Security Policies - Gestione Operativa e dei Controlli

- Gestione delle Identità e degli Accessi (IAM)
- Gestione della Sicurezza delle Risorse Umane
- Asset Inventory (TBD)

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.

Gestione della Sicurezza delle Risorse Umane

La sicurezza delle risorse umane copre l'intero ciclo di vita del personale (prima, durante e dopo l'impiego) per mitigare i rischi legati a minacce interne o errori umani.

- **Procedure di Selezione e Controlli Preliminari (*Background Checks*):**
  - Durante la fase di recruiting e prima dell'assunzione, vengono effettuate verifiche adeguate e proporzionate al ruolo (es. controllo delle referenze professionali, verifica dei titoli di studio e delle certificazioni dichiarate), nel pieno rispetto della privacy e delle normative vigenti.
- **Accordi di Riservatezza (NDA):**
  - Sottoscrizione obbligatoria di accordi di non divulgazione (NDA) e patti di riservatezza da parte di tutti i dipendenti, collaboratori esterni, consulenti e fornitori.
  - Tali accordi tutelano la proprietà intellettuale, il codice sorgente di *Forma LMS* e le informazioni confidenziali o i dati personali dei clienti gestiti in modalità SaaS.
- **Piano di Formazione e Consapevolezza sulla Sicurezza (*Security Awareness*):**
  - **Onboarding:** Formazione obbligatoria iniziale per tutti i neoassunti sulle politiche di sicurezza aziendali, sull'uso corretto dei dispositivi e sulla gestione delle password.
  - **Aggiornamenti periodici:** Sessioni formative ricorrenti (es. focus su tecniche di phishing, social engineering e protezione dei dati) per mantenere alta l'attenzione del personale.
  - **Test e misurazione:** Campagne periodiche di verifica (es. simulazioni di phishing) per valutare l'efficacia della consapevolezza interna e identificare aree che richiedono ulteriore supporto formativo.

Asset Inventory (TBD)