POLITICHE SPECIFICHE DI DOMINIO

Le **Politiche Specifiche di Dominio** a supporto del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) per **Forma Farm S.r.l.** definiscono le regole operative e i comportamenti richiesti in aree specifiche dell'organizzazione.

Controllo degli Accessi e IAM (Identity and Access Management)

- **Scopo:** Regolare le modalità di profilazione, autorizzazione e gestione delle credenziali per l'accesso ai sistemi aziendali e agli ambienti di produzione cloud.
- **Principi chiave:**
  - Adozione rigorosa del principio del *minimo privilegio* (*least privilege*) per tutti gli operatori e amministratori.
  - Obbligo di utilizzo di meccanismi di autenticazione forte (es. autenticazione a due fattori - MFA) per l'accesso agli ambienti cloud critici, ai server e ai pannelli di controllo della piattaforma LMS.
  - Revisione periodica dei permessi e immediata revoca delle credenziali in caso di cessazione del rapporto di lavoro o cambio di mansione.

Utilizzo dei Dispositivi Mobili e dello Smart Working (Mobile Device & Teleworking Policy)

- **Scopo:** Regolamentare la sicurezza e la protezione delle informazioni aziendali al di fuori del perimetro fisico tradizionale della sede di Via Savona a Milano.
- **Principi chiave:**
  - Obbligo di protezione mediante password robuste, PIN o biometria e cifratura del disco per tutti i dispositivi (notebook, smartphone, tablet) utilizzati per accedere ai sistemi di Forma Farm.
  - Divieto di utilizzo di reti Wi-Fi pubbliche o non protette senza l'uso di una connessione sicura (VPN aziendale).
  - Obbligo di custodire i dispositivi con cura e di segnalare immediatamente eventuali smarrimenti o furti al team tecnico.

Classificazione e Gestione delle Informazioni

- **Scopo:** Stabilire le regole per trattare, etichettare e proteggere i dati e gli asset aziendali (in particolare i dati dei clienti, i contenuti formativi e i codici sorgente dei plugin e di Forma Lms).
- **Principi chiave:**
  - Classificazione delle informazioni in base alla criticità e alla confidenzialità (es. Pubblico, Interno, Confidenziale, Strettamente Confidenziale/Dati Personali GDPR).
  - Regole per la gestione sicura, la conservazione e la distruzione o cancellazione sicura dei dati al termine del ciclo di vita o dei contratti di servizio (*Data Processing Agreement*).

Clean Desk e Clean Screen

- **Scopo:** Garantire la protezione fisica delle informazioni sensibili e dei dati dei clienti sia all'interno degli uffici sia durante il lavoro da remoto, prevenendo accessi non autorizzati o la visualizzazione accidentale di dati critici.

- **Principi chiave:**
  - Obbligo di bloccare lo schermo (*screen lock*) ogni volta che si lascia incustodito il terminale di lavoro.
  - Rimozione e archiviazione sicura di documenti cartacei o supporti di memorizzazione rimovibili dalle scrivanie al termine dell'orario di lavoro o in caso di assenza prolungata.

Sicurezza delle Password e Autenticazione

- **Scopo:** Definire standard robusti di accesso ai sistemi informatici per prevenire violazioni derivanti da credenziali deboli o compromesse.
- **Principi chiave:**
  - Requisiti minimi di complessità per le password (lunghezza minima, uso di caratteri misti, numeri e simboli) o adozione di password manager aziendali approvati.
  - Divieto assoluto di condivisione delle credenziali personali o di scrittura delle password su supporti cartacei non protetti.

Sicurezza dello Sviluppo e delle Operazioni Cloud (Integrazione DevOps / Secure SDLC)

- **Scopo:** Assicurare che la piattaforma *Forma Cloud LMS* e i relativi plugin siano sviluppati, aggiornati e gestiti in sicurezza.
- **Principi chiave:**

- Separazione rigorosa tra gli ambienti di sviluppo, test e produzione.
- Gestione costante delle vulnerabilità e applicazione tempestiva degli aggiornamenti di sicurezza (*Patch Management*) sui componenti open source e sulle infrastrutture cloud.

Revision #1
Created 2026-10-13 09:32:56 UTC by Alberto Pastorelli
Updated 2026-10-13 09:36:29 UTC by Alberto Pastorelli