WORKSHEET 1.7

A Policy That Staff Can Check

Subchapter 1.7 · case in the book: Kyoto

Give your information security policy to a receptionist who joined last month and ask her to find the sentence that tells her what to say to a caller asking whether a named guest is staying in the hotel. If the sentence is not there, your policy is addressed to an auditor, and your staff have learned the real one somewhere else.

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
Reduce the general policy to one page that speaks about guests and the hotel, and have the owner sign it.		
Write ten to fifteen checkable rules for each guest-facing department.		
Write the rules in the working language of the department, with the department.		
Work through real situations with each team and rewrite the rules where they are silent.		
Give staff the words to refuse politely and to offer to pass a message.		
Decide and announce that staff who follow the rules will be supported when a guest complains.		
Record that each person has read and acknowledged the rules for their job.		
Review the rules after every incident and near miss, and at least once a year.		

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
«The policy has to be comprehensive to satisfy the auditor.»	It has to contain a small number of elements the standard specifies and be appropriate to the organisation. Length is not one of the requirements.	
«The policy is a statement of values.»	It must provide a framework for the system. In a hotel, the useful framework is a set of rules staff can apply and check.	

What is commonly believed	What actually holds	Our position
«Topic-specific policies belong in the IT manual.»	They belong wherever the people who must follow them will read them. The one on responding to requests about guests belongs at the front desk.	
«Once translated and signed, the policy has been communicated.»	Communication means the people concerned understand it and acknowledge it. A translation read once at signature is not that.	
«A receptionist who refuses a caller is being unhelpful.»	A receptionist who follows the hotel's rule on disclosure is applying the policy, and management is required to support her in doing so.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Adopting a policy from a template that could belong to any organisation.		
Writing values where staff need rules.		
Leaving the rule on disclosure of guests' presence unwritten.		
Translating abstract policy text instead of writing rules in the working language.		
Never testing the policy against the calls and requests that actually arrive.		
Criticising staff who protect a guest when the guest complains.		
Keeping topic-specific rules in a manual the people who need them never open.		

Operative synthesis

- **A policy protects information only when the people who handle information can apply it. In a hotel that means rules staff can check, written for the situations they meet, in the language they work in, and supported by management when applying them makes a guest or a caller unhappy. The general commitments the standard requires belong on one page signed by the owner. The rules belong at the desk.**
- **The instrument is a page of checkable rules for each department beneath a one-page policy: sentences such as never confirming a guest's presence to a third party, never accepting a security code by email, and changing contact details only after confirming with the guest. Each can be trained, tested and enforced, and each tells staff exactly what the hotel expects of them at the moment it matters.**
- **In Kyoto nothing had been done without care. A consultant wrote a complete policy, the owner and the management company approved it, the translation was faithful, and a talented**

receptionist tried to give the service she had been told the hotel's guests expected. The policy on the wall had nothing to say to her, and the policy she had seen enforced told her to help.

› **Which raises the question the next subchapter takes up. A policy states what the hotel will and will not do, and a risk assessment decides where it should spend its effort to make that true. What happens when a hotel assesses a hundred and eighty risks and assigns every one of them to the IT department, so that nobody with the authority to accept a risk ever sees one, 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 1.7. 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.