PROTECT THE PEOPLE AND PROPERTY AROUND YOU

TOP 7 COSTLY MISTAKES

TO AVOID WHEN RUNNING A DIGITAL GUARD TOUR SYSTEM

omnigo

1. SKIPPING INITIAL SETUP AND CONFIGURATION

The Mistake:

Launching the system with default settings or incomplete route details.

Scenario: A corporate campus deploys its new guard tour software but doesn't customize routes to match their high-risk areas. Six months later, an incident occurs in an unmonitored stairwell—revealing that the checkpoint for that location was never added.

Avoid it by:

Start with a thorough risk assessment and site walkthrough involving both supervisors and frontline officers. Identify critical areas, vulnerable access points, and common trouble spots, then create a visual route map. Enter all checkpoints into the system with accurate names, locations, and risk ratings. Test the route with a small pilot group to ensure coverage and scan reliability before full deployment. Periodically review routes as site layouts or security priorities change.

2. NOT TRAINING ALL USERS THOROUGHLY

The Mistake:

Assuming a quick demonstration is enough for officers to use the system effectively.

Scenario: At a manufacturing plant, a new guard is told, “Just scan each checkpoint with your phone.” He doesn’t know how to log defects or hazards. A leaking chemical drum goes unreported because he thought only Maintenance should document it.

Avoid it by:

Create a structured onboarding process that includes both classroom-style instruction and hands-on practice in the field. Demonstrate all functions—from scanning checkpoints to reporting hazards, taking photos, and adding notes. Provide quick-reference guides or in-app tips for common tasks. Follow up with ride-alongs or supervisor check-ins during the first few shifts to ensure correct usage. Schedule quarterly refresher courses and update training whenever the software changes.

3. IGNORING DATA REVIEW AND ANALYSIS

The Mistake:

Treating patrol data as a record-keeping formality instead of a tool for proactive improvement.

Scenario: A hotel security team completes every tour on schedule, but no one reviews the reports. When guests start complaining about poorly lit parking areas, management realizes guards have been noting “light out” for weeks—with no action taken.

Avoid it by:

Establish a recurring review process where supervisors analyze reports for trends, missed checkpoints, or repeat hazards. Use dashboards or automated summaries to flag problem areas. Assign follow-up tasks for maintenance or additional patrols based on findings. Share key insights with leadership to justify resource adjustments or technology upgrades. Treat the system’s analytics as a live operational tool, not just an archive.

4. OVERCOMPLICATING TOUR SCHEDULES

The Mistake:

Creating unrealistic patrol routes with too many checkpoints and too little time.

Scenario: A retail mall sets a patrol route with 85 checkpoints to be completed in 45 minutes. Guards start skipping less visible checkpoints to keep up, and a shoplifter uses one of those areas to exit with stolen merchandise.

Avoid it by:

Build patrol schedules with input from officers who know the pace and layout of the site. Balance the number of checkpoints with the time needed for thorough inspections, factoring in possible delays for incidents or guest interactions. Stagger routes to cover different areas at different times rather than trying to hit everything on every tour. Pilot new schedules for a week and adjust based on completion rates and feedback before locking them in.

5. FAILING TO MAINTAIN CHECKPOINTS AND DEVICES

The Mistake:

Letting hardware and checkpoints go unchecked until they stop working.

Scenario: At a hospital, an NFC checkpoint in the basement stops working months ago. Guards skip it each night without reporting the failure. Eventually, an unauthorized person uses the basement as a hiding spot because it's never patrolled.

Avoid it by:

Include checkpoint inspections in your regular maintenance routine—physically verify tag placement and functionality at least once a month. Keep spare tags and mounting supplies on hand for immediate replacement. Implement a reporting process so officers can flag malfunctioning devices on the spot. Also, maintain a device charging and update schedule so mobile units are always ready and running the latest software.

6. NOT INTEGRATING WITH OTHER SECURITY PROCESSES

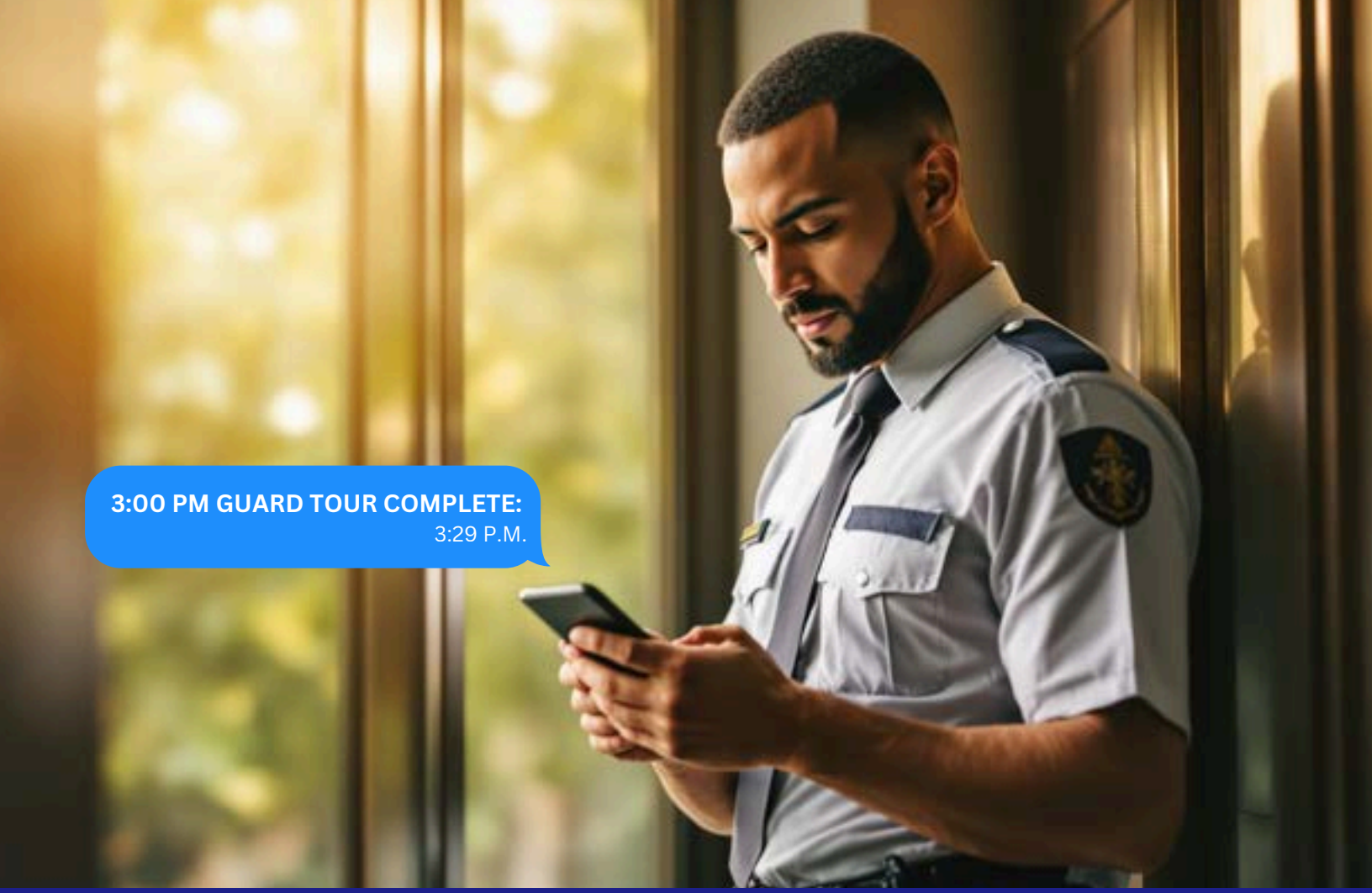
The Mistake:

Running the guard tour system in isolation from incident reporting, dispatch, or maintenance workflows.

Scenario: A university security officer scans a checkpoint at a broken door but has no way to submit a maintenance request through the patrol app. Weeks later, the door is still unsecured, and a theft occurs in the building.

Avoid it by:

Connect your guard tour software with your incident management, dispatch, or work order systems so issues can be logged and assigned instantly. If direct integration isn't possible, create clear workflows for exporting and sharing data. Train officers on when and how to escalate issues found during patrols. Use integrated reporting to close the loop and confirm issues are resolved—not just recorded.



7. UNDERUTILIZING SYSTEM ALERTS AND NOTIFICATIONS

The Mistake:

Not enabling or customizing alerts to match operational priorities.

Scenario: A late-night patrol at a warehouse skips two checkpoints. The system could have sent an alert to the supervisor immediately—but alerts weren't set up. The oversight goes unnoticed until a morning shift discovers a break-in.

Avoid it by:

Identify the types of patrol exceptions that require immediate attention—missed scans, delayed tours, or activity in restricted areas—and configure alerts for those events. Assign responsibility for monitoring alerts to specific roles or shifts, and ensure there's a documented response procedure. Periodically review alert settings to keep them relevant to evolving risks. Avoid alert fatigue by limiting notifications to issues that truly demand action.

omnigo

1.866.421.2374
omnigo.com