



# Corporate Security Policy

Società XYZ

Pagina 1 di 4

Documento Interno

Versione 2.0 Del 28 Mag 2004

Sezione

Password Policy

Protocollo Interno

VERSIONE DEMO

## Password Policy

### 1.0 Introduzione

Le Password sono un importante aspetto della sicurezza digitale. Sono la prima linea di protezione per gli accessi degli utenti. La scelta di una password "debole" può diventare l'anello debole dell'intera infrastruttura informativa aziendale. Per cui tutti i dipendenti della XYZ (inclusi consulenti esterni o agenti) sono responsabili per la corretta applicazione delle linee guida per la scelta e l'archiviazione della password descritte in seguito in questo documento.

### 2.0 Finalità

L'obiettivo di questa policy è di stabilire degli standard per la creazione di password "forti", la protezione delle password e la frequenza con la quale vengono sostituite.

### 3.0 Ambiti di applicabilità

Questa policy è di riferimento per tutto il personale che ha un account o è responsabile di un account (o qualsiasi altra forma di accesso che necessita di password) per il sistema informatico interno alla XYZ, o ha accesso remoto al network della XYZ o archivia dati riservati della XYZ.

### 4.0 Policy

#### 4.1 Generale

- Tutte le password system-level (root, enable, NT admin, application administration accounts, etc.) devono essere cambiate al massimo ogni 3 mesi.
- Tutte le password user-level (email, web, desktop computer, etc.) devono essere cambiate al massimo ogni 6 mesi. L'intervallo consigliato è di 4 mesi.
- Gli account utente che hanno privilegi di sistema devono essere univoche ovvero diverse dalle altre password utilizzate dall'utente.
- Le password non devono mai essere inserite nei messaggi di posta elettronica o in altre forme di comunicazione elettronica.
- Tutte le user-level e system-level password devono essere conformi alle linee guida descritte in seguito.

#### 4.2 Guidelines

##### A. Linee guida per la scelta della password

Le password vengono utilizzate per differenti finalità alla XYZ.

Alcuni degli utilizzi più comuni sono: user level accounts, web accounts, email accounts, screen saver protection

Poiché pochi sistemi utilizzano one-time password ogni soggetto interessato deve essere accorto nella scelta delle proprie password.



© Internet Centre of Excellence SpA - digitaltrust

Documento di proprietà di Internet Centre of Excellence SpA. Nessuna parte del documento può essere riprodotta o diffusa senza specifica autorizzazione scritta di Internet Centre of Excellence SpA. Tutti i diritti sono riservati



	<b>Corporate Security Policy</b> Società XYZ		<b>Pagina</b> 2 di 4	
			<b>Documento</b> Interno	
			<b>Versione</b> 2.0	<b>Del</b> 28 Mag 2004
<b>Sezione</b>	Password Policy	<b>Protocollo Interno</b>		VERSIONE DEMO

Password definite "deboli" o "povere" hanno le seguenti caratteristiche:

- La password contiene meno di otto caratteri
- La password è una parola del dizionario (Italiano o straniero)
- La password è una parola di utilizzo comune come per esempio:
- Nomi propri di familiari, animali, amici, colleghi, personaggi, etc.
- Termini e nomi informatici, comandi, siti, società, hardware, software.
- La parola "XYZ", o ogni derivazione
- Compleanni e altre informazioni personali come indirizzi e numeri di telefono.
- Pattern di nomi o parole come ad esempio: aaabbb, qwerty, zyxwvuts, 123321, etc.
- Ciascuna delle precedenti scritta al contrario.
- Ciascuna delle precedenti seguita o preceduta da una cifra (e.g., secret1, 1secret)

Le password "forti" hanno le seguenti caratteristiche:

- Contengono lettere upper e lower case (a-z, A-Z)
- Contengono simboli e punteggiatura insieme a lettere: 0-9, !@#\$%^&\*()\_+|~- =\ {} [] : " ; ' < > ? , . / )
- Sono di almeno 8 caratteri alfanumerici.
- Non sono parole di alcuna lingua, slang, dialetto, etc.
- Non sono basate su informazioni personali, nomi di famiglia, etc.
- Le password non devono mai essere scritte o salvate online. Bisogna cercare di creare password facilmente ricordabili. Una valida soluzione è di creare una password che fa riferimento ad una canzone, una poesia o un'altra frase. Per esempio, la frase potrebbe essere: "This May Be One Way To Remember" e la password potrebbe essere: "TmB1w2R!" or "Tmb1W>r~" o altre variazioni

NOTA: Non usare alcuno di questi esempi come password!

## B. Standard di Protezione della Password

Non usare la stessa password per gli account XYZ e per altri accessi non relativi al network aziendale (per esempio il collegamento internet personale, l'home banking, etc.) Se possibile non utilizzare la stessa password per differenti accessi ai servizi dei network XYZ.

Per esempio, in presenza di reti diverse utilizzare password differenti, scegliere una differente password a seconda della tipologia di sistema utilizzato (Win/Unix)

Non condividere la password XYZ con nessuno inclusi i colleghi e familiari.

Tutte le password devono essere considerate come informazioni sensibili e trattate ai sensi della legge del "31 dicembre 1996 n. 675" dalla XYZ



© Internet Centre of Excellence SpA - digitaltrust

Documento di proprietà di Internet Centre of Excellence SpA. Nessuna parte del documento può essere riprodotta o diffusa senza specifica autorizzazione scritta di Internet Centre of Excellence SpA. Tutti i diritti sono riservati



	<b>Corporate Security Policy</b> Società XYZ	<b>Pagina</b>		3 di 4
		<b>Documento</b>		Interno
		<b>Versione</b>	2.0	<b>Del</b>
<b>Sezione</b>	Password Policy	<b>Protocollo Interno</b>		VERSIONE DEMO

Una lista di cose da NON fare:

- Non comunicare mai la password al telefono a nessuno
- Non comunicare mai la password in un messaggio email
- Non comunicare mai la password al superiore
- Non parlare della password in presenza di più persone
- Non suggerire mai la password (es. "il nome di mia figlia")
- Non comunicare mai password a persone non autorizzate
- Non comunicare mai la password quando si è in vacanza

Per ogni richiesta di password fare riferimento a questo documento o contattare il responsabile della sicurezza informatica

Disabilitare la funzionalità "Ricorda Password" o "Remember Password" (per esempio in: Eudora, Outlook, Netscape Messenger).

Non scrivere mai la password per lasciarla in qualche luogo in ufficio. Non salvare mai la password su alcun supporto digitale senza criptarla.

Cambiare password al massimo ogni 6 mesi (ad eccezione delle system-level password che devono essere cambiate ogni 3 mesi) l'intervallo consigliato è di 4 mesi.

Se si sospetta che un account o una password siano state diffuse, riportare l'incidente al responsabile della sicurezza.

Test di verifica della "robustezza" delle password possono essere eseguiti periodicamente o 'random' da società terze referenziate che effettuino adeguati test.

Se una password viene "crackata" durante queste verifiche, all'utente verrà chiesto di cambiarla immediatamente

### C. Standard per gli sviluppatori di applicazioni

Gli sviluppatori di applicazioni devono assicurarsi che programmi contengano le seguenti precauzioni

Le applicazioni:

- Devono supportare l'autenticazione degli utenti e non dei gruppi
- Non devono salvare le password in chiaro.
- Devono prevedere una gestione dei livelli di accesso affinché un utente possa utilizzare le funzionalità dell'altro senza necessariamente conoscere la sua password.
- Deve supportare TACACS+ , RADIUS e/o X.509 con LDAP dove possibile.



© Internet Centre of Excellence SpA - digitaltrust

Documento di proprietà di Internet Centre of Excellence SpA. Nessuna parte del documento può essere riprodotta o diffusa senza specifica autorizzazione scritta di Internet Centre of Excellence SpA. Tutti i diritti sono riservati





# Corporate Security Policy

Società XYZ

Pagina 4 di 4

Documento Interno

Versione 2.0 Del 28 Mag 2004

Sezione

Password Policy

Protocollo Interno

VERSIONE DEMO

## D. Uso di Password per l'utente con accesso remoto

L'accesso remoto al network XYZ deve essere effettuato tramite one-time password o altrimenti un sistema PKI con "passphrase"

## E. Pass-phrase

La passphrase viene utilizzata per abilitare la chiave privata altrimenti inaccessibile

Le passphrase sono password più evolute e complesse contenenti upper e lowercase, lettere, numeri, punteggiatura

Un buon esempio: "The\*?#>\*@TrafficOnThe101Was\*&!#ThisMorning"

Tutte le regole delle password vengono applicate anche alle passphrase.

## 5.0 Azioni disciplinari

L'organizzazione si riserva il diritto di ispezionare i sistemi informatici dell'utente per individuare eventuali violazioni di questa policy.

Il dipendente che viola questa policy può essere soggetto ad azione disciplinare



© Internet Centre of Excellence SpA - digitaltrust

Documento di proprietà di Internet Centre of Excellence SpA.  
Nessuna parte del documento può essere riprodotta o diffusa senza  
specifico autorizzazione scritta di Internet Centre of Excellence SpA.  
Tutti i diritti sono riservati

