POLITICA DELLE PASSWORD

IT MANAGEMENT - POLICY

Via Mozart, 47 – 20093
Cologno Monzese (MI), Italia
Contatti: info@nuvyta.com
www.nuvyta.com

SOMMARIO

Document Information

Title	IT_P_ITManagement_Password			Status	Published
Type	*Policy*	Version	1.0	Created	07/06/2022
DocCode	*IT_P_005*	Language	ITA	Modified	07/06/2022
Author	Chiara Savino	Reviewer	Vania Manzelli	Approver	Alice Magni

Document Control

Intended Audience	Employee, Auditor, All
Distribution List	Public

Revision History

Ver.	Publish Date	Note
1.0	07/06/2022	First Release

1 OBIETTIVI (PURPOSE)

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 alla rete di Nuvyta. In ragione di quanto sopra esposto, ottemperando ai requisiti dettati dalla ISO 27001 e a quanto previsto dal Codice in materia di protezione dei dati personali (D.Lgs. 196/03 modificato/integrato *ex* D.Lgs. 101/2018) e dal Regolamento Europeo 679/2016, è introdotta la seguente *password policy* che stabilisce i criteri per la creazione, l'utilizzo, la conservazione e la gestione delle credenziali di autenticazione alle diverse componenti del sistema informativo aziendale.

Lo scopo di questa "policy" è quello di stabilire uno standard per la creazione di password complesse, la protezione di tali password e stabilire la relativa frequenza di variazione nell'ambito dei "sistemi" di "Information Technologies (IT)".

2 CAMPO DI APPLICAZIONE (SCOPE)

Questa "policy" si applica a tutti i dipendenti che hanno o sono responsabili di "account" di rete o di risorse (e/o di qualsiasi altra forma di accesso che supporti o richieda una password) su qualsiasi sistema aziendale.

In particolare, la seguente *policy password* si applica e regolamenta (*inter alia*) l'accesso ai singoli *client* aziendali al *server* aziendale; ai software gestionali *xxxx* ed alla posta elettronica aziendale.

3 RESPONSABILITÀ (RESPONSABILITIES)

L'attuazione e l'aderenza a questa "policy" è responsabilità di tutti i dipendenti di Nuvyta. È molto importante che ogni utente consideri seriamente l'utilizzo, la protezione e l'integrità delle proprie password e di qualsiasi altra password di sistema di cui possa essere a conoscenza, e che inoltre incoraggi, guidi ed informi il personale, anche in riferimento a coloro che sono responsabili del coordinamento di collaboratori.

4 DEFINIZIONI E ABBREVIAZIONI (DEFINITIONS)

Nessuna

5 PROCEDURE (PROCEDURES)

5.1 Principi generali

Lo strumento di accesso degli utenti al sistema informativo è costituito da un sistema di autenticazione 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 dall'utente. I due elementi, uniti insieme, costituiscono la credenziale di accesso ("account" o "utenza") così come definito dalla normativa vigente in tema di sicurezza dei dati personali.

Lo username viene assegnato dall'Amministratore del sistema o da un suo delegato all'atto dell'attivazione dell'utenza. La password viene gestita, dopo la sua prima assegnazione da parte dell'Amministratore del sistema, esclusivamente dall'utente. Lo username, una volta assegnato ad un utente, non potrà più essere riassegnato ad altri soggetti, nemmeno in tempi successivi, al fine di garantire un'archiviazione e storicizzazione delle utenze.

5.2 Regole generali di corretta composizione della password

Di seguito sono riassunte le principali regole da adottare nella scelta delle password personali e nella loro gestione:

- la password è personale e non cedibile;
- è fatto divieto di scegliere una password facilmente associabile ad informazioni relative all'utente, quali ad esempio il nome di familiari, codice fiscale, numeri di telefono, la user-id, ecc.;
- è fatto divieto di utilizzare sequenze digitate alla tastiera (ad esempio: qwerty o 123456);
- è fatto divieto di scrivere la password in posti visibili a terzi (ad esempio su post–it incollato sul proprio monitor);
- la lunghezza deve essere al minimo di 8 caratteri e deve essere composta da lettere (maiuscole e minuscole), numeri e caratteri speciali;
- è fatto divieto di scegliere password deboli (tutte lettere o numeri uguali);
- la password dovrà essere necessariamente sostituita ogni 180 giorni;
- la password non deve essere comunicata mediante messaggi e-mail o altre forme di comunicazione elettronica;
- nel caso in cui si sospetti che la propria password sia stata compromessa deve essere immediatamente cambiata;
- le credenziali di autorizzazione non utilizzate per più di sei mesi possono essere bloccate;
- nel caso di cambio di incarico, dimissioni etc. le *user id* saranno disabilitate;
- l'account potrà essere bloccato qualora venga superato il numero di tentativi di accesso consentiti per garantire la protezione da attacchi "*brute-force*".

Nel caso in cui la tecnologia utilizzata all'interno di Nuvyta non consenta automaticamente di implementare i meccanismi di complessità e robustezza delle *password* richiamati in questo documento, sarà cura dell'utente stesso applicare i criteri minimi di complessità e durata definiti dalle regole sopra indicate.

5.3 Violazione della Policy

Violazioni di questa policy e / o incidenti di sicurezza possono essere definiti come eventi che potrebbero provocare perdita o danneggiamento delle risorse dell'organizzazione o un evento che è in violazione alle procedure di sicurezza di Nuvyta.

Tutti i dipendenti di Nuvyta hanno la responsabilità di segnalare incidenti di sicurezza e violazioni di questa policy il più rapidamente possibile con l'ausilio della procedura di segnalazione degli incidenti. Questo obbligo si estende anche a qualsiasi organizzazione esterna incaricata di supportare o accedere ai sistemi informativi dell'organizzazione.

6 RIFERIMENTI (REFERENCES)

CONTROLLI ISO27001	TITOLO
A.9.1.1	Politica di controllo degli accessi
A.9.2.1	Registrazione e de-registrazione degli utenti
A.9.2.2	Provisioning degli accessi degli utenti
A.9.2.3	Gestione dei diritti di accesso privilegiato
A.9.2.4	Gestione delle informazioni segrete di autenticazione degli utenti
A.9.2.5	Riesame dei diritti di accesso degli utenti
A.9.3.1	Utilizzo delle informazioni segrete di autenticazione
A.9.4.2	Procedure di log-on sicure
A.9.4.3	Sistema di gestione delle password
A.9.4.4	Uso di programmi di utilità privilegiati