WORKSHEET 2.10

The Laptop That Left in a Taxi

Subchapter 2.10 · case in the book: Singapore

Count the laptops, tablets and phones that leave your property with your managers every week, and ask your IT provider which of them are encrypted and can be wiped remotely. Every device that is not is one taxi ride away from an incident you will have to explain to guests.

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
Encrypt every laptop, tablet and phone the hotel issues, by default, with keys held by IT.		
Enable remote location, locking and wiping, and test it.		
Reach sensitive lists through the system instead of downloading them.		
Limit exports to the fields the task requires.		
Mark the most sensitive documents as confidential and keep them in the system.		
Give staff one number, answered at any hour, for lost devices, and ask them to call it at once.		
Write short rules for devices taken home, to meetings and to social occasions.		
Check every quarter that every device is encrypted and can be wiped.		

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
«A password on the laptop protects the data.»	A login password stops casual use. Without encryption, the disk can be read by anybody who removes it or starts the laptop another way.	
«Encryption is for finance and IT.»	Any device that leaves the building with guests' or clients' information needs it, and in hotels that is most of them.	
«Downloading a list to work offline is harmless.»	It creates a copy outside every control of the system, on a device that travels.	

What is commonly believed	What actually holds	Our position
«The export takes what it takes.»	Access must be restricted to need. An export should contain only the fields the task requires.	
«It is better to look for the device before reporting it.»	Every hour of delay is an hour in which the device could have been wiped. Report first, search afterwards.	

Common mistakes: a self-check

Mistake (from the book)	Present here?	Action / owner
Encrypting only the devices of departments that asked.		
Relying on a login password to protect an unencrypted disk.		
Downloading full guest and delegate lists to work offline.		
Letting exports include every field by default.		
Leaving remote wiping unconfigured for laptops.		
Searching for a lost device before reporting it.		
Treating the most sensitive documents like any other spreadsheet.		

Operative synthesis

- **Devices that leave a hotel will be lost, and what decides the consequence is whether the information on them can be read. Encryption and remote wiping on every device, sensitive information kept in the systems that protect it, exports limited to what the task needs and losses reported at once turn a lost device from an incident with guests to tell into a recorded event and a replacement to order.**
- **The instrument is a page that lists every kind of device that leaves the building, whether it is encrypted and wipeable, what may be stored on it and whom to call when it is lost, backed by a quarterly report from the IT provider. It is the cheapest page in this volume and one of the most valuable.**
- **In Singapore nothing had been done carelessly. A director of events worked long hours on a demanding summit, took her work with her so that she could keep up, and left her bag in a taxi, as people do. The front office manager who lost his phone the same week was no more careful. His device had been encrypted by default, and hers had not, because nobody had asked.**
- **Which raises the question the next subchapter takes up. Losing a device is one kind of incident; being attacked is another. What happens in the first seventy-two hours after an email arrives on a Friday evening claiming to hold the hotel's guest data, and who in the hotel decides what to do, is the case that follows.**

Action plan for our property

Action	Owner	Due	How we will know it worked

Action	Owner	Due	How we will know it worked

Source: Francesco Dore, The Helm and the Lens, Volume 5a «The Helm», subchapter 2.10. 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.