To enhance the VoIP Security for installed telecom equipment, we must take care of the following check points:

- The system should have the latest firmware, as the latest firmware have upgraded security settings.

- System Engineer (SE), System Administrator (SA) and Front Desk User Password should be strong and must follow the below mentioned password policy and should be different for all configured IP extensions.

  ❖ **Password Policy:**
  
  - Character length of the password must be 6 characters or more.
  - Password must include at-least 1 uppercase, 1 lowercase, 1 number and 1 special character.
  - Allowed characters are 0-9, a-z, A-Z, all special characters except %, =, #, +, \, <, >, " , ' and space.

  - System Engineer (SE), System Administrator (SA) Login Password for phones should be changed from its default value.

  - Trusted IP Addresses must be configured in Security Settings page to allow the WEB GUI access and IP Phone Registration from Trusted IP Addresses only.

- HTTP and HTTPS ports should not be forwarded for the system to restrict access of the system from public network.

- While using IP Phones/ Trunks, TLS and SRTP settings should be configured to encrypt the data.
- The SIP TCP/ TLS/ RTP ports should be changed from their default values.

- Trusted IP addresses and Digest Authentication should be configured for peer to peer SIP Trunks.

- International dialing should be disabled, if the customer is not using it. If you are dialing international numbers, PIN dialing feature should be used. (Do not share the PIN to other users)

- Refer the below link for configuration of PIN dialing:
- Use Generate Password feature (for SARVAM UCS and PRASAR UCS).

- Check Enable Device Flag for unused locations to restrict the SIP Extension Registration on these locations.
**Disclaimer:** The information contained in this document may contain confidential or privileged information. Unauthorized use, disclosure or copying is strictly prohibited and may constitute unlawful act and can possibly attract legal action, civil and/or criminal. The contents of this document need not necessarily reflect or endorse the views of Matrix Comsec on any subject matter. Any action taken on or omitted in this document is entirely at your risk and the originator of this document or Matrix Comsec does not take any responsibility or liability towards the same. If you are not the intended recipient, please notify us immediately and permanently delete the document.