

SECURITY ASSESSMENT

Grand Marina Hotel Water Monitoring System

Prepared for: Marcus Webb, General Manager

Prepared by: Alexander Sher

Date: 10/5/2026

EXECUTIVE SUMMARY

I recommend turning on encryption, with identity checks, for Grand Marina's water monitoring system immediately. Our testing showed that without it, anyone on the hotel network can read what the sensors report, and with it, they see nothing. The protection adds a delay too small to notice, and the system handled more than double our emergency load without a single failure.

SECURITY RISKS ADDRESSED

Before Security:

Right now, sensor readings travel across the hotel network like postcards: anyone handling them along the way can read them. During testing, I listened in on the network and captured 5 messages in plain text, each showing the sensor's ID, the water pressure, the flow rate, and the exact time.

What this means for Grand Marina:

- A person who can read the system can learn what the sensors are reporting and when. If the system also accepts messages from unverified sources, someone could send fake readings, such as an "all clear" while something is wrong.
- Fake alerts send maintenance staff to the wrong place, while a real leak or pressure problem could be hidden. Either one can mean water damage, closed rooms, and cancelled bookings.
- If guests or the press learn the hotel's building systems were readable by anyone on the network, the story becomes about carelessness, not a technical flaw. This has

happened elsewhere: in 2021, someone broke into a Florida city's water treatment system and tried to change the chemical levels in the drinking water.

After Security:

With encryption enabled:

- All sensor data is scrambled while it travels. Someone intercepting it sees only random characters, with no temperatures, no locations, and no alerts.
- The system turns away any device that doesn't have the right digital credentials. A laptop or fake sensor that tries to connect, or to send false readings, is blocked.
- Grand Marina moves from "known exposure" to a defensible position. If an insurer or inspector asks how the building systems are protected, we have a tested, documented answer.

PERFORMANCE IMPACT

What We Measured	Before Security	After Security	Verdict
How fast readings arrive	50.54 ms or 0.051 seconds	50.61 ms or 0.051 seconds	No noticeable difference
How many sensors at once	100 msg/per sec	100 msg/per sec	Meets requirements

Encryption added about seven hundredths of a thousandth of a second to each reading, an increase of 0.14%. A single blink of an eye takes about 300 thousandths of a second, so the delay is thousands of times shorter than a blink. Staff will see alerts just as fast as they do today.

TESTING EVIDENCE

We ran four security tests on the water monitoring system:

1. Can outsiders see sensor data?

From a laptop on the hotel network, I captured 5 sensor messages in plain text. Each one clearly showed the sensor's ID, the water pressure, the flow rate, and the time it was sent.

After security: The same attempt returned an error and no readable messages. Encryption blocked the eavesdropping.

2. Does the system block unauthorized connections?

- A sensor with the correct credentials connected normally.
- A sensor presenting credentials from an unrecognized source was blocked.
- A sensor connecting with identity checking switched off was allowed in any way.

The third result matters most. Encryption alone hides the data, but the identity check is what ensures it goes only to the right place. Without that check, a fake system could pose as the real one. It's like sealing an envelope but never checking who you're handing it to. I recommend that identity checking can never be turned off.

3. Does security slow things down?

Average delivery time was 0.0505 seconds without encryption and 0.0506 with it, a difference of 0.14%. That is far shorter than a blink and has no effect on how quickly staff see an alert.

4. Can the system handle a crisis?

I tested four loads, with encryption on and off, and everything succeeded each time:

Load	Without Security	With Security
10 messages/sec (normal)	Success	Success
25 messages/sec (moderate)	Success	Success
50 messages/sec (emergency)	Success	Success
100 messages/sec (beyond requirements)	Success	Success

The system kept up at double our emergency load, so it meets Grand Marina's requirements.

RECOMMENDATION

Right now, the readings that tell us whether the building's water systems are safe can be read by anyone on the network. Encryption closes that gap, and it costs guests and staff nothing they'll notice: the delay is 0.14%, and the system handled twice our emergency load with no failures. The cost of doing nothing is also real: water damage, lost room nights, and reviews that stay online for years. Industry research shows security failures are getting more expensive every year, with IBM reporting a record U.S. average of \$11.5 million per data breach in 2026.

The protection is tested and ready, and the only remaining step is to turn it on.

NEXT STEPS

1. Turn on encryption for all sensors and the central monitoring screen (Weeks 1-2)

Our team will do this during low-occupancy hours. Marcus will see no change in how the system looks or behaves, and unprotected connections will be blocked automatically.

2. Require identity checks on every device (Weeks 3-4)

Each sensor gets its own digital ID, and the setting that allows connections without checking IDs is permanently disabled. We'll confirm with a repeat of the test where a device with no valid credentials tries to connect.

3. Train engineering staff and set up alerts (Weeks 4-5)

We'll brief the engineering and IT teams on what to watch for and what to do if a sensor stops connecting, and set up alerts that notify them immediately if any sensor goes offline.