Password Policy

La gestione delle credenziali di accesso (elettroniche e meccaniche)

Rif. Regolamento UE 2016/679 (GDPR)

Titolare del Trattamento	Diocesi di Sabina – Poggio Mirteto (RI)
Indirizzo sede legale	Piazza Mario Dottori, 14 – 02047 Poggio Mirteto (RI)
Codice Fiscale	91000810571
PEO	diocesi@diocesisabina.it
Responsabile	S.E. Mons. Ernesto MANDARA
DPO	Giuliano PALOTTO

Edizione	Revisione	Data	Descrizione	il Titolare	il DPO
1	0	04/03/2024	Prima emissione	*approvato*	*verificato*

Documento di nr 5 pagine compresa la presente realizzato su format della

1 PREMESSA

La protezione delle credenziali di accesso elettroniche (password) e/o meccaniche (chiave) rappresenta uno dei principi fondamentali della sicurezza delle informazioni, in particolare la creazione e la gestione delle password che costituiscono la principale contromisura agli accessi non autorizzati.
Visto quanto previsto dall'attuale codice in materia di protezione dei dati personali – ex D.Lgs. 196/03 – e, successivamente, ripreso dal nuovo regolamento europeo 2016/679 in vigore dal 24/05/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - GDPR, occorre definire misure di protezione adeguate ed idonee per il trattamento e la tutela dei dati personali degli utenti.

2 SCOPO

Il presente documento ha lo scopo di definire una procedura - la password policy del Titolare del trattamento - che stabilisca i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione fornite agli utenti che siano autorizzati a consultare, modificare, trasmettere, cancellare ovvero compiere qualsivoglia attività di trattamento di dati personali e che agiscano nell'ambito dell'autorità che gli viene concessa (incaricati al trattamento – rif. Art. 29 GDPR) e agli utenti identificati quali responsabili del trattamento (rif. art. 28 GDPR).
In generale, l'Amministratore di Sistema del Titolare del trattamento individua, come strumento di accesso per gli utenti, un sistema di autenticazione (e di autorizzazione) basato su credenziali di accesso. Esso consiste in un codice per l'identificazione dell'utente ("username" o "nome utente"), associato ad una parola chiave riservata ("password") conosciuta esclusivamente dal solo utente. I due elementi, uniti insieme, costituiscono la credenziale di accesso ("account" o "utenza") così come definito dalla normativa vigente in materia di dati personali.
Parimenti, il documento ha lo scopo di definire una procedura che stabilisca i criteri per la gestione delle chiavi di chiusura degli accessi (block security) agli archivi contenenti dati personali.

3 GESTIONE PASSWORD ELETTRONICHE

3.1 CAMPO DI APPLICAZIONE

La password policy (elettronica) si applica a tutti i servizi informatici centrali, gestionali ed applicativi, compresi quelli web, alle postazioni di lavoro, alla rete wi-fi, al servizio di posta elettronica e a tutte le applicazioni e risorse informatiche presenti che prevedono un sistema di autenticazione per l'accesso, ivi compresi i sistemi e le risorse informatiche presenti in eventuali strutture decentrate.

3.2 RESPONSABILITÀ DEGLI AMMINISTRATORI DI SISTEMA

Gli amministratori di sistema devono proteggere la riservatezza e l'integrità delle password sui sistemi da loro gestiti e configurare i servizi informatici, forzando l'applicazione ove tecnicamente possibile, per soddisfare i requisiti della presente password policy.
Lo username viene assegnato, salvo diverso avviso, esclusivamente dall'amministratore del servizio (o amministratore del sistema) o da un suo delegato. La password viene gestita, dopo la sua prima assegnazione da parte dell'amministratore, esclusivamente dall'utente, con l'eccezione dei casi in cui ricorrano necessità di carattere tecnico-organizzative.
Il codice identificativo, una volta assegnato ad un utente, non potrà più essere riassegnato ad altri soggetti, nemmeno in tempi successivi, proprio per poter garantire un'archiviazione e storicizzazione delle utenze (come riportato dalla normativa vigente in tema di dati personali).
Le credenziali di accesso non utilizzate da almeno **6 (sei) mesi** dovranno essere disattivate (a meno che non siano state preventivamente autorizzate quali credenziali per soli scopi di gestione tecnica, che prevedono pertanto periodi di inattività anche più lunghi del semestre). Le credenziali devono essere disattivate anche quando l'utente perde il ruolo, la mansione e le qualità che gli consentono di utilizzarle per accedere ai vari servizi (es. cessazione del rapporto di lavoro, trasferimento, demansionamento, licenziamento, sostituzione, pensionamento, ecc.).
Laddove vi sia la ragionevole certezza che l'utenza sia stata utilizzata da persona diversa dal titolare, la stessa dovrà essere cambiata immediatamente dall'utente. In caso di inerzia, tale cambio verrà disposto direttamente dall'amministratore del sistema.

Le password di default - *come quelle create per i nuovi utenti o assegnate dopo una reimpostazione della password* - devono poter essere cambiate dall'utente al primo accesso. Se tecnicamente possibile, tale cambio password deve essere imposto all'utente dal sistema.

3.3 RESPONSABILITÀ DEGLI UTENTI

Gli utenti (responsabili e incaricati al trattamento) si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso di seguito indicati.
Gli utenti, una volta in possesso delle credenziali, devono cambiare la password al primo accesso rispettando i criteri di seguito descritti, evitando – per quanto possibile – combinazioni facili da identificare. Devono scegliere password univoche, che abbiano un senso solo per l'utente che le sceglie, evitando – per quanto possibile – di usare la stessa password per altre utenze.
La password è strettamente personale e non deve essere comunicata e/o condivisa (per nessun motivo) con altre persone all'interno dell'organizzazione, compresi borsisti, assegnisti, collaboratori, consulenti, ecc.
Gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, a rispondere ad e-mail sospette e/o a cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto d'identità, ecc.).
Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account.
Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà cambiare immediatamente la password.
Per la conservazione sicura delle credenziali di accesso è consigliabile usare un software di gestione delle password (es. KeePass, LastPass, ecc.) installato su un dispositivo diverso da quelli utilizzati per lavoro, evitando di memorizzarle su fogli di carta, documenti cartacei e file conservati all'interno della postazione di lavoro. Tali software permettono anche di automatizzare il processo di login alle varie applicazioni usate.
Qualora l'utenza venga bloccata a seguito della scadenza della password oppure sia necessario modificare la password perché dimenticata o per altra motivazione, l'utente deve prediligere l'utilizzo di servizi self-service di reimpostazione o di cambio password oppure (ove non disponibili) contattare l'amministratore di sistema.

3.4 REQUISITI TECNICI PER LA CREAZIONE E GESTIONE DELLE PASSWORD

Come regola generale, la password deve essere ragionevolmente complessa e difficile da individuare e/o ricavare. Le password, a seconda di lunghezza e complessità, possono essere considerate:

- deboli (password riconducibili all'utente, corte, memonicamente facili da ricordare – es. 1234)
- medie (password alfanumeriche riconducibili all'utente)
- forti (password non riconducibili ai primi due casi)

Si consiglia che, nei limiti tecnici consentiti dai sistemi, la password:

a. deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui il sistema non lo dovesse prevedere, di lunghezza pari al massimo consentito;
b. deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni 6 (sei) mesi;
c. deve contenere, ove possibile, almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali (es. S@p13nZa);
d. deve essere sempre diversa da almeno le ultime 4 precedentemente utilizzate;
e. non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti;
f. deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata a terzi;
g. non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
h. non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere) o che si riferiscano ad informazioni personali;
i. non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

Ove tecnicamente possibile, i requisiti di cui ai punti da a) a e) compresi devono essere imposti da meccanismi automatici del sistema.

Se la password fornisce accesso ad archivi elettronici contenenti dati a carattere speciale c.d. sensibili (art. 9) o giudiziari (art. 10) deve essere considerata FORTE ovvero doppia password non FORTE.
Per motivate necessità di urgente accesso alle informazioni, in caso di impedimento del titolare delle credenziali (utente), la password può essere annullata e sostituita dagli amministratori di sistema con una nuova password tramite istanza scritta dell'utente all'amministratore di sistema.
In questo caso la nuova password dovrà essere consegnata dall'amministratore di sistema all'utente, il quale dovrà modificarla al primo accesso.

4 GESTIONE PASSWORD MECCANICHE

4.1 CAMPO DI APPLICAZIONE

La password policy (meccanica) si applica a tutti gli archivi contenenti dati personali in formato cartaceo quali, a titolo meramente indicativo e non esaustivo: magazzini, archivi, uffici, armadi, cassettiere, casseforti, ecc., ivi compresi gli archivi presenti in eventuali strutture decentrate.

4.2 RESPONSABILITÀ DEL GESTORE DELLE CHIAVI

Il gestore delle chiavi (il legale rappresentante del Titolare del trattamento o suo delegato) deve proteggere la riservatezza e l'integrità delle password meccaniche, forzando l'applicazione ove tecnicamente possibile, per soddisfare i requisiti della presente password policy.
La chiave viene assegnata a uno o più utenti in forza delle mansioni assegnate, ai responsabili del trattamento "esterni" (es. impresa di pulizie, manutenzione, fornitori di servizi), trattenendo la "madre" in un apposito luogo fisico identificato come "archivio delle chiavi" protetto da sistema antintrusione (es. cassaforte, impianto di allarme, guardiania presidiata, ecc.).
La chiave deve essere disattivata (sostituzione della serratura) quando l'utente perde il ruolo, la mansione e le qualità che gli consentono di utilizzarle per accedere ai vari servizi (es. cessazione del rapporto di lavoro, trasferimento, demansionamento, licenziamento, sostituzione, pensionamento, ecc.), fatto salvo la certezza (c.d. oltre ogni ragionevole dubbio) che l'utente non abbia provveduto a farne copia.
Laddove vi sia la ragionevole certezza che la chiave sia stata utilizzata da persona diversa dall'utente, la stessa dovrà essere sostituita immediatamente.

4.3 RESPONSABILITÀ DEGLI UTENTI

Gli utenti (responsabili e incaricati al trattamento) si impegnano a rispettare i criteri di conservazione e gestione delle chiavi di accesso di seguito indicati.
Gli utenti, una volta in possesso delle chiavi, devono conservarle in modo da evitare usura eccessiva, in un luogo ove sia ridotta al minimo la possibilità di perdita, smarrimento o furto.
La chiave è strettamente personale e non deve essere condivisa (per nessun motivo) con persone terze all'interno dell'organizzazione che non hanno accesso ad archivi non presidiati, compresi borsisti, assegnisti, collaboratori, consulenti, ecc.
Ogni utente è responsabile di tutte le azioni e le funzioni svolte dalla chiave.
Qualora vi sia la ragionevole certezza che le chiavi assegnate siano state utilizzate da terzi non autorizzati, l'utente dovrà darne comunicazione, senza indugio, al Gestore delle chiavi e al Titolare del trattamento.
L'accesso ad archivi cartacei contenenti dati a carattere speciale c.d. sensibili (art. 9) o giudiziari (art. 10) deve essere consentito tramite doppia chiave, ovvero accesso tramite chiave e disinserimento di sistema antintrusione (c.d. accesso FORTE).

Sommario