Device Provisioning Policy

The Grand Marina Hotel — Water Monitoring System

Document Version	1.0
Created By	Prescott Narcisse
Date	August 28, 2026
Approved By	

1. Scope and Purpose

This policy governs the provisioning, management, certificate lifecycle, incident response, 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

Register the new HYDROLOGIC sensor in Hydroficient's device inventory and assign a unique device ID based on its deployment location and sequence, such as HYDROLOGIC-NewWing-004. Record the device serial number, planned Grand Marina location, and assigned device ID before credentials are created.

Step 2: Certificate Generation

An authorized Hydroficient security engineer generates a unique TLS client certificate and private key using generate_client_certs.py. The certificate is signed by Hydroficient's trusted Certificate Authority (CA). Access to the CA private key is restricted to authorized security personnel and must not be stored on or shared with field devices. Certificates and private keys are unique to each HYDROLOGIC device and are never reused.

Step 3: Certificate Installation

Securely transfer the device certificate, private key, and trusted CA certificate to the intended HYDROLOGIC device during provisioning. Verify the device ID and certificate identity/fingerprint against the provisioning record before installation. If the certificate does not match the intended device, stop the process, revoke the credential, and generate a replacement.

Step 4: Connection Verification

Connect the device to The Grand Marina's mTLS MQTT broker using the secure mTLS listener on port 8883. Verify that the device successfully authenticates with its valid client certificate and publishes test sensor readings to its assigned MQTT topic. Confirm that connections without a client certificate, with a certificate from an untrusted CA, or with an expired certificate are rejected. The device must not be placed into service until secure connectivity and data delivery are confirmed.

Step 5: Documentation

Update the device inventory with the device ID, serial number, physical location, certificate filename or fingerprint, certificate expiration date, provisioning date, and technician/security engineer responsible. Notify the Hydroficient security team and the designated Grand Marina operations/IT contact that the device has been securely onboarded and is active.

Estimated time for full onboarding: 30–45 minutes per device

3. Certificate Rotation Schedule

Current certificate validity period: 1 year

Rotation Schedule:

- Manual rotation begins 30 days before certificate expiration.
- Rotation may also be triggered immediately after suspected credential exposure, device compromise, or a security incident.
- Certificate expiration dates are tracked in the device inventory so the Hydroficient security team can initiate renewal before service is affected.

Rotation Procedure:

1. An authorized Hydroficient security engineer generates a new certificate and private key for the same device identity using the approved certificate-generation process.
2. The new certificate is securely installed on the correct HYDROLOGIC device and its identity/fingerprint is verified against the updated provisioning record.
3. The device is reconnected to the mTLS broker and tested to confirm successful authentication and normal sensor data publishing.
4. After the replacement credential is verified, the old certificate is revoked and must not be reused.
5. The device inventory is updated with the new certificate fingerprint, issue date, expiration date, and rotation date.

Who is responsible: Hydroficient Security Engineering team; the designated Grand Marina IT/operations contact is notified of planned rotations.

4. Compromised Device Procedure

If a HYDROLOGIC device is suspected to be compromised:

IMMEDIATE ACTIONS (within 15 minutes):

1. Revoke or disable the affected device's certificate so it can no longer authenticate to the mTLS broker.
2. Disconnect or isolate the device from The Grand Marina network to stop further communication.
3. Notify Hydroficient Security Engineering and the designated Grand Marina IT/operations contact, and record the time the incident was identified.

INVESTIGATION (within 24 hours):

1. Review MQTT broker, device, and relevant network logs for unusual connections, unexpected messages, authentication failures, or other anomalous behavior.
2. Assess whether sensor data, device credentials, private keys, or other system information may have been exposed or altered, and document the findings.

RECOVERY:

1. Factory reset or securely rebuild the affected device so untrusted configuration, firmware, and stored credentials are removed.
2. Generate a completely new certificate and private key; never reuse credentials suspected of compromise.
3. Re-provision the device using the standard onboarding process, verify mTLS authentication and sensor publishing, and monitor the restored device for abnormal activity.

Emergency contact: Hydroficient Security Engineering / designated on-call security contact; Grand Marina IT/operations management.

5. Decommissioning Process

Step 1: Revoke Certificate

Immediately revoke the device's client certificate when the device is permanently removed from service. The revoked credential must never be reused, even if the same device ID is later assigned to replacement hardware.

Step 2: Remove from Monitoring

Remove the retired device from authorized-device records, dashboards, expected-data monitoring, and alerting rules. Verify that monitoring systems no longer expect sensor readings from the decommissioned device.

Step 3: Physical Removal

Factory reset or securely wipe the device to remove its certificate, private key, CA material, and configuration. Return serviceable hardware to Hydroficient through the approved inventory process, or securely dispose of end-of-life hardware according to company procedures.

Step 4: Documentation

Update the device inventory to mark the device as Decommissioned. Record the decommission date, physical location, reason for removal, certificate revocation status, disposition of the physical device, and the technician or security engineer who completed the process. Retain relevant security and broker logs according to Hydroficient's record-retention requirements.

6. Policy Review

This policy will be reviewed:

- Annually
- After any security incident involving a HYDROLOGIC device
- When new devices, hotel wings, or major water-monitoring expansions are added
- When certificate, broker, provisioning, or security requirements materially change

Next review date: August 28, 2027

Signatures

Role	Signature	Date
Prepared by: Prescott Narcisse		
Reviewed by: Maya Chen, Senior Security Engineer		
Approved by: Marcus Webb, General Manager, The Grand Marina Hotel		