WORKSHEET 1.4

Leadership, and Why Security Is Not the IT Department's Job

Subchapter 1.4 · case in the book: Prague

List the three decisions taken in the last year that most affected how your property protects its information. Beside each, write who took it. If none of them was taken by the owner or the general manager, either the property has an unusually good IT provider, or the decisions that mattered were taken without anybody noticing that they were security decisions.

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
Name an owner of the information security system inside the business, reporting to the owner of the property.		
Write the one-page list of management decisions that are security decisions.		
Replace shared logins with named accounts, beginning at the front desk.		
Require a second person for refunds, overrides and write-offs above a set amount.		
Protect the owner's and senior managers' accounts first, with named access and a second factor.		
List every administrator account, who holds it, and review the list every quarter.		
Put management's decisions, not only the provider's report, on the agenda of the management review.		
Give security its own line in the budget, approved by the owner.		

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
«We have outsourced information security to our IT provider.»	The work can be outsourced. The responsibility of top management to direct it, resource it and assign roles cannot.	
«Shared logins are an IT matter.»	They are the consequence of a licence or staffing decision taken by management, and they remove the ability to know who did what.	

What is commonly believed	What actually holds	Our position
«The owner needs full access to everything.»	The owner needs the information to run the business. Full administrative rights, without a second factor, on a shared password, are a different thing.	
«Signing the policy is how leadership is shown.»	Leadership is shown by the decisions management takes and the rules it applies to itself.	
«If the IT provider has not raised it, it is not a risk.»	Providers rarely raise risks whose remedy costs the owner money or convenience. Those risks have to be looked for from the management side.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Appointing the IT provider's consultant as the hotel's information security manager.		
Treating licence and staffing decisions as costs with no security consequence.		
Granting senior people exceptions that nobody else would be allowed.		
Allowing shared accounts at the front desk because it is quicker.		
Letting one person post, approve and check the same transaction.		
Holding a management review whose only content is the provider's report.		
Mistaking a signed policy for demonstrated leadership.		

Operative synthesis

- **Information security in a hotel is decided where budgets, staffing and supplier contracts are decided, which is to say by management. An IT provider can implement controls, but it cannot decide how many licences the hotel buys, what exceptions the owner grants himself, who may approve a refund or which supplier holds the keys. Those decisions settle the hotel's exposure, and unless management takes them knowingly, they are taken by default.**
- **The instrument is a page listing the handful of management decisions that are security decisions, where each is usually taken, what it decides and the rule the hotel has adopted. It turns leadership from a signature into a set of choices that can be seen and reviewed, and it is the first document an owner should ask for.**
- **In Prague nothing had been done carelessly. The owner hired a good provider, the provider built a sound system, and the budget meeting that saved money on licences was conducted with the care the owner applied to every cost. The system could only protect what management allowed it to protect, and management had allowed, without seeing it, the one arrangement that made every action at the front desk anonymous.**

› **Which raises the question the next subchapter takes up. Among the decisions that only management can take, one comes before all the others and is often taken by somebody else: where the system begins and ends. What happens when a hotel certifies the part of itself that is easiest to protect, and leaves outside the boundary the places where guests' information actually lives, 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 1.4. 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.