



Community Library

ISO 27001 Travel Checklist

What to do before a trip, while you are away, and when you get back.

6

Before you
leave

7

While you are
away

4

When you
return

4

If something
goes wrong

1.0 · 2026-10

itrygg.com

How to use this checklist

A trip takes company information outside the office. Give this list to the traveler. Each step also names the proof your ISO/IEC 27001 program should already be able to show.

1. Hand this to anyone who travels with company information. Work the parts in order: before you leave, while you are away, when you return, and if something goes wrong.
2. The Proof line is the record your program keeps. If you cannot produce it, the task is not done.
3. References point to ISO/IEC 27001:2022 Annex A controls, for example A.7.9.

Before	Away	Return	If lost
Before you go	On the trip	Back at work	The same day

Before you leave

Leave with an approved device, a current copy of your work, and a way to report a problem the same day.

- ☐ Take a company-approved device. Do company work on that device, not on a personal one. A.8.1

Proof: The traveler is on the approved endpoint list, or the exception is recorded.

- ☐ Confirm the device is current before it leaves: updates are installed, malware protection is running, and the screen locks on its own. A.8.1, A.8.7, A.8.8

Proof: Endpoint status dated before the trip.

- ☐ Know which information may travel with you, and which must stay behind. A.5.12, A.5.10

Proof: Classification rules the traveler has acknowledged.

- ☐ Use a sign-in the company can reset. Do not keep the only copy of a password in a note, an email, or an unlocked browser. A.5.17, A.8.5

Proof: Acceptable use acknowledgment covering authentication information.

- ☐ Save company work to the company location so the laptop is not the only copy. A.8.13

Proof: The backup or storage location named in the program.

- ☐ Carry the way to report a lost device the same day: who to call, and what to say. A.5.24, A.6.8

Proof: Incident contact in the travel guidance or the incident procedure.

While you are away

Keep the device with you, lock it when you step away, and use the company path for network and files.

- ☐ Keep the device with you. Do not leave it in a car, an unattended bag, or a room you are not in. A.7.9

Proof: Off-premises rule in the guidance the traveler was given.

- ☐ Lock the screen whenever you step away, including at an airport, a client site, or a hotel desk. A.7.7

Proof: Clear screen rule and the traveler's acknowledgment.

- ☐ Use the company way onto the network. Do not do company work on a network you do not know. A.6.7, A.8.21

Proof: Remote working rule for networks away from the office.

- ☐ Do not hand the device to anyone else, including family, hotel staff, or a client. A.5.10, A.5.15

Proof: Acceptable use rule the traveler has acknowledged.

- ☐ Do not read sensitive information where another person, a camera, or a line of people can see it. A.7.7, A.5.12

Proof: Clear screen rule applied away from the office.

- ☐ Do not plug into an unknown charger, USB stick, or kiosk, and do not install an app just to join a meeting. A.8.1, A.7.10

Proof: Endpoint rule for untrusted media and software.

- ☐ Report a strange sign-in, a missing device, or a request to skip a control the same day. A.6.8, A.5.24

Proof: Event report with the date and the person who reported it.

When you return

Bring the device back onto the company build, and put copies and media back where the program expects them.

- ☐ Reconnect the device and let it catch up: updates, malware protection, and the company build. A.8.1, A.8.8

Proof: Endpoint status dated after the return.

- ☐ If the device was out of your sight, say so, and reset the access your program requires. A.5.17, A.5.18

Proof: Access change, or a note that no gap was reported.

- ☐ Remove copies you no longer need, including downloads and photos of whiteboards or badges. A.8.10, A.5.10

Proof: The deletion rule the traveler followed, or a record that the copies were removed.

- ☐ Put paper and removable media back in the controlled place, or dispose of them the approved way. A.7.10, A.7.14

Proof: Media back in the register, or a disposal record.

If something goes wrong

A lost or tampered device is an incident. Report it, cut off its access, and keep what the investigation needs.

- ☐ Report a lost, stolen, or tampered device as soon as you know, including where you last had it. A.5.24, A.6.8

Proof: Incident record opened the same day.

- ☐ The company removes that device's access and checks what it could reach. A.5.18, A.8.1

Proof: Access removal record tied to the incident.

- ☐ Keep the device and the messages. Do not wipe them until the person who handles incidents says so. A.5.28

Proof: Evidence note on the incident.

- ☐ Name the information that was on the device, tell the people who need to know, and record what will change before the next trip. A.5.26, A.5.27

Proof: Incident update, and the lesson recorded for the next trip.

Want this running in the program, not only on paper?

Trygg keeps the owner, the rule, and the proof in one place, so a trip does not start a search.

[Book a demo](https://itrygg.com/#demo) (itrygg.com/#demo)

[ISO 27001 Preparation Checklist](https://itrygg.com/community/library/iso-27001-preparation-checklist) (itrygg.com/community/library/iso-27001-preparation-checklist)

Portal demos follow a mutual NDA.

isms@itrygg.com

This checklist is guidance, not a substitute for the ISO/IEC 27001:2022 standard. Purchase the standard from ISO or your national standards body. Certification decisions are made only by accredited certification bodies.

© 2026 Trygg, Inc.