POLICY

GESTIONE DELLE PASSWORD

COD. C.19

CONTIENE:

1. POLICY

PREMESSA

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. n. 196/2003 - 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 dell'Istituzione Scolastica - che stabilisca i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione fornite agli utenti della scuola per l'accesso ai servizi informatici erogati.

CREAZIONE ACCOUNT

In occasione dell'avvio del rapporto di lavoro e/o di collaborazione, saranno fornite al collaboratore delle credenziali per entrare nell'account di posta elettronica e nei diversi sistemi quali, ad esempio, registro elettronico, sistema di didattica a distanza, sistemi di *conference call* creati appositamente utilizzando i dati anagrafici dello stesso (nome e cognome, di solito). Creato l'account, sarà necessario fornire delle chiavi di ingresso al collaboratore. I collaboratori devono essere espressamente invitati a modificare le credenziali di accesso, e in particolare la password, contestualmente al primo log in, in modo da evitare possibili accessi abusivi.
Per quanto attiene la creazione e la gestione dell'account di posta elettronica si rinvia alla apposita policy del Sistema di Gestione EUservice.

RESPONSABILITÀ DEGLI AMMINISTRATORI DI SISTEMA

Gli amministratori di sistema, ovvero in loro luogo assistenti tecnici, 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/credenziale utente, 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 dell'Ateneo (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.

REQUISITI PASSWORD

La password deve necessariamente rispettare tutti i seguenti requisiti di forma:

1) deve essere di lunghezza non inferiore a otto 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 tre caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali
4) deve essere sempre diversa da almeno le ultime quattro 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
9) ove consentito dal sistema è necessario fruire dell'autenticazione a due fattori, a rafforzamento della password semplice

La password dovrà essere necessariamente modificata il giorno 15 gennaio ed il giorno 15 luglio di ogni anno. La verifica di tale adempimento spetterà all'amministratore di sistema o in suo luogo all'assistente tecnico.

CUSTODIA PASSWORD

Il personale è tenuto a custodire la password in luoghi lontani dal terminale e a non comunicarla a nessuno. È espressamente vietato l'utilizzo di fogliettini adesivi nei pressi del terminale con indicazione delle credenziali. Allo stesso modo, pur essendo consentito scrivere la password su supporti cartacei e/o elettronici, è fatto espresso divieto di annotare affianco alla password informazioni tali da permettere ad un malintenzionato di risalire al fatto che tale password è quella utilizzata per l'accesso ai sistemi della scuola.

ESEMPIO: È POSSIBILE ANNOTARE "PASSWORD XXXXXXX" MENTRE È VIETATO SCRIVERE "PASSWORD DOCENTE TIZIO DELLA SCUOLA ALPHA".

La password non dovrà essere condivisa con gli altri colleghi. Solo nel caso di necessità potrà essere condivisa con il proprio responsabile.
Gli utenti devono prestare attenzione a fornire le proprie credenziali di accesso, a rispondere a email sospette e/o a cliccare sui link durante la navigazione web (o nelle 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.

ELIMINAZIONE PASSWORD

Le credenziali di accesso ad un profilo utente sono disabilitate ed eliminate, oltreché per i casi di cui sopra, contestualmente alla cessazione del rapporto. Per la gestione degli account mail si rinvia alla relativa policy. Nel caso di malattia o maternità, il profilo verrà messo in "stand by" sino alla ripresa dell'attività lavorativa.