HYDROLOGIC Device Provisioning & Lifecycle Policy

Project: Grand Marina Hotel Water Systems Security

Analyst: Tung Thanh Nguyen

1. Device Onboarding (The "Birth" Stage)

To maintain the "Chain of Trust," every new sensor must be formally provisioned before it is allowed to touch the hotel network.

- **Unique Identity:** Every device must have a unique **Common Name (CN)** following the standard: HYDROLOGIC-[Location]-[DeviceNumber] (e.g., HYDROLOGIC-NewWing-004).
- **Credential Generation:** We use a **Manual Provisioning** workflow for the current phase. A Security Engineer must generate a unique Private Key and Certificate Signing Request (CSR) for each new unit.
- **Root CA Signing:** All device certificates must be signed by the established **Grand Marina Root CA**.
- **Secure Installation:** Private keys must be loaded onto devices via a secure, wired connection in the IT workshop. Keys should never be transmitted over the air or stored in plain text on shared drives.

2. Active Use & Authentication

Once deployed, the broker acts as the gatekeeper to ensure only these provisioned devices can communicate.

- **Mutual TLS Enforcement:** The broker is configured to **require** a valid certificate from every client (require_certificate true).
- **Identity Mapping:** We use use_identity_as_username true. This ensures that the logs specifically show which physical device is sending data, preventing a compromised device from "spoofing" another location.
- **Port Restriction:** All secure traffic must flow through Port **8885** (to avoid Windows port conflicts identified in testing).

3. Maintenance & Renewal (The "Mid-Life" Stage)

Certificates are not permanent. They must be managed to prevent system outages.

- **Validity Period:** All HYDROLOGIC certificates are issued with a **1-year (365-day)** expiration.
- **Renewal Window:** IT staff must begin the renewal process **30 days** before expiration.

- **Rotation Protocol:** We implement "Make-Before-Break." A new certificate is generated and pushed to the device while the old one is still valid, ensuring the water monitoring never goes offline during the transition.

4. Revocation & Retirement (The "End-of-Life" Stage)

This is our critical defense against physical theft or hardware failure.

- **Immediate Revocation:** If a device is reported missing (e.g., from the Pool Pump House), its certificate must be revoked immediately using the **Certificate Revocation List (CRL)**.
- **Decommissioning:** When a sensor is replaced or a wing is closed:
    1. The certificate is invalidated at the broker.
    2. The device hardware is physically wiped of all cryptographic keys.
    3. The device ID is "retired" in the central database to prevent reuse.

5. Policy Summary for Stakeholders

Stage	**Action**	**Expected Outcome**
Expansion	Provisioning a new sensor	Only the new, verified sensor can connect.
Theft	Revoking a certificate	A stolen device becomes a "brick" and cannot access the data.
Renewal	Rotating certificates	Continuous security without downtime.