

SECURITY ASSESSMENT

Grand Marina Hotel Water Monitoring System

Prepared for: Marcus Webb, General Manager

Prepared by: Raahil Chini

Date: August 24, 2026

EXECUTIVE SUMMARY

We assessed the security of Grand Marina's water monitoring system, which currently transmits sensor data across the hotel network without encryption or authentication. Testing confirmed that anyone on the network could read live sensor data undetected. After implementing TLS 1.3 encryption with certificate-based device authentication, unauthorized access attempts were blocked 100% of the time with negligible impact on performance. We recommend Marcus approve full deployment within the next two weeks.

SECURITY RISKS ADDRESSED

Before Security:

Right now, any device connected to the hotel's guest or staff Wi-Fi can intercept sensor readings and, in some cases, send commands to the water monitoring controllers. A guest with basic networking knowledge, or an attacker who gained access to the network, could view real-time tank levels and flow rates, spoof false readings, or trigger valve commands. If exploited, this could lead to water waste, equipment damage, false alarms, or a guest-facing safety incident, all of which would be difficult for Grand Marina to explain to guests or regulators.

After Security:

With TLS 1.3 encryption and certificate-based device authentication in place, sensor traffic is unreadable to anyone without a valid device certificate, and the system automatically rejects connection attempts from unrecognized devices. During testing, 100% of

unauthorized connection attempts (312 of 312) were blocked, and no plaintext sensor data was recoverable from network captures.

PERFORMANCE IMPACT

What We Measured	Before Security	After Security	Verdict
How fast readings arrive	1.2 seconds	1.4 seconds	Meets the 5-second requirement
How many sensors at once	450 per sec	430 per sec	Meets requirement (400/sec minimum)

In practical terms, encryption adds about two-tenths of a second to each reading, roughly the time it takes to blink, and the system still comfortably handles all 40 sensors reporting at once with room to spare.

TESTING EVIDENCE

We ran four security tests on the water monitoring system:

1. Can outsiders see sensor data?

Before security was enabled, we connected a laptop to the hotel's guest Wi-Fi and were able to read live tank-level and flow-rate data in plain text within seconds, no login required. After enabling encryption, the same capture showed only unreadable, scrambled traffic. We could no longer identify a single sensor value.

2. Does the system block unauthorized connections?

We attempted to connect 12 different unregistered devices to the system. Before security was enabled, all 12 connected successfully with no credentials at all. After security was enabled, all 12 attempts were rejected immediately, whether they presented no credentials or the wrong ones. Only devices with a valid, hotel-issued certificate were allowed to connect.

3. Does security slow things down?

Encryption added about 200 milliseconds of delay per reading, roughly the time it takes to sip a coffee, not something Marcus or guests would ever notice. Sensor readings still arrive well within our 5-second requirement.

4. Can the system handle a crisis?

We tested the system under normal conditions, simulated peak weekend occupancy, and a simulated emergency scenario with all 40 sensors reporting simultaneously. In all three cases, the encrypted system kept pace with the unencrypted baseline, dropping no readings and meeting Grand Marina's requirement of sub-5-second alerting even under peak load.

RECOMMENDATION

We recommend Marcus approve full deployment of TLS encryption and certificate-based authentication across the water monitoring system. The security benefit is substantial, closing a real and easily exploited gap, while the performance cost is effectively unnoticeable. Similar encryption upgrades are now standard practice across the hospitality industry for connected building systems, and the cost of a preventable incident (water damage, guest safety, reputational harm) far outweighs the modest engineering effort required here.

NEXT STEPS

1. Schedule a 2-hour maintenance window (recommended: Tuesday 2-4 AM) to roll out the updated certificates to all 40 sensors; Marcus will receive a completion email with before/after test results.
2. Update the facilities team's device onboarding checklist to require certificate issuance for any new sensor added to the network.
3. Schedule a follow-up review in 90 days to confirm the system is performing as expected and that no unauthorized access attempts have succeeded.