



Customer Detail			
Customer		Client Contact Number	
Full Service Address		Client Contact E-Mail	
Client Contact Name		Installation Auditor	
Contact Job Title		Installation Date	
Installation Date			

IP PBX INSTALLATION PREREQUISITES					
Rack Mount Implementation Requirements	Requirements Met (Y/N)	If no, specify planned compliance date	Comments	Compliance Verification Date	Verified By Installer Staff
Maximum temperature is 30 degrees, internal temperature should be considered. Do not restrict airflow.					
Rack needs to be stable					
Sufficient cabinet space					
Surge protection / UPS, Power Surge Plug Protector					
Earthing Requirements		Proper earthing installed (Y/N)	If no, specify earthing installation date	Compliance Verification Date	Verified by (Installer Staff)
Ensure that Com.X and rack is earthed to an earthing bar. (Insufficient earthing of the IP PBX may add noise to the audio path that may reduce performance. Proper earth with < 0.5 ohm measured from the Com.X stud to the earthing bar. An earth bar should be present prior to installation.) <i>Please note that Far South Networks cannot be held liable for problems arising from failure to provide adequate earthing.</i>					
		Comments			



IP PBX LOCKDOWN AND RELATED SECURITY		
Security Checks	Requirement Met (Y/N/NA)	Comments
IP PBX and General VoIP Security		
Access to the unit is restricted to authorised personnel		
Default Comma/FreePBX/Root/SSH passwords have been changed		
Strong passwords are used and have been verified using the FreePBX Weak Password Detection module		
Enabled Fail2Ban features (Asterisk Jail) so that logging is enabled to check for unauthorised activity: <code>/var/log/asterisk/*</code> AND <code>/var/log/syslog*</code>		
Enabled Fail2Ban features so that PBX console messages are logged to <code>/var/log/asterisk/messages</code> for periodic monitoring as a large number of rejected VoIP registrations may indicate an attack on the system.		
Available tools have been used to check if the system allows to anyone make calls without authentication.		
Com.X and IP telephone firmware has been updated to the latest stable version		
Unused modules have been disabled to reduce surface attacks. Unneeded protocols (e.g. IAX2, H323) are also disabled. (<i>Proceed with caution!</i>)		
All VoIP extensions have strong passwords (Extension numbers have not been used as passwords)		
Network security		
Remote access to the Com.X is allowed (where necessary) via VPN only		
The Com.X and IP phones are on a separate network partition of a managed switch, or on a completely separate physical network		
The Com.X is behind a firewall or appropriate firewall rules have been configured in iptables		
Port forwarding is performed on a non-standard port to port 22 on the Com.X for SSH access. HTTP access is tunneled through the SSH connection.		
Administrator access is limited to a whitelist of IP addresses.		
Fail2ban features have been activated to ban the IP address of anyone who tries to get into the Com.X system without providing correct credentials for <i>n</i> number of times		
Firewall is configured to block all incoming VoIP traffic except that from a white-list of remote extensions.		



Other		
Feature codes have been disabled for unused administrative features, and the default feature codes have been changed for access to features that are enabled. (Feature E.g. ChanSpy, ZapBarge).		
Where direct database access is configured for CDR access, the access has been limited to a white list of MAC addresses, IP addresses or networks.		
Client has been advised to use pins and pin sets on international and other high-cost outbound routes.		
Client has been advised that all users should set their voicemail pin and user portal login passwords to something other than the default.		
The system configuration and other important data has been backed up		

DOCUMENT CONTROL			
CUSTOMER SIGNATURE: Upon acceptance of requirements and information as documented.		DATE:	
ENGINEER SIGN OFF: Sign and handover to project manager once installation and configuration has been completed.		DATE:	