COGECO | BUSINESS

PBX Security Guidelines for SIP Trunking Customers

Learn how to maximize the security of your advanced phone system. Protect your business from negligent mistakes and help prevent unauthorized access by following these guidelines.

Remote access

Remote access logs

→ A comprehensive log should be kept to ensure that all remote access users are identified.

→ These logs should include an audit trail to identify who has accessed the PBX, including the time, date, user identification and, if possible, event logs (transactions that occurred).

→ Although it is not necessary to review these logs on a daily basis, they should be reviewed periodically. This log becomes especially important when investigating unusual activity.

→ Consider who accesses your PBX remotely (for example, vendors, administrators or technical support within the organization).

Authentication methods

→ Authentication devices such as smart cards or other token authentication devices provide an additional layer of security.

Posting remote access information

→ Remote access telephone numbers, login procedures and passwords should never be posted or published.

Repeated login attempts

→ The PBX should terminate the call after 3 unsuccessful login attempts to deter unauthorized users.

Managing DISA access

→ If Direct Inward System Access (DISA) is used to access the PBX, the access code or password should be kept confidential, changed often and deleted immediately if no longer required. We also recommend using the maximum number of characters (10-15 if possible).

Toll restriction

Calling patterns

→ It's important to determine the calling pattern within the organization. For example, is international calling required for everyone, or only for a select few?

→ A Call Detail Recorder (CDR) device will give a current view of toll calling patterns and help determine if restrictions are needed and if they are working when activated.

Toll-free numbers

→ If your business makes use of toll-free numbers (such as 1-800, 1-866, 1-877 or 1-888), we recommend blocking all unnecessary area codes and country codes if possible to prevent fraudulent calls.

Activating toll restrictions

→ Block all unnecessary country codes and other appropriate NNXs, as well as 1-900, where appropriate.

Voicemail systems

Password security

→ Passwords or PINs should be a minimum of 6 characters (this can be set in the system). It is best to use the maximum number of characters.

→ Passwords should not be easy to guess, and should never be posted or shared. Don't use common number schemes such as the location of the telephone or the 7-digit telephone number. Software packages that test for common passwords should be used when possible.

→ When activating a new subscriber, passwords should be randomly generated and should never be set to the location of the telephone.

→ Software should be utilized to prompt employees to change their passwords at a minimum of every 90 days (every 30 days is preferable). If the software is not available, then policies should be in place that inform all employees about the importance of frequently changing their passwords.

Port activity reports

→ Ports in the voicemail system should be monitored through activity reports to ensure unauthorized access has not occurred. This will determine if there have been unauthorized attempts trying to get into the voicemail system, as well as toll abuse.

Shared mailboxes

→ Shared or group mailboxes should have an individual assigned to manage them, including removing messages and ensuring that the greeting has not been changed.

Through-dialing

- → If the capability of through-dialing is not necessary, this feature should be disabled, as a significant amount of fraud occurs when using this feature within the voicemail system.
- → If the feature must be used, daily reports for through-dialing should be monitored, especially after hours.
- → Typical outgoing trunk access codes should not be used, such as 9, 8, 9+0, 9+1, 9+011, 9+1-800/866/877/888.

Unassigned mailboxes

- → All mailboxes that are empty or unassigned should be removed. Vacant mailboxes can be used for fraudulent purposes.

Access codes

Access code selection

- → All access codes used should be randomly selected and not in sequential order, so they are not easily guessed. A minimum of 6 characters should be used for access codes or passwords, whenever possible.

Dormant access codes

- → Deactivate codes in the system not being used by current employees.

Call forwarding

Call forwarding restrictions

- → Call forwarding should be restricted to 4 digits when possible, to prevent forwarding to an external number. This prevents toll abuse through the call forwarding feature.

Telephone room

Hardware security

- → To protect the PBX hardware and its peripheral devices, the telephone room or equipment room should be locked and have an audit trail logging who has accessed it.
- → Card access devices that have your employees scan a card to gain access to the room can accomplish this.

Additional resources

If you have any questions about toll fraud or PBX security, our experts are here to assist you and answer any questions that you may have at **1-866-264-3262**.