



Community Library

ISO 27001 Onboarding Checklist

What to do before they start, on the first day, and in the first weeks.

5

Before they
start

5

First day

4

First weeks

4

In the program

1.0 · 2026-10

itrygg.com

How to use this checklist

A new person is new access to company information. Give this list to the people who bring them in. Each step also names the proof your ISO/IEC 27001 program should already be able to show.

1. Use this when someone joins. Work the parts in order: before they start, the first day, the first weeks, and the confirmation that they are in the program.
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.6.1.

Before	Day one	Weeks	Confirmed
Before they start	First day	First weeks	In the program

Before they start

Know who is joining, what they may see, and which device they will use, before the first day.

- ☐ Screen the person to the level the role requires. A.6.1
Proof: Screening record completed before the start date.
- ☐ Put information security responsibilities into the employment terms. A.6.2
Proof: Signed terms that include those responsibilities.
- ☐ Sign the confidentiality agreement before they see company information. A.6.6
Proof: Signed confidentiality or non-disclosure agreement.
- ☐ Name the manager, the role, and the access that role is allowed to have. A.5.15, A.5.18
Proof: Role record and the access approved for it.
- ☐ Decide which device they will use. A.8.1
Proof: The device is on the endpoint list, or the plan to issue one is recorded.

DAY ONE · FIRST DAY

First day

Give the identity, the access, and the device the role needs, and no more.

- ☐ Create the company identity and give only the access the role needs. A.5.16, A.5.18
Proof: Identity record and the access granted, with the date.
- ☐ Give privileged access only when the role requires it, and record who approved it. A.8.2
Proof: Privileged access approval, separate from ordinary access.
- ☐ Issue the device, or confirm the one they will use matches the company build. A.8.1
Proof: Endpoint record tied to the person and the date.
- ☐ Have them acknowledge acceptable use before they use company information. A.5.10
Proof: Signed acceptable use acknowledgment.
- ☐ Show them how to report a security event, and who receives it. A.6.8
Proof: Note that they were shown the reporting path.

First weeks

Train them on the rules, the information they will handle, and what happens if a rule is broken.

- | | |
|--|--------|
| ☐ Complete security awareness training for the role. | A.6.3 |
| Proof: Completion record with the person and the date. | |
| ☐ Show which information they will handle, and how it is classified. | A.5.12 |
| Proof: The classification rules they were shown. | |
| ☐ Add the assets they are responsible for, with an owner on each row. | A.5.9 |
| Proof: Asset register rows tied to the person. | |
| ☐ Tell them what happens if a security rule is broken. | A.6.4 |
| Proof: The disciplinary process is part of the terms they signed. | |

In the program

A manager confirms the access, and the records are stored where the program can find them later.

- ☐ A manager confirms the access still matches the role. A.5.18
Proof: Access check dated after the start, with the manager named.
- ☐ Include them in the next awareness cycle. A.6.3
Proof: The person is on the awareness audience list.
- ☐ Put them on the people record with a start date, so a later leaver check can find them. A.5.16
Proof: People record with the start date.
- ☐ Store the signed terms, confidentiality agreement, and acceptable use where the program keeps them. A.6.2, A.5.33
Proof: The three records stored with dates.

Want a new person to show up in the program, not in a side spreadsheet?

Trygg keeps the person, the access, and the proof in one place.

[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.