WORKSHEET 2.12

Guest Wi-Fi and the Network Behind It

Subchapter 2.12 · case in the book: Cartagena

Connect a laptop to your guest Wi-Fi in the lobby and ask your IT provider to show you what it can see. If the answer includes a printer, a file server or another guest's computer, the network you give to strangers is the same network you run the hotel on.

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
Connect to the guest Wi-Fi and see what it can reach, in the lobby, the rooms and the conference wing.		
Draw the network on one page, with what each network must never reach.		
Switch on guest isolation and keep it on.		
Provision event networks as the hotel, isolate them and remove them at the end of each event.		
Record every change that connects networks, with its reason, owner and date of reversal.		
Protect file shares and printers on the hotel's own network as if anybody could reach them.		
Set alerts for scanning and attacks on the guest network, and have a named person read them.		
Check the network against the page every quarter and after every large event.		

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
«Our guest network was designed to be separate.»	It was separate when it was designed. Only a check shows whether it is separate now.	
«Temporary changes for an event do not need recording.»	Changes to networks must follow change management. Unrecorded temporary changes are the ones that become permanent.	
«Guests can see each other on the network, but that is their business.»	The hotel provides the network and should stop guests' devices reaching each other.	

What is commonly believed	What actually holds	Our position
«Shared folders on our own network do not need passwords.»	They do, because the network may not be as closed as assumed.	
«The audio-visual company knows what it is doing.»	It knows what the event needs. What the hotel's network must not reach is the hotel's decision.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Connecting networks temporarily for an event without recording it.		
Assuming the network still matches its original design.		
Switching off guest isolation and forgetting to switch it on again.		
Leaving shared folders and printers open on the assumption that only staff can reach them.		
Letting suppliers connect their equipment wherever the event requires.		
Never monitoring the network that carries the most strangers.		
Letting marketing, sales, IT and suppliers each own a part of the guest network, and nobody the whole.		

Operative synthesis

- **A hotel's guest network carries strangers every day, and it must reach the internet and nothing else, with each guest invisible to every other. Separation is easy to design and easy to lose, because events, suppliers and convenience keep connecting things. It survives when somebody owns it, every connecting change is recorded and reversed, event networks are provisioned and removed by the hotel, and the network is checked from the guest's side after every change.**
- **The instrument is the network on one page: each network, who uses it, what it can reach, what it must never reach, who owns it and when it was last checked. With a quarterly look from the guest's side, it keeps the hotel's design and the hotel's reality in step.**
- **In Cartagena nothing had been done carelessly. The network had been designed correctly, a technician connected two parts of it for an event that needed it, and an audio-visual company served a demanding conference well. The connection outlived the event by eighteen months, and the first person to notice it was a delegate at a summit on digital fraud.**
- **Which raises the question the next subchapter takes up. Networks can be separated and devices encrypted, but most attacks on hotels begin with a person being persuaded to do something. What happens when a hotel's staff have all completed their security training, and one of them reads a verification code aloud to a stranger on the telephone the following week, 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 2.12. 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.