What is the principle of least privilege?

1 November 2026 · 4 min read · blogs.iictp.org/what-is-least-privilege

The principle of least privilege says that every person, program and service should have only the access it needs to do its job, and no more. It limits the damage if an account is stolen, a program is compromised or someone makes a mistake.

TL;DR The short version

- Least privilege means every person, program and service gets only the access it needs, and no more.
- It limits the damage from a stolen account, a compromised program or a mistake.
- Start from no access, add only what is needed, and review regularly because access tends to grow; it is a core idea of zero trust.

Read online, listen to it, or change the text size: https://blogs.iictp.org/what-is-least-privilege

Why does it matter?

Access that is not needed is access an attacker can use. If a stolen credential can only read one table, the harm is small. If it can change everything, one mistake or one breach can take down the whole system.

What are examples?

A database account for a reporting tool that can only read. A deployment pipeline that can update one service and not the whole cloud account. A support agent who can see tickets but not payment details. A container that runs without administrator rights.

How do you apply it?

Start with no access and add what is required. Group permissions into roles that match real jobs, avoid shared accounts, and give high-power access only for a limited time and with approval. Prefer short-lived credentials to permanent keys.

How do you keep it from eroding?

Access tends to grow and rarely shrinks. Review who has what on a schedule, remove access when people change roles or leave, and check for unused permissions. Log use of powerful accounts.

How does it relate to zero trust?

It is one of its core ideas. A zero trust design assumes any account could be compromised, so each one’s reach is kept small. See what is zero trust.

> Related credential: Associate Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. NIST. SP 800-53, control AC-6 Least Privilege. csrc.nist.gov.
2. OWASP. Access Control Cheat Sheet. cheatsheetseries.owasp.org.

Published by IICTP, an independent technical credential body, on 1 November 2026. The current version of this post is at https://blogs.iictp.org/what-is-least-privilege. More guides: blogs.iictp.org.