# Gestione delle Identità e degli Accessi (IAM)

La politica IAM regola l'accesso logico ai sistemi aziendali, agli ambienti di produzione cloud e ai repository di codice, garantendo che ogni accesso sia autorizzato, tracciato e limitato.

- **Profilazione:**
  - Adozione rigorosa del principio del **minimo privilegio** (*least privilege*), per cui ogni utente, amministratore o sviluppatore dispone esclusivamente dei permessi necessari allo svolgimento delle proprie mansioni.
  - Categorizzazione dei ruoli in profili standard (es. operatore supporto, sviluppatore, amministratore di sistema/cloud).
- **Assegnazione dei Permessi:**
  - Ogni richiesta di creazione utenza o innalzamento dei privilegi deve essere inoltrata formalmente e approvata dal responsabile tecnico o dal Security Manager.
  - Obbligo di adozione di meccanismi di **autenticazione forte a due fattori (MFA)** per l'accesso agli ambienti cloud critici (es. AWS), ai database dei clienti e ai pannelli di controllo della piattaforma LMS.
- **Revisione Periodica:**
  - Esecuzione di verifiche periodiche (almeno semestrali) sulla matrice dei ruoli IAM e sui privilegi attivi per identificare ed eliminare utenze obsolete, inattive o non più necessarie.
- **Revoca dei Permessi:**
  - Processo di *offboarding* tempestivo: in caso di cessazione del rapporto di lavoro o di cambio di mansione, la disattivazione o la modifica delle credenziali avviene in tempo reale (entro la giornata lavorativa) per impedire accessi non autorizzati.

---

Revision #1
Created 2026-10-19 18:41:10 UTC by Alberto Pastorelli
Updated 2026-10-19 18:41:31 UTC by Alberto Pastorelli