IT'S HOW
WE CONNECT

SECURITY
FOR YOUR SYSTEM

As a rule, business communication tools need to be protected from potential security breaches, and your new Private Automated Branch Exchange (PABX) system and voicemail solutions are no exception.

If your PABX equipment isn't properly configured and maintained, you leave your business vulnerable to fraudulent activity from outsiders who could make unauthorised calls to domestic or international numbers, or hack into your confidential voicemail messages. As the responsible account holder, you'd face significant costs in phone charges and potentially other losses if this happened.

The following security tips are a guide to the preventative actions you should consider including in a regular security audit of your PABX system.

SECURITY AUDIT ESSENTIALS

1. General Checks
- Read the product manual to understand all of your system's features and how to use them securely.
- Conduct regular security audits of all your voicemail, telephone and PABX system.

2. Call Usage
- Check your account regularly – looking for outbound call records to unusual destinations and calls made at unusual times.
- Don't wait for your Telstra bill to check calls and costs – sign up for Online Billing so you can access your call records when it suits you.

3. Voicemail and call queuing platforms
- Make sure every user who has access to your PABX system changes their PIN and passwords regularly.
- Cancel any old or unused mailbox accounts.
- Disable access to international and/or 19XX numbers unless they're critical for your business needs.
- Never publish the remote access numbers to your voicemail system.
- Use firewall rules to block all undesirable internet activity and close unused IP ports on Voice over IP (VoIP) systems and internet connections.

4. PABX Security
- Make sure access to your phone or PABX system is strictly limited, controlled and secured.
- Prepare a contingency plan and be ready to put it into action when a security breach incident occurs.
- Never publish the remote access numbers to your PABX system.
- After your new PABX system is installed, immediately change the master password from the installed default.
- Make sure your PABX system password doesn't reset to the default if there is a system or power outage.

5. PIN/Password Security
- Treat phone PINs as seriously as any other financial or computer access code.
- Ban employees from using easy-to-guess PIN numbers (eg postcodes, date of birth, extension, repeating or sequential numbers).
- Make sure all PIN and passwords are kept secure, not written anywhere, and are changed regularly.
- Always use a mixture of alpha and numeric characters for passwords.
- Set a minimum length of six characters and fix a maximum length.

Please note: this list is not a substitute for independent legal and professional advice.

You should also seek tailored input from your equipment's manufacturer or another suitably qualified expert.

CALL TBS HELPDESK 1800 022 218
OR SEND AN EMAIL TO
ucdfrontline@team.telstra.com