PASSWORD POLICY ENEA
La gestione delle credenziali di accesso

Obiettivi generali

La protezione delle credenziali di accesso 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 - D.Lgs. 196/03 - e, successivamente, ripreso dal nuovo regolamento europeo in vigore dal 24/05/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - GDPR UE 2016/679, occorre definire misure di protezione adeguate ed idonee per il trattamento e la tutela dei dati personali degli utenti.

Il presente documento ha lo scopo di definire una procedura - la password policy di ENEA - che stabilisca i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione fornite agli utenti della comunità accademica per l'accesso ai servizi informatici erogati.

In generale, i servizi informatici presenti in ENEA individuano, 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 tema di dati personali.

Campo di Applicazione

La password policy 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 in ENEA che prevedono un sistema di autenticazione per l'accesso.

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.

Lo *username* , 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 di ENEA (es. cessazione del rapporto di lavoro, trasferimento, demansionamento, licenziamento, sostituzione, 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.

Responsabilità degli utenti

Gli utenti 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 combinazioni facili da identificare. Devono scegliere password univoche, che abbiano un senso solo per l'utente che le sceglie, evitando di usare la stessa password per altre utenze.

La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona 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.

Qualora l'utenza venga bloccata a seguito della scadenza della password oppure sia necessario modificare la password perché dimenticata ovvero a fronte di qualsiasi altra motivazione, l'utente deve utilizzare i servizi self-service di reimpostazione o di cambio password messi a disposizione dal sistema oppure (ove non disponibili) contattare il servizio di assistenza tecnica o l'amministratore di sistema.

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.

Nei limiti tecnici consentiti dai sistemi, la password:

1. 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;
2. deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni 6 (sei) mesi;
3. deve contenere, ove possibile, almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali;

4. deve essere sempre diversa da almeno le ultime 4 precedentemente utilizzate;
5. non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti;
6. deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri;
7. non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
8. 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;

Ove tecnicamente possibile, i requisiti di cui ai punti da 1) a 5) devono essere imposti da meccanismi automatici del sistema.

Per motivate necessità di urgente accesso alle informazioni, in caso di impedimento del titolare delle credenziali, la password può essere annullata e sostituita dagli amministratori di sistema con una nuova password.
In questo caso la nuova password dovrà essere consegnata dall'amministratore di sistema all'utente, il quale dovrà modificarla al primo accesso.