5.1 Common Best Practice

Si forniscono nel seguito un insieme di raccomandazioni generali 'trasversali' che realizzano la base comune per affrontare le problematiche di sicurezza delle specifiche componenti.

Ogni argomento è strutturato in un paragrafo contenente una o più tabelle.

Ciascuna tabella riporta una problematica di sicurezza, le minacce che possono determinarla o comunque applicabili, e le contromisure generali suggerite per farvi fronte.

5.1.1 Utenze

Registrazione / Cancellazione utenti	
Minaccia	Abuso di privilegi da parte dell'utente.
Contromisure	Definire, per ogni sistema/piattaforma, un processo di registrazione/cancellazione degli utenti ai quali deve essere concesso/revocato un account. Il processo deve prevedere almeno: - l'uso di User ID individuali in modo che gli utenti possano essere resi responsabili delle proprie azioni. L'uso dell'ID di gruppo dovrebbe essere permessa solo per esigenze aziendali od operative previa approvazione e produzione della documentazione di supporto; - la verifica che il livello di accesso richiesto sia in linea con il principio del "need to know"; - l'obbligo di disabilitare o rimuovere immediatamente le UserId degli utenti che hanno cessato il rapporto di lavoro; - la verifica periodica (almeno trimestrale) dell'assenza di account inconsistenti, ridondanti o obsoleti e la loro eliminazione.

Assegnazione e revoca dei diritti di accesso degli utenti	
Minaccia	Abuso di privilegi da parte dell'utente.
Contromisure	Definire un processo che disciplini l'assegnazione e la revoca dei diritti di accesso dell'utente, identificato con UserId personale. L'accesso a ogni sistema/piattaforma da parte di persone fisiche deve essere soggetto a: - autenticazione, in modo univoca attraverso un identificativo personale (es. username o UserId) e credenziali private (es. password, PIN, token); - autorizzazione, nei limiti del principio del need-to-know ovvero attribuire il privilegio minimo necessario per svolgere l'attività lavorativa; - registrazione di tutti i diritti di accesso assegnati al sistema/piattaforma, in un sistema di anagrafica centralizzato. Verificare che il livello di accesso consentito sia coerente con le politiche di accesso e con il principio di separazione dei compiti. - i profili di accesso devono essere costantemente aggiornati; - eventuali deroghe ai criteri di assegnazione/revoca dei diritti di accesso dovrebbero essere limitate, registrate e approvate almeno dai responsabili del sistema/piattaforma e dai responsabili funzionali.

Autorizzazione all'assegnazione dei diritti di accesso privilegiato	
Minaccia	Abuso di privilegi da parte dell'utente.
Contromisure	L'assegnazione dei diritti di accesso privilegiato dovrebbe essere controllata attraverso un processo di autorizzazione che preveda: - l'identificazione dei diritti di accesso privilegiato relativi al sistema/piattaforma e gli utenti a cui è necessario assegnarli; applicazione principio della *segregation of duty* nel processo autorizzativo;