Managed UC

Security Domain	Zayo	Customer	Notes
Logical Security, Access, Change Control, Network Protection			
Authentication to VoIP/SIP portals	X	X	Zayo secures provider and UC portals; Customer secures admin credentials.
Access control to customer environment (SBC, IP phones, SIP endpoints)	—	X	
Network security for SIP infrastructure	X	—	Zayo provides DDoS protection, SBC protection (if hosted).
Customer firewall and NAT configuration	—	X	Common failure point; must be documented as CUEC.
Monitoring for fraud / anomalous call patterns	Shared	Shared	Customer must react to alerts.
Patch management of provider systems	X	—	Zayo manages UC platform and SIP endpoints
Patch management of firewall	X	—	Customer ensures firewall is updated as necessary
Uptime, redundancy, resilience, incident response			
UC platform uptime, HA, redundancy	X	—	
Provider-side monitoring (SIP, RTP paths)	X	—	Zayo alerts Customer of outages.
Customer LAN/WAN availability/QoS	—	X	Critical for VoIP.
Disaster recovery of provider platform	X	—	
Accurate call routing, complete CDRs, functioning SIP signaling			
Correct and complete setup of DIDs, SIP routing	X	X (validates)	Zayo provisions; Customer ensures correct mapping of lines.
Number porting accuracy	X	X	Customer provides LOA; Zayo executes port.
Call routing integrity	X	X	Zayo ensures accurate external routing; Customer handles internal dial plans.
CDR (Call Detail Record) accuracy	X	—	Zayo must ensure billing correctness.
Call encryption, data protection, secure transmission			
Encryption in transit (TLS/SRTP if offered)	X (provides)	—	
Protection of CDRs/customer metadata	X	—	
Voicemail and call recording retention & encryption	X	—	
Endpoint (IP phones, softphones) confidentiality	—	X	
Handling customer personal information (names, DIDs, recordings, caller ID)			
Handling of personal data in CDRs	X	—	
Customer consent and notification for call recording	—	X	Customer must meet jurisdictional laws.
Retention/Deletion of PII in provider systems	X	—	
Caller ID masking or privacy features	X	X (requests/configures)	Shared responsibility.
Incident Response			
UC platform incident detection & response	X	—	
Endpoint compromises (e.g., toll fraud)	X	—	
Fraud alerts and escalation	Shared	Shared	Both parties must collaborate
Coordinated investigation for call failures	Shared	Shared	Both parties must collaborate
E911 issues	Shared	Shared	Zayo provides routing; Customer maintains location accuracy.

SIP Trunking

Security Domain	Zayo	Customer	Notes
Logical Security, Access, Change Control, Network Protection			
Authentication to VoIP/SIP portals	X	X	Zayo secures provider portals; Customer secures PBX/admin portals.
SIP trunk authentication (IP allowlists, credentials, TLS/SRTP if supported)	X (platform)	X (implement on PBX/SBC)	Shared when TLS/SRTP is used.
Access control to customer environment (PBX, SBC, IP phones)	—	X	
Network security for SIP infrastructure	X	—	Zayo provides DDoS protection, SBC protection (if hosted).
Customer firewall and NAT configuration	—	X	Common failure point; must be documented as CUEC.
Monitoring for fraud / anomalous call patterns	Shared	Shared	Customer must react to alerts.
Patch management of provider systems	X	—	
Patch management of PBX, phones, SBC	—	X	Customer secures endpoints and PBX.
Uptime, redundancy, resilience, incident response			
SIP trunk platform uptime, HA, redundancy	X	—	
Provider-side monitoring (SIP, RTP paths)	X	—	Zayo alerts Customer of outages.
Customer LAN/WAN availability/QoS	—	X	Critical for VoIP.
PBX uptime, system resilience	—	X	Customer responsible for PBX power, server HA, UPS, etc.
Disaster recovery of provider platform	X	—	
Customer DR for PBX / call routing	—	X	Customer responsible for failover PBX or alternate routing.
Accurate call routing, complete CDRs, functioning SIP signaling			
Correct and complete setup of DIDs, SIP routing	X	X (validates)	Zayo provisions; Customer ensures correct mapping on PBX.
Number porting accuracy	X	X	Customer provides LOA; Zayo executes port.
Call routing integrity	X	X	Zayo ensures accurate external routing; Customer handles internal dial plans.
Codec selection and compatibility	Shared	Shared	Requires cooperation.
CDR (Call Detail Record) accuracy	X	—	Zayo must ensure billing correctness.
Internal call logs (PBX)	—	X	
Call encryption, data protection, secure transmission			
Encryption in transit (TLS/SRTP if offered)	X (provides)	X (enables on PBX/SBC)	
Protection of CDRs/customer metadata	X	—	
Protection of internal PBX data	—	X	Customer ensures logs, voicemail servers, and recordings are secure.
Voicemail and call recording retention & encryption	Shared	X	Zayo only if recording service is provider-hosted.
Endpoint (IP phones, softphones) confidentiality	—	X	
Handling customer personal information (names, DIDs, recordings, caller ID)			
Handling of personal data in CDRs	X	—	
Customer consent and notification for call recording	—	X	Customer must meet jurisdictional laws.
Retention/Deletion of PII in provider systems	X	—	
Retention/Deletion of PII inside PBX	—	X	Customer owns phone system data lifecycle.
Caller ID masking or privacy features	X	X (requests/configures)	Shared responsibility.
Incident Response			
SIP platform incident detection & response	X	—	
Customer PBX compromises (e.g., toll fraud)	—	X	Customer must secure PBX.
Fraud alerts and escalation	X	X	Customer must act quickly to avoid loss.
Coordinated investigation for call failures	Shared	Shared	Both parties must analyze logs.
E911 issues	Shared	Shared	Zayo provides routing; Customer maintains location accuracy.