POLITICA DI GESTIONE DELLE PASSWORD

Approvazione
Data: **03/11/2021**
Dirigente ASI: **Dott.ssa Francesca Pruneti**
Firmato digitalmente ai sensi del D.Lgs. n. 82/2005

Informazioni sul documento		
Redazione a cura di: *U.O. Sicurezza IT*	**Destinatari:** *Chiunque debba utilizzare delle credenziali o realizzare dei sistemi di autenticazione ai servizi dell'Università di Parma*	**Deposito del documento:** *www.unipr.it/regolamento-sicurezza-IT*

Sommario

1. Scopo del documento

Lo scopo di questo documento è definire una politica che permetta di comprendere i criteri e le accortezze necessari per creare e gestire delle password non facilmente ricavabili da una persona terza o programmi preposti a forzare le credenziali.

2. Ambito di applicazione

Questa politica si applica sia agli utenti che devono utilizzare le credenziali loro assegnate per accedere a strumenti e servizi che trattano i dati dell'Università di Parma, sia a chi deve realizzare e gestire dei sistemi di autenticazione (federati o meno) in Ateneo,

3. Regole di composizione e gestione delle password

Tipo di regola	Contenuto regola
Obbligatoria	La password deve contenere almeno 8 caratteri. La password deve contenere i seguenti tipi di caratteri: • Lettere minuscole da a alla z; • Lettere maiuscole dalla A alla Z; • Numeri da 0 a 9; • Caratteri speciali (es. !, $, #, ^, %,*,ecc.). La password deve contenere almeno un numero, una lettera maiuscola e un carattere speciale. La password deve essere modificata entro 90 giorni. La password deve essere diversa dalle password utilizzate nell'ultimo anno. La password non deve essere riconducibile all'identità del titolare dell'account. La password non deve contenere più di due caratteri consecutivi del nome utente.
Obbligatoria	Le password non devono essere condivise con nessuno, nemmeno con assistenti amministrativi, segretari, colleghi e familiari.
Obbligatoria	Le password non devono essere inserite nei messaggi di posta elettronica o in altre forme di comunicazione elettronica insieme al nome dell'utente o a qualsiasi altra informazione relativa al servizio (es. sito di accesso al servizio).
Obbligatoria	Le password non devono essere annotate e memorizzate in nessun posto all'interno del luogo di lavoro.
Obbligatoria	Le password non devono essere memorizzate in un file su un sistema informatico o su dispositivi mobili (es. telefono, tablet) senza crittografia.
Obbligatoria	La funzione «Ricorda la password» delle applicazioni (es. browser web) non deve essere utilizzata se non con programmi di gestione avanzati che utilizzano sistemi di crittografia forte.

Obbligatoria	Gli account con privilegi da amministratore devono avere una password diversa dagli account standard e devono prevedere almeno l'autenticazione a due fattori.
Consigliata	Si raccomanda di **non utilizzare la stessa password** dell'utenza federata di Ateneo (IDEM) **per altri account** non federati o esterni.
Consigliata	Si raccomanda di non utilizzare password contenenti **informazioni personali**, in quanto sono facili da indovinare o scoprire (ad es. numero di telefono dell'utente, nome, compleanno dei figli, anniversari etc.)
Consigliata	Si raccomanda di non utilizzare parole di uso comune, o contenute in un dizionario, perché possono essere facilmente indovinate.
Consigliata	Se si sospetta che una password non sia più sicura o affidabile, deve essere cambiata immediatamente.
Consigliata	Le password devono essere bloccate dopo 5 tentativi sbagliati nell'arco di tempo di 10 minuti. Dopo 40 false inserzioni nell'arco di 24 ore, le credenziali possono essere sbloccate solo contattando il gestore (es. Help Desk Informatico).

Revisioni del documento

Ver.	Descrizione modifiche	Autore	Data modifica
1.0	*Versione iniziale*	*U.O. Sicurezza IT*	*16/06/2021*