WORKSHEET 2.5

The Messaging Group That Runs the Hotel

Subchapter 2.5 · case in the book: Rio de Janeiro

Ask your duty manager to show you the messaging groups on their phone that are used for work, and count the members of the largest one. Then ask how many of those members still work at the hotel. The group is where your hotel's day is actually organised, and you have never decided who belongs to it.

This worksheet turns the tools of the subchapter into a form you can fill in. The texts come from the book; the empty columns are for your own property. Adapt it before use: an unadapted checklist is exactly what the book warns against.

Practical application: what to do in your property

Step (from the book)	Done?	What we found / owner
List every messaging group used for work, its members and what it carries.		
Choose a messaging tool the hotel controls and that staff will find as easy as the one they use.		
Create groups as the hotel, and tie membership to employment.		
Remove leavers from every group on their last day.		
Never forward images of identity documents or cards; enter the information and delete the image.		
Give guests a hotel channel for reservations and the concierge.		
Remove sensitive images automatically after a short period where the tool allows it.		
Move the duty managers' group first, so that management leads by example.		

These steps are the book’s method, not requirements of ISO/IEC 27001. Evidence can take whatever form suits the property; a separate document is needed only where an applicable requirement, or the property’s own system, makes it necessary.

Verification Pact: what is believed, tested against the standard

What is commonly believed	What actually holds	Our position
«Forbidding personal messaging solves the problem.»	Without an equally quick alternative, it drives the practice out of sight and teaches staff that the rules are unrealistic.	
«Messaging groups are informal and outside the system.»	They are a transfer facility, and the rules on information transfer and access apply to them.	
«People leave the group when they leave the hotel.»	They leave only if somebody removes them. Membership is an access right and must be removed like any other.	

What is commonly believed	What actually holds	Our position
«Staff phones are personal, so the hotel cannot act.»	The hotel can protect its own information on user devices through a tool that separates work from personal content.	
«A guest who sends a passport photograph has consented.»	The guest has chosen a convenient channel. The hotel decides what happens to the image once it arrives.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Forbidding personal messaging without providing an equally quick alternative.		
Letting individuals create work groups and never clean their membership.		
Leaving former staff in groups that carry guests' information.		
Letting guests send documents and cards to staff's personal numbers.		
Forwarding photographs of passports and cards as ordinary content.		
Ignoring what happens to work content on personal phones and their backups.		
Having management use the groups the memo forbids.		

Operative synthesis

- **Staff who work away from desks use the quickest tool that reaches the people they need, and in many hotels that is a messaging group on a personal phone. Forbidding it without an alternative fails. Managing it succeeds: a tool the hotel controls, groups created by the hotel, membership tied to employment, sensitive content removed automatically, a hotel channel for guests, and a few rules staff can remember.**
- **The instrument is a map of the hotel's operational messaging: each channel, what it is for, who manages its membership, what may be shared in it and how long it is kept. Maintained with human resources, it turns the hotel's real operating system into a part of its information security system.**
- **In Rio nothing had been done in bad faith. A head concierge took a document from a guest's assistant in the way guests preferred, a reception team used the group that made its work possible, and a general manager issued a sensible memo that nobody could follow. The passport reached a website through a friend who had left eight months earlier and had never been removed from a group nobody owned.**
- **Which raises the question the next subchapter takes up. Staff are not the only people outside the hotel's direct control who reach its systems. Its suppliers do too, and some of them reach in at night. What happens when a night auditor watches the cursor on his screen move by itself at three in the morning, and discovers that the property system's supplier has been connected all along, is the case that follows.**

Action plan for our property

Action	Owner	Due	How we will know it worked

Source: Francesco Dore, The Helm and the Lens, Volume 5a «The Helm», subchapter 2.5. Edizioni Effedore, 2026. Clause references are paraphrased; this sheet does not reproduce the text of ISO/IEC 27001. It is not legal advice: data protection and information security law is that of the place where the property operates.