POLITICA PASSWORD

SCOPO

Tutti i dipendenti ed il personale che ha accesso ai computer dell'organizzazione devono rispettare i criteri di password definiti nella seguente politica, al fine di proteggere:

- ✓ la sicurezza della rete
- ✓ l'integrità dei dati
- ✓ i sistemi informatici.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutte le persone che hanno un account che richiede una password su un computer collegato alla rete dell'organizzazione (Es. account di dominio, account di posta elettronica, etc.).

MODALITÀ OPERATIVE

Questa politica è stata definita per proteggere le risorse organizzative della rete mediante la richiesta di password complesse unitamente alla protezione di queste password e nello stabilire un tempo minimo tra le modifiche delle password.

Protezione della Password

- **a)** Non annotare mai la password.
- **b)** Non inviare mai una password tramite e-mail.
- **c)** Non includere una password documento archiviato non-crittografato.
- **d)** Non dire mai a nessuno la tua password.
- **e)** Non rivelare la propria password al telefono.
- **f)** Non accennare mai al formato della password.
- **g)** Non rivelare o suggerire la propria password in un modulo in internet.
- **h)** Non utilizzare mai l'opzione "ricorda password", di programmi come internet explorer, di posta elettronica, o qualsiasi altro programma.
- **i)** Non utilizzare mai la password personale dell'organizzazione o di rete per un account internet, che non dispone di un accesso protetto (dove l'indirizzo browser web inizia con https:// invece di http:/).
- **j)** Segnalare eventuali sospetti concernenti la sicurezza della password al reparto/incaricato della sicurezza it.
- **k)** Se qualcuno ti chiede la password, indirizzali al reparto/incaricato di sicurezza it.
- **l)** Non usare acronimi comuni come parte della password.
- **m)** Non usare parole comuni o invertire l'ortografia delle parole come parte della password.
- **n)** Non utilizzare nomi di persone o luoghi, come parte della password.

o) Non utilizzare una parte del tuo nome utente per la tua password.

p) Non utilizzare parti di numeri facili da ricordare, come numeri di telefono, numeri di indirizzo o altro di similare .

q) Stare attenti a lasciare che qualcuno veda la digitazione della password.

Requisiti di Password (soggetto a variazioni)

Coloro che fissano i requisiti di password devono ricordare che rendere queste regole troppo difficili può effettivamente diminuire la sicurezza: gli utenti possono decidere che sono impossibili da soddisfare o, se le password sono cambiate troppo spesso, gli utenti tendono ad annotarle o rendere la loro nuova password una variante di una vecchia, cosa che la renderebbe più vulnerabile ad un attacco. I seguenti requisiti di password verranno impostati dal reparto/incaricato di sicurezza IT:

- ✓ Lunghezza Minima → 8 caratteri raccomandato
- ✓ Lunghezza Massima → 14 caratteri
- ✓ Minimo livello di complessità → Nessuna parola del dizionario. Ciascuna password deve includere tre o quattro dei seguenti tipi di caratteri:
  - Minuscole
  - Maiuscole
  - Numeri
  - caratteri Speciali, ad esempio !@#$%^&*(){}[]
- ✓ le Password differenziano tra maiuscole e minuscole, mentre il nome utente o l'ID di accesso no.
- ✓ Ripetizione Password → numero min. di password prima che una vecchia password possa essere riutilizzata: questo numero non deve essere inferiore a 24.
- ✓ Validità Massima password → 180 giorni.
- ✓ Validità Minima password → 2 giorni.
- ✓ Memorizzare le password tramite crittografia reversibile → Questo non dovrebbe essere fatto senza una speciale autorizzazione da parte del reparto/incaricato IT, dato che ne ridurrebbe il livello di protezione.
- ✓ Soglia di blocco degli Account → 4 tentativi di login falliti.
- ✓ Reset blocco account → Il tempo che intercorre tra tentativi di accesso non valido e la possibilità di ritentare: il valore raccomandato è di 20 minuti. Questo significa che se ci sono tre tentativi non validi in 20 minuti, l'account verrà bloccato.
- ✓ Account durata di blocco → Alcuni esperti raccomandano che il blocco dell'account sia compreso tra 30 minuti e 2 ore.
- ✓ Uno Screen saver protetto da Password dovrebbe essere attivato e dovrebbe proteggere il computer entro 5 minuti di inattività dell'utente. Il computer non dovrebbe essere lasciato incustodito mentre è connesso (logged-on) e senza aver attivato uno screen saver protetto da password. Gli utenti dovrebbero avere l'abitudine di non lasciare i loro computer sbloccati; per facilitarne il compito si può impostare una combinazione rapida di tasti (es. CTRL-ALT-CANC e selezionare “Blocca Computer“).
- ✓ Le regole che si applicano per le password, sono applicate anche alle frasi che vengono utilizzate per l’autenticazione della chiave pubblica/privata

Scelta della Password
In primo luogo bisogna essere sicuri che la password soddisfi i requisiti minimi delle linee guida sopra citate, di seguito sono elencati alcuni suggerimenti per la creazione di una nuova password:

- ✓ Incorporare una parola o parte di una parola all'interno di un altra. ***Es.*** Mare + sabbia. Password: "Marebbia".
- ✓ Sbagliare volontariamente l'ortografia di una parola, soprattutto se si usa una sola parola come parte della vostra password. ***Es.*** Cioccolato. Password: "Ciocolatto".
- ✓ Utilizzare una frase che è personale e usare il primo, il secondo o il terzo carattere di ogni parola nella frase. Ci possono essere diverse varianti di questo approccio:
    - o Utilizzare una frase che ha un numero alla fine.

      Es. Il mio numero preferito è 333. Password: "IMNPE333"
    - o Dopo la creazione della password, combinare i numeri e caratteri in modo che da poterli ricordare.

      Es. Quanto darò oggi? Il 100%. Password: "qdo?I100%"
    - o Usare lettere maiuscole e lettere minuscole in modo insolito.

      Es. Non rimandare a domani ciò che puoi fare oggi! Password: "NraDccpfO!"
    - o Utilizzare una rappresentazione numerica delle lettere dell'alfabeto per parte della frase o parte di una parola. Per esempio A è 1, B 2, C 3, etc.

      Es. Il nome di mia nonna è Gina. Password: "IndMnè79121".
    - o Utilizzare i segni di punteggiatura o caratteri speciali.

      Es. Preferisci mare o montagna? Mare. Password: "Pm/m?111165"

      ⇒ In molti degli esempi sopra citati, è facile inserire punteggiatura come "?" quando parte della frase è una domanda. Se la frase coinvolge numeri aggiungere $, %, # può facilitarne l'uso. Se nella frase si usa la lettera "e" o "o", è possibile sostituire "&" o "|". Inoltre, è possibile dividere le password con "/" o "\".

Applicazione
Dal momento che la password di protezione è fondamentale per la sicurezza dell'organizzazione, tutti i dipendenti che non rispettano questa politica possono essere soggetti a provvedimenti disciplinari.

Altre Considerazioni
Le password dell'account di Amministratore devono essere protette con particolare attenzione: dovrebbe essere consentito esclusivamente il livello minimo di accesso necessario per lo svolgimento della loro funzione e non devono essere condivise.