ASL Salerno
Azienda Sanitaria Locale Salerno

POLICY PRIVACY

PER LA GESTIONE DELLE PASSWORD

Rev. 0/2024

Sommario

Glossario

Policy: procedura, ossia insieme di regole di cui l'Azienda si dota al fine di organizzare prestabiliti processi interni.
Password: codice alfanumerico di riconoscimento, che consente di verificare l'identità dell'utente.
Utente, account o user: oggetto del processo di autenticazione.
Autenticazione: processo tramite il quale un sistema informatico, un computer, un software o un utente verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole comunicare attraverso una connessione, autorizzandolo ad usufruire dei relativi servizi associati.
Credenziali: associazione di nome utente (user o account) e password nel processo di autenticazione.
Misure di sicurezza organizzative: tutte le misure volte a conformare l'Azienda al GDPR, rispettando il principio di "*Accountability*", volte alla regolamentazione di processi interni.
Misure di sicurezza tecniche: tutte le metodologie, soprattutto di tipo informatico, che consentono di proteggere il dato personale e mirano a prevenire eventuali violazioni di dati personali.
Tracciabilità: registrazione delle operazioni compiute dall'utente, la quale può avvenire, ad esempio, tramite l'analisi dei *file* di *log* raccolti.

I. Introduzione e Obiettivo della *policy*

L'Azienda sanitaria locale "Salerno" (da adesso in poi: "Azienda") ha adottato la presente policy per l'assegnazione e la gestione delle credenziali di accesso ai sistemi informatici direttamente riferibili al perimetro dell'Azienda, vale a dire a sistemi il cui accesso è mediato dal sistema di autenticazione centrale predisposto dalla UOC SIA(SSO).
Questa politica definisce dunque i requisiti per la creazione, l'uso e la gestione delle password al fine di proteggere i dati sensibili, i sistemi informatici e le reti dell'azienda sanitaria locale.
lle postazioni di lavoro (PC) e, eventualmente, ai software applicativi le cui autorizzazioni di accesso al relativo profilo funzionale saranno fornite dal Soggetto designato al relativo trattamento.
La presente *policy* è stata predisposta per dotare l'Azienda di un'organizzazione strutturale in grado di assicurare la riservatezza delle informazioni aziendali in chiave elettronica.

Le credenziali di accesso sono costituite dallo *user* (o anche *Utente*) che contraddistingue univocamente l'assegnatario, e rimane fisso per tutta la durata del rapporto giuridico. Per "*password*" deve intendersi la sigla di riconoscimento fornita dall'utente all'elaboratore al fine di accedere ad un sistema operativo (PC/Server/Workstation), ad un software applicativo o ad un file. Dunque, le *credenziali di accesso* permettono la protezione delle informazioni e, in particolare, si utilizzano nelle fasi di autenticazione e per proteggere i contenuti di archivi informatici.
La *Password* è soggetta a scadenza, e deve essere modificata secondo le modalità appresso indicate.
La *password policy* per la gestione delle *password* rappresenta un insieme di norme comportamentali volte a conformare l'Azienda ai principi di diligenza e correttezza ed a sensibilizzare e responsabilizzarne i dipendenti.
Infatti, una corretta gestione delle *password* ha come diretta conseguenza una riduzione dei rischi derivanti da un accesso non autorizzato, una modifica indesiderata o perdita, anche accidentale, dei dati personali e/o aziendali.
Invero, in assenza di una *password policy* si rende altamente probabile l'intrusione di utenti non autorizzati con la conseguente acquisizione di informazioni che potrebbero causare un grave danno all'Azienda, configurando così un vero e proprio *data breach* nel caso della presenza di dati personali.
Tali misure trovano la loro fonte negli artt. 24, 25 e 32 del Regolamento Generale Europeo sulla protezione dei dati personali n. 679 del 2016 (GDPR), all'interno dei quali si sottolinea la necessità della previsione di misure di sicurezza "*tecniche e organizzative*" adeguate, con l'intento di prevenire un'eventuale violazione dei dati personali (*data breach*).
L'adozione della presente *policy* rientra tra le misure di sicurezza organizzative che devono essere implementate dal Titolare del trattamento; la gestione delle *password* rientra, di converso, tra le misure di sicurezza tecniche che il Titolare intende adottare per garantire la sicurezza dei dati personali contenuti all'interno di documenti digitali, ai sensi e per gli effetti dell'art 32 GDPR.

In un contesto aziendale, la conservazione della maggior parte dei documenti digitali avviene all'interno di archivi protetti da *password.*
La sicurezza di questi documenti è garantita, dunque, dalla predisposizione di regole chiarificatrici sulle modalità di creazione e di utilizzo delle *password* con cui accedere a tali archivi.
La tutela degli archivi digitali deve inoltre procedere parallelamente con la tutela dei locali all'interno dei quali sono collocati *server* e *database*, nonché

delle *workstation*, rendendosi quindi necessario per l'Azienda estendere l'applicazione di tali regole alla gestione delle modalità di accesso a tali archivi. Pertanto, la policy *password* è rivolta a tutti quei soggetti che, a qualunque titolo, devono utilizzare le *password* di accesso per diverse finalità, quali ad esempio la consultazione di documentazione contenuta negli archivi digitali, ovvero l'accesso alle postazioni di lavoro o ai servizi applicativi aziendali.
In tal senso, un'adeguata *policy* permette, da un lato, un'operatività organizzata ed efficiente nello svolgimento delle attività di competenza dell'Azienda e, dall'altro lato, garantisce una più adeguata protezione e controllo dei dati particolari trattati dal personale, in particolare, e una maggiore protezione degli *assets* aziendali dell'Azienda, in generale.

II. Modalità operative

L'Azienda sanitaria locale Salerno, ai fini della corretta messa in *compliance*, stabilisce le politiche di creazione e gestione delle *credenziali di accesso* con l'intento di minimizzare il rischio di *malpractices* aziendali e rendere più sicuro e responsabilizzato il controllo.
Fermo restando quanto specificato nella Introduzione (Par.I), le credenziali di accesso (*user* e *password*) sono assegnate dalla UOC Servizio Informativo Aziendale (UOC SIA), secondo i seguenti criteri:

- **Assegnazione delle credenziali personali ai dipendenti per l'accesso alla postazione di lavoro (PC) e ai servizi applicativi**.
  La UOC ove il dipendente prende servizio, comunica alla UOC SIA**,** secondo le modalità convenute, i dati anagrafici del dipendente (o personale convenzionato), compreso di matricola, codice fiscale e numero di telefono mobile (i dati sono trattati con riservatezza dal personale della UOC SIA).
  La UOC SIA, verificata la completezza delle informazioni, provvede a comunicare all'interessato le credenziali personali di accesso, con password di primo accesso, utilizzabile esclusivamente per consentirne la personalizzazione (cambio password).
  Con l'attivazione delle credenziali, il Dipendente viene automaticamente abilitato d'ufficio all'accesso, oltre che a tutti i PC attestati nel dominio aziendale (aslsalerno.local), ai seguenti servizi applicativi on line:
  - Gestione Password (per modificare/resettare la password);
  - Help desk (per la richiesta di assistenza informatica);
  - Portale del Dipendente (per la gestione del cartellino delle Presenze e visualizzazione cedolini Paga/CU);
  - Indirizzo di Posta elettronica aziendale;

- Navigazione Internet (Siti istituzionali).

Nel caso di rapporto di lavoro a tempo determinato, viene impostata una scadenza sull'*account,* che corrisponde al decimo 10 giorno successivo all'ultimo giorno lavorativo, in modo da disattivarlo in automatico.

Per quanto attiene alla cessazione degli *account* del personale a tempo indeterminato, la UOC GRU comunica mensilmente alla UOC SIA l'elenco del personale in via di dimissione programmata nei mesi successivi a quello in corso, indicando per ogni dimesso: Cognome, Nome, Matricola e data di cessazione. L'*account* viene disattivato il decimo giorno successivo alla fine del rapporto di lavoro, ivi compreso l'indirizzo di posta elettronica aziendale.

- **Assegnazione delle credenziali alle Ditte per attività di assistenza e manutenzione sui sistemi forniti.** Al personale delle ditte che operano a vario titolo con l'Azienda, viene rilasciato un *account* necessario per l'accesso (anche da remoto in VPN, se necessario) ai sistemi forniti per assistenza, manutenzione e supporto. Su questi *account* è impostata una scadenza che corrisponde alla fine del contratto.

  Il DEC del relativo contratto comunica alla UOC SIA, secondo le modalità convenute, i dati della ditta a cui assegnare le suddette credenziali.
- **Scadenza password.** La password ha una validità massima di 90 giorni. Entro questo termine, l'assegnatario deve provvedere a modificarla.

  L'assegnatario viene avvisato, mediante SMS, 7 giorni prima della scadenza. Nei 30 giorni successivi, l'utente può ancora resettarla, in autonomia, mediante l'applicazione web di Gestione password.

  Trascorso inutilmente anche questo termine, l'account viene disattivato.
- **Disattivazione delle credenziali di accesso.** L'account viene disattivato, oltre per quanto specificato al punto precedente, qualora l'utente assegnatario perda il ruolo, la mansione o la qualità che giustifica l'accesso e l'utilizzo dei servizi o, infine, su iniziativa della UOC SIA per ragioni di cybersicurezza. In questa ultima circostanza la UOC SIA provvede ad avvisare tempestivamente l'assegnatario.

  In caso di necessità di riattivazione (sblocco) di un account disattivato, sarà necessario che il direttore della UOC a cui appartiene il dipendente assegnatario produca formale richiesta alla UOC SIA, secondo le modalità convenute.

III. Responsabilità dell'Utente/Operatore

La presente *policy password* prevede anche delle responsabilità riconducibili direttamente all'utente/operatore (assegnatario delle credenziali di accesso).

Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account. Le *password* sono delle chiavi di accesso riservate che, in quanto tali, devono essere conosciute solo dall'utente assegnatario.
A tale riguardo, è fatto divieto di:

- comunicare la propria *password* ad altri. Difatti, la *password* deve essere nota esclusivamente all'utente e da quest'ultimo non divulgata ad altri soggetti;
- scrivere le proprie *password* su foglietti, documenti cartacei o *file* conservati all'interno delle postazioni di lavoro e lasciarle incustodite;
- digitare la *password* al posto dell'*user* in quanto, in tal caso, rimane registrata nei *log* dei sistemi;
- salvare le *password* direttamente nel *browser*. Se qualcuno ha accesso al PC, ha automaticamente accesso alle altre risorse pur non conoscendone direttamente le credenziali di accesso;
- non chiudere le sessioni di connessione in modo forzato, ed utilizzare la funzione di logout.

La UOC SIA applica le regole di composizione e di complessità delle password previste dai regolamenti AgID.

IV. Revisione della policy

La presente *policy* viene revisionata in ragione della variazione della normativa di riferimento in materia.