



Community Library

ISO 27001 Offboarding Checklist

What to do on the last day, and what to confirm after they are gone.

3

Last day

4

Access

4

Equipment

4

After they
leave

1.0 · 2026-10

itrygg.com

How to use this checklist

A person who leaves can still reach company information until the access, the device, and the copies are closed. Give this list to the people who close that out. Each step also names the proof your ISO/IEC 27001 program should already be able to show.

1. Use this when someone leaves. Work the parts in order: the last day, the access, the equipment and information, and the check after they are gone.
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.6.5.

Last day	Access	Equipment	After
The last day	Same day	What comes back	After they leave

The day they leave

The people who grant access know the last day, the work has a new owner, and confidentiality continues.

- ☐ Tell the people who grant access that the person is leaving, and the last working day. A.6.5

Proof: Notice with the last day and the date it was sent.

- ☐ Name who receives the work, and hand it over before access ends. A.5.14, A.6.5

Proof: Handover note naming the person who receives the work.

- ☐ Remind them which information stays with the company, and that confidentiality continues. A.6.6, A.5.10

Proof: Reminder dated on the last day, and the confidentiality agreement still on file.

Access

Ordinary access, privileged access, and the identity itself stop when the person stops.

- ☐ Remove ordinary access on the last day, or sooner if the departure is immediate. A.5.18, A.5.16

Proof: Access removal record with the accounts and the date.

- ☐ Remove privileged access first, and change any shared secret they knew. A.8.2, A.5.17

Proof: Privileged access removal, and the shared secret change.

- ☐ Disable the company identity so it cannot sign in. A.5.16

Proof: Identity marked disabled, with the date.

- ☐ Check shared mailboxes, shared logins, and vendor accounts that were in their name. A.5.15, A.5.18

Proof: Review of shared and external access tied to the person.

Equipment and information

Devices, badges, paper, and copies come back, or they are removed the approved way.

- ☐ Collect the company device, badge, keys, and removable media. A.5.11, A.8.1
Proof: Return of assets record listing what came back.
- ☐ Remove company information from any personal device that was allowed to hold it. A.8.10, A.5.10
Proof: Confirmation the copies were removed, or the device was wiped.
- ☐ Put returned media back in the controlled place, or dispose of it the approved way. A.7.10, A.7.14
Proof: Media record or disposal record.
- ☐ Take back paper records and tokens. A.5.11
Proof: Those items listed on the return of assets record.

After they are gone

Someone confirms the person is closed out, and the records stay where the program can find them.

- ☐ A manager confirms the person can no longer reach company systems. A.5.18
Proof: Check dated after the last day, with the result.
- ☐ Keep the agreements and the return record for as long as the program requires. A.5.33, A.6.5
Proof: The records stored with a retention date.
- ☐ If access is still open, treat it as an incident and remove it. A.5.24, A.5.18
Proof: Incident record if access was found after the last day, or a note that none was found.
- ☐ Record what the next leaver should do differently, if this one found a gap. A.5.27
Proof: Lesson on the leaver record.

Want a leaver to close in the program, not in someone's memory?

Trygg keeps the access removal, the returned assets, and the proof in one place.

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

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