WORKSHEET 2.1

Access Is Granted at Hiring and Forgotten at Leaving

Subchapter 2.1 · case in the book: Athens

Ask for a list of every account on your property management system and set it beside this month's payroll. Count the names that appear on the first list and not on the second. Whatever the number, each of those accounts belongs to somebody the hotel no longer employs and can no longer instruct.

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
Set every account on every system beside the payroll, once, and close what belongs to nobody.		
Define a small number of roles for each system, and grant access by role.		
Add a notice to IT to the human resources process for joiners, movers and leavers.		
Close every account on every system on each leaver's last day.		
Remove the old role's rights whenever somebody moves.		
Have department heads review and sign their people's accounts every quarter.		
Require a second factor on hosted systems and alert on unusual logins from outside.		
Replace shared accounts with named ones, and give suppliers named accounts for stated purposes.		

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
«Access is an IT matter.»	IT administers accounts. Whether each person needs each right is a business decision that belongs to the head of their department.	
«When staff leave the building, their access ends.»	For hosted systems reachable from anywhere, access ends only when the account is closed.	

What is commonly believed	What actually holds	Our position
«Copying a colleague's account is a quick way to set up a new starter.»	It copies whatever the colleague has accumulated. Rights should come from the role, not the person.	
«Once a year, IT checks the list of accounts.»	Access rights must be reviewed, and only department heads can judge whether their people's rights are still needed.	
«Logs are for investigations.»	Logs must also be analysed, and a simple alert on unusual logins is often the earliest warning a hotel gets.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Opening accounts by copying a colleague's.		
Running a leaving process that recovers the building's keys and not the systems'.		
Adding rights when people move and never removing the old ones.		
Forgetting that hosted systems can be reached from anywhere.		
Letting IT review access instead of the heads of department.		
Keeping shared accounts because they are quicker.		
Recording logins and never looking at them.		

Operative synthesis

- **In a hotel, people join, move and leave far faster than systems change, and access that is not managed at the speed of people drifts away from the people the hotel employs. Every account that belongs to nobody, every right left over from an old job and every shared login is a door the hotel can no longer see, and on hosted systems those doors open from anywhere in the world.**
- **The instrument is a page that sets out, for joining, moving, leaving, temporary cover, suppliers and the quarterly review, who triggers each event, who decides the access and what is done by when. With roles for each system, reviews signed by department heads and an alert on unusual logins, it keeps the hotel's accounts in step with its people.**
- **In Athens nothing had been done out of neglect. Managers asked for accounts so their staff could work, an IT coordinator created them quickly, human resources ran a careful leaving process, and a hosted system made the hotel more efficient. The step that joined the leaving process to the systems had never been written, and a night auditor who left angry found that his password still worked eleven weeks later.**
- **Which raises the question the next subchapter takes up. Of all the information the people at a hotel's front desk handle, the most sensitive is what guests hand over at the counter: their passports and identity cards. What happens when those documents are copied, scanned and kept because the desk believes the law requires it, 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 2.1. 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.