Standard Operating Procedure (SOP) for IT Operations

For Burj Al Arab – IT Department

1. Purpose

This SOP establishes guidelines for managing IT infrastructure, cybersecurity, and digital services at **Burj Al Arab**, ensuring seamless operations, data security, and compliance with industry standards such as **ISO 27001 (Information Security Management)** and **PCI DSS (Payment Card Industry Data Security Standard)**.

---

2. Scope

Applies to all IT personnel, contractors, and authorized staff accessing IT systems, including:

- **Network infrastructure**
- **Guest services (Wi-Fi, smart room controls, digital concierge, etc.)**
- **Property management systems (PMS)**
- **Payment processing systems**
- **Cybersecurity measures**

---

3. IT Infrastructure & Network Management

3.1 Network Security

- **Segregate networks**: Guest Wi-Fi, internal staff network, and administrative systems must remain isolated.
- **Deploy firewalls and intrusion detection/prevention systems (IDS/IPS)** to monitor network traffic.
- **VPN access** is required for remote IT staff and authorized personnel.
- **MAC address filtering** should be enforced for internal device connections.

3.2 Wi-Fi & Internet Services

- Provide **high-speed, encrypted Wi-Fi** for guests using **WPA3 security**.
- Limit bandwidth for **public Wi-Fi** to prevent network congestion.
- Implement **content filtering** to block malicious websites and inappropriate content.

3.3 Server & Data Center Management

- Maintain **24/7 monitoring** of data center servers using **SNMP-based monitoring tools**.
- Schedule **automatic backups** for all critical systems and store them in **geo-redundant locations**.
- Ensure **biometric and keycard access** for data center entry.

---

4. Guest IT Services & Smart Room Technology

4.1 Digital Concierge & Smart Room Controls

- Ensure **real-time connectivity** of **in-room tablets, voice assistants, and smart controls**.
- Encrypt and secure **IoT devices** against cyber threats.
- Regularly test **guest room automation (lighting, AC, curtains, etc.)** for seamless operation.

4.2 Payment Systems & PCI Compliance

- Implement **end-to-end encryption (E2EE)** for online and POS transactions.
- Perform **quarterly PCI DSS compliance audits**.
- Restrict **credit card data storage**; use **tokenization** for guest payments.

---

5. Cybersecurity & Data Protection

5.1 Access Control & Authentication

- Implement **multi-factor authentication (MFA)** for all administrative systems.
- Follow **role-based access control (RBAC)** and grant minimum privileges.
- **Disable inactive user accounts** after **30 days** of non-use.

5.2 Threat Detection & Incident Response

- Use **SIEM (Security Information & Event Management)** tools for threat monitoring.
- Employees must report **phishing emails, unauthorized access, or anomalies** immediately.
- Incident response team must **contain, investigate, and mitigate breaches** within **4 hours**.

5.3 Data Privacy & GDPR Compliance

- Secure all **guest personal data** under **GDPR** and UAE **Data Protection Laws**.
- Automatically **purge guest data** after **12 months of checkout** unless legally required.
- Encrypt guest communications via **TLS 1.2 or higher**.

---

6. IT Support & Helpdesk Operations

6.1 Helpdesk Support

- Provide **24/7 IT support** for guests and staff.
- **Categorize support requests**:
  - **Priority 1** – System-wide failure (Response: <15 min)
  - **Priority 2** – Guest impact issue (Response: <30 min)
  - **Priority 3** – Routine support (Response: <2 hours)
- Maintain **IT ticketing system (ServiceNow, Zendesk, etc.)** for tracking.

6.2 Hardware & Software Maintenance

- **Patch management**: Apply software updates every **30 days**.
- **Replace outdated hardware** every **3-5 years**.
- **Secure disposal of retired devices** via certified **e-waste recycling**.

---

7. Compliance & Audits

- Conduct **annual cybersecurity audits** as per **ISO 27001** standards.
- Perform **vulnerability assessments and penetration testing** every **six months**.
- Ensure all IT systems meet **Dubai Tourism and Jumeirah Group IT regulations**.

---

8. Disaster Recovery & Business Continuity

- Maintain **real-time backup systems** for critical hotel operations.
- Test **disaster recovery (DR) procedures** every **six months**.
- Establish **failover data centers** to ensure **99.99% uptime**.

---

9. Review & Continuous Improvement

- Conduct **quarterly IT policy reviews** to update security measures.
- Train employees on **cyber hygiene & phishing awareness** annually.
- Implement **AI-driven anomaly detection** to enhance security.

---

by: Irphan Salam

📅 *Effective Date:*

🔄 *Next Review Date:*