiz service secure	• Always include two or more Electronic Account Authorities (authorisers) on every account linked to your **Comm**Biz service. • Regularly review the Electronic Account Authorities (authorisers) to ensure they are valid and up-to-date. • Regularly review the users that have access to your **Comm**Biz service. Also check that users have the correct permissions assigned to view, create and authorise transactions. • If people leave the business or go on extended leave, suspend or delete their access to ensure only authorised users access your service. • Limit the days and times that users can access your service to ensure users access **Comm**Biz only when they are supposed to. • Regularly change your password.
Keep your computer secure	• Install a firewall and ensure that it stays up to date. • Install the latest security updates for software, especially your operating system and internet browser. • Install an internet security and anti-spyware program and keep your virus definitions up-to-date. If you do not already have an internet security program, **Comm**Biz offers all users 6-months free McAfee anti-virus protection.
Avoid security risks	• Keep your login details, security token and NetLock device secure at all times. • Avoid opening emails that ask for details of your accounts or your **Comm**Biz service. Never reply to these emails or open hyperlinks within the email. • Avoid opening, installing or using programs or files from an organisation you do not know you can trust. Be particularly careful of unsolicited emails and attachments. • Don't leave your computer unattended while your **Comm**Biz session is still active. • Always log off when you have finished your **Comm**Biz session. • Do not access suspicious screens and pop up notifications.
Monitor your account	• Watch for any unusual or unauthorised account activity, and call the **Comm**Biz help desk on **13 23 39** immediately if you notice anything suspicious.