Device Provisioning Policy

The Grand Marina Hotel — Water Monitoring System

Document Version	**1.0**
Created By	Diego Corsino
Date	08/31/2026
Approved By	[Leave blank — for client signature]

1. Scope and Purpose

This policy governs the provisioning, management, and decommissioning of HYDROLOGIC devices connected to The Grand Marina Hotel's water monitoring system.

Devices Covered

Device ID	Location	Certificate	Status
HYDROLOGIC-MainBuilding-001	Mechanical Room A	device-001.pem	Active
HYDROLOGIC-PoolSpa-002	Pool Pump House	device-002.pem	Active
HYDROLOGIC-Kitchen-003	Kitchen Mechanical	device-003.pem	Active
[Future devices as deployed]			

2. New Device Onboarding Process

Step 1: Device Registration

Device registration is done through Mutual TLS encryption. Each device must possess a unique client certificate to be registered. This certificate must be signed by the Grand Marina Root CA as a chain of trust.

Step 2: Certificate Generation

Simply run `generate_client_certs.py` as it automates the provisioning of these device specific files.

Step 3: Certificate Installation

Flash the certificate to the device via the secure USB provisioning station in the IT office. The device must be physically present — remote provisioning is not permitted.

Step 4: Connection Verification

Verify the following within 10 minutes:

Device establishes an encrypted data channel (MQTT connection on port 8883). Unencrypted connections (port 1883) must be rejected.

Device sends vitals through its assigned data route (MQTT topic): hydroficient/grandmarina/sensors/[location]/readings.

Vitals appear on the clinical dashboard within 60 seconds.

Run connectivity test: send 10 test messages from the device. Verify all 10 are received by the message server (broker) and displayed on the dashboard.

Step 5: Documentation

[What records are kept about the provisioned device?]

The specific records and data points kept for each provisioned device include:

- **Unique Identity (Common Name):** Each certificate includes a `COMMON_NAME` (e.g., `device-001` or `rogue-device`) that uniquely identifies the hardware within the MQTT hierarchy.
- **Organizational Metadata:** Records include the `ORGANIZATION_NAME` (e.g., "Hydroficient") and `COUNTRY_NAME` to ensure the device belongs to the correct entity.
- **Validity Period:** The certificate stores "Not Valid Before" and "Not Valid After" timestamps. The system uses these to reject devices with expired credentials.
- **Public Key:** The certificate contains the device's public key, which is used during the mTLS handshake to establish a secure, encrypted tunnel.

- **The Signature (Chain of Trust):** Crucially, the record includes a signature from your **Grand Marina Root CA**.

Estimated time for full onboarding: 45 minutes per device

3. Certificate Rotation Schedule

Current certificate validity period: 90 days

Rotation Schedule:

- Manual rotation triggered 30 days before expiration
- Automated email alerts at 30, 14, and 7 days before expiration

Rotation Procedure:

1. Generate a new security credential for the same device ID
2. Schedule a maintenance window during low-activity hours (2:00 AM - 4:00 AM) to minimize impact on the dashboard
3. Install the new credential on the device
4. Verify the device reconnects to the message server (MQTT broker) within 60 seconds
5. Revoke the old credential in the Certificate Authority. Add to the revocation list (a registry of credentials that are no longer valid).

Who is responsible:

4. Compromised Device Procedure

If a device is suspected to be compromised:

IMMEDIATE ACTIONS (within 15 minutes):

1. Revoke the device's security credential immediately. This blocks all future connections from that device — even if the attacker still has physical access to it.

2. Disconnect device from the network.

3. Notify security team immediately

INVESTIGATION (within 24 hours):

1. Review the message server logs for the affected device. Look for: unauthorized connections, unexpected data patterns, connections from unusual network addresses, or messages sent outside normal intervals.

2. Assess what data was exposed.

RECOVERY:

1. Factory reset the device to remove any compromised firmware or stored credentials.

2. Generate a completely new security credential with fresh encryption keys (do NOT reuse the old keys — they may be compromised).

3. Re-provision the device following the standard onboarding process (Section 2, Steps 2-5).

4. After reinstatement, monitor the device's network activity for 48 hours. Flag any anomalies for immediate review.

Emergency contact: _____

5. Decommissioning Process

When a device is removed from service:

Step 1: Revoke Certificate

[How is the certificate revoked?]

Revoke the device's certificate immediately — even if the device is being retired, not compromised. Add it to the revocation list so no system will accept it again. A revoked credential must never be reused, even if the same device ID is assigned to a replacement unit later.

Step 2: Remove from Monitoring

[How is the device removed from dashboards/alerts?]

Remove the device from the message server's authorized device list. Remove the device from the dashboard. Verify the dashboard no longer shows a "device offline" warning for the retired device.

Step 3: Physical Removal

[What happens to the physical device?]

Factory reset the device to wipe all stored certificates, encryption keys, and configuration data.

Step 4: Documentation

[What records are updated?]

Update the Hydroficient Device Registry: mark the device as "Decommissioned" with the decommission date, reason, and technician name. Update Grand Marina's IT asset database to match. Archive 90 days of the device's network activity logs for compliance and audit purposes.

6. Policy Review

This policy will be reviewed:

- Annually
- After any security incident
- When new devices are added
- Other: _____

Next review date: August 31, 2027

Signatures

Role	Signature	Date
Prepared by: Diego Corsino, Junior Security Engineer	Diego Corsino	August 31, 2026
Reviewed by: Maya Chen, Senior Security Engineer		
Approved by: Marcus Webb, General Manager, The Grand Marina Hotel		