Objective Evidence in a Business That Runs on Trust

GUIDING QUESTION *Name the three kinds of information in your hotel you would be most reluctant to show an outside auditor. For each, ask how you would prove to anybody, your owner included, that it is protected, without revealing it. If the only answer is «trust us», the protection may be real, but nobody outside the room where it happens can know.*

Property: _____ Completed by: _____ Date: _____

How to use this sheet: work through the five parts with the people who own the process. The text in the left-hand columns comes from the book; the empty columns are for what is true in your property.

1. Verification Pact: what is commonly believed, what actually holds, and your property

What is commonly believed	What actually holds	In our property
«Confidential information cannot be audited.»	The information need not be seen. The control protecting it must be shown to work.	
«A signed statement from the director is evidence.»	It is an assertion by an interested party. Evidence must be verifiable.	
«The auditor is an outsider who must be kept away.»	The certifier is bound by confidentiality and can work under agreed conditions.	
«Few people know about it, so it is safe.»	Secrecy without logging means nobody can tell who has seen it.	
«A confidentiality clause protects data at suppliers.»	It promises silence. It does not give the hotel evidence of protection.	

2. What the standard requires, and what demonstrates it

From Table 4.6.a. The third column of the book (what is method, not requirement) is left out here: write what your property actually holds as evidence.

What is required	What demonstrates it in a confidential area	In our property
Restricted information declared in advance	A note to the certifier listing restricted records and the evidence offered instead	
Adequacy of the audit judged	Agreement with the certifier before the audit on alternative evidence	
Objective evidence	Masked records sampled by the auditor, negative tests, logs, observation	
Data masking	Reports and extracts that show controls without identities	
Logging	Access to sensitive records logged by user, reviewable without names	
Supplier agreements	Right to evidence and audit in contracts with firms receiving guest data	

3. The instrument: Table 4.6.b, Evidence without exposure

The instrument of this subchapter. Agreed with the certification body before the audit, one line for each control in a confidential area.

Control	What cannot be shown	Evidence offered instead	Outcome in Macau
Access to protected guest profiles	Profiles and identities	Negative test with an unauthorised account; rights report with users only	Verified
Allocation of suites on restricted floors	Occupants' names	Ten records chosen by the auditor by date and room, names masked	Verified

Control	What cannot be shown	Evidence offered instead	Outcome in Macau
Viewing of camera recordings	The recordings	Viewing log by user and file reference; interview with both authorised viewers	Verified
List of most sensitive guests	The list	Location, access rights and log of the file	Not verifiable: no log; finding raised
Transport by outside security firm	Names, flights, itineraries	Contract terms; supplier's evidence of protection	Not verifiable: no right to evidence; limitation recorded
Staff confidentiality undertakings	Personal files	Signed undertakings for a sample chosen by staff number	Verified
Incidents involving protected guests	Incident details	Register entries with guest references masked; dates and handling	Verified

The rows above are the book's; the empty rows are for lines your property needs to add.

4. Common mistakes: self-check

Common mistake	Present here? (Yes / Partly / No)	Where we see it
Treating confidential areas as unauditable rather than as needing different evidence.		
Offering signed statements from managers in place of evidence.		
Declaring restrictions on the morning of the audit instead of in advance.		
Designing controls in confidential areas that cannot be demonstrated to anyone.		
Protecting the most sensitive records by secrecy alone, without logging.		
Relying on suppliers' confidentiality clauses without any right to evidence.		
Exposing protected information to the auditor to show good faith.		

5. Action plan

Step from the book / gap found	Action in our property	Owner	Deadline
List the information no outside auditor may see, and the control that protects each.			
Build masked reports and user-level logs so each control can be shown without identities.			
Tell the certifier before each audit what is restricted and what evidence is offered.			
Let the auditor choose samples from masked populations.			
Use negative tests and observation to show controls working.			
Obtain the right to evidence from every supplier that receives protected guests' data.			

Step from the book / gap found	Action in our property	Owner	Deadline
Agree that no guest's name leaves the building in the auditor's notes.			
Treat any control the certifier cannot verify as one the hotel cannot verify either.			

In brief

In a business built on discretion, controls must be demonstrable without revealing what they protect. The hotel lists what cannot be shown, builds masked reports, user-level logs and test procedures into the controls themselves, agrees the evidence with the certifier before the audit, lets the auditor choose samples from masked populations, obtains evidence from suppliers, and keeps guests' names out of the audit. Where a control cannot be evidenced, the hotel treats that as a gap in its own knowledge, not only in the auditor's.

Source: The Helm and the Lens, Volume 5b: The Lens, subchapter 4.6. This sheet does not reproduce the text of the standard; work with your own copy of ISO/IEC 27001:2022 from an authorised source.