

THE HOTEL SYSTEMS PTE. LTD. ANNEX C – TECHNICAL SPECIFICATIONS

Last Updated: October 21, 2025

(This Annex C is made pursuant to, and governed by, the Master Services Agreement (“MSA”) between The Hotel Systems Pte. Ltd. (“Provider”) and the Customer. This Annex C constitutes a mandatory precondition for the Provider to commence any work under the MSA.)

The Customer shall fulfill all requirements set forth in this Annex C, including ensuring the readiness and availability of its computer hardware, handheld devices, and all necessary networks.

Except as expressly specified in this Annex C, all other terms and conditions of the MSA shall remain in full force and effect.

1. Customer Responsibility

1.1. The Customer is solely responsible for:

- a. Procuring, installing, and maintaining all required end-user hardware, network infrastructure, and peripherals.
- b. Ensuring all necessary firewalls, security rules, network settings, and bandwidth requirements are implemented and continually maintained prior to and during the Service Term.
- c. Providing the Provider with accurate, timely, and functional credentials, API access, and test environments as required for integration.

2. Network and Internet Connectivity Requirements

2.1. As a cloud-based service, the stability and quality of the Customer’s Internet connection are paramount to system performance.

2.2. Internet Service Provider (ISP) and Bandwidth:

Requirement	Minimum Specification	Notes
Primary Connection Speed	100 Mbps Download/ 20 Mbps Upload.	Recommended dedicated capacity for the property.
Minimum Per-User Bandwidth	1 Mbps dedicated per concurrent user (for optimal performance).	Usage is concurrent (e.g., Front Desk operations).

Requirement	Minimum Specification	Notes
Network Redundancy	MANDATORY secondary ISP or failover connection (e.g., 4G/5G backup).	Critical to prevent service interruptions during high-traffic periods.
Latency (Ping)	Less than 100 milliseconds (ms) to the Provider's data center.	High latency significantly degrades user experience.
Jitter	Less than 30 ms.	High jitter results in lag and instability.

3. Firewall and Security Whitelisting

3.1. The Customer's network security team must configure its perimeter firewalls and local devices to allow outbound traffic to the Provider's cloud infrastructure.

Requirement	Detail
IP Whitelisting	Customer must whitelist the Provider's API, Web Application, and support IP ranges (provided separately). NOTE: These IPs may change and the Customer must update rules upon notification.
Required Ports	Outbound TCP/UDP traffic must be permitted on: Port 443 (HTTPS/SSL) for primary application access. Port 80 (HTTP) for initial DNS resolution and redirects (if applicable).
Proxy Servers	If the Customer uses a proxy server, it must be configured to pass traffic without inspection or interference for the Provider's URLs.

4. Integration and Interface Readiness

4.1. Successful deployment of the Cloud Solution relies heavily on reliable access to the Customer's existing core systems, particularly the Property Management System (PMS).

4.2. User Access and Authentication:

Requirement	Detail
PMS Interface License	Confirmation that the necessary PMS interface license (e.g., API license, Vendor key) has been procured from the PMS vendor.
Dedicated Test Environment	Provision of a non-production/sandbox environment of the PMS for initial testing and configuration.
Integration Credentials	Provision of valid and authorized API/Web Service URLs, Client IDs, Secrets, and User Credentials to access the PMS interface.
Interface Protocol	Customer must confirm the PMS supports a standard protocol such as HTNG, REST API, or XML Web Services for data exchange.

5. Third-Party Interfaces

5.1. Any interfaces to non-PMS systems (e.g., Telephone Switch, Door Locks, Energy Management) must be managed and secured by the Customer. The Provider will only interface with Customer-supplied API endpoints or certified vendor gateways.

6. Security and Compliance Requirements

6.1. Security requirements ensure both the Customer's network and the Provider's Solution are protected.

6.2. User Access and Authentication:

Requirement	Detail
User List Provisioning	Customer must provide a final list of all users, their roles, and their corresponding access levels a minimum of seven (7) days prior to the Go-Live date.
SSO Integration	If Single Sign-On (SSO) is requested, the Customer must provide a functional SAML 2.0 or OAuth 2.0 identity provider endpoint and all associated metadata required for configuration.

Requirement	Detail
Local System Access	Customer must provide the Provider's Implementation Team with temporary, secure access to relevant Customer systems (e.g., Firewalls, PMS backend) for the duration of the setup phase.

7. Provider Remote Access and Support

7.1. To enable efficient implementation and ongoing support, the Customer must ensure reliable and secure remote access capabilities.

- a. VPN Tunnel: A pre-configured, secure VPN connection or equivalent dedicated access mechanism must be available for the Provider's certified support team.
- b. Remote Desktop: Remote desktop access (e.g., TeamViewer, RDP) to the PMS or necessary interface gateway must be available and whitelisted only for Provider personnel.
- c. Access Revocation: The Customer retains the right to revoke all remote access immediately upon completion of the implementation or in the event of a security concern.

8. Data Sovereignty and Compliance

8.1. The Customer is responsible for confirming that the Provider's cloud data center location meets all applicable regional data sovereignty, GDPR, CCPA, PCI, or other applicable standards.

8.2. Provider maintains compliance with cloud infrastructure regulations, but ultimate responsibility for jurisdictional compliance lies with the Customer.

9. MSA Reference

9.1. This Annex C is governed by, and forms part of, the Master Services Agreement (MSA) between The Hotel Systems Pte. Ltd. and the Customer. All defined terms, general provisions, confidentiality obligations, and dispute resolution mechanisms in the MSA shall apply to this Annex C.

9.2. Any conflict between this Annex C and the MSA is resolved in favor of this Annex C for technical specifications only.