



N U V Y T A

POLICY RELATIVA ALLA CRITTOGRAFIA DEI DATI

IT MANAGEMENT - POLICY

CI RISERVIAMO IL DIRITTO DI APPORTARE
MODIFICHE UTILI ALL'EVOLUZIONE
TECNICA E FUNZIONALE DEL PRODOTTO.

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

SOMMARIO

1	Obiettivi (Purpose)	3
2	Campo di applicazione (Scope)	3
3	Responsabilità (Responsabilities)	3
4	Definizioni e abbreviazioni (Definitions)	3
5	policy (policy).....	3
5.1	<i>Trasferimento Dati</i>	3
5.2	<i>Memorizzazione Dati</i>	4
5.3	<i>Chiavi per la Crittografia</i>	4
6	Riferimenti (References)	4

Document Information

Title	IT_P_DataCryptography			Status	Published
Type	Policy	Version	1.0	Created	09/06/2022
DocCode	IT_P_001	Language	ITA	Modified	09/06/2022
Author	Chiara Savino	Reviewer	Michele Ziparo	Approver	Vania Manzelli

Document Control

Intended Audience	Employee, Auditor, All
Distribution List	Public

Revision History

Ver.	Publish Date	Note
1.0	09/06/2022	Primo rilascio

1 OBIETTIVI (PURPOSE)

Nuvyta Srl utilizza sistemi crittografici per proteggere dati che non hanno carattere pubblico. In particolare, quei dati che per la loro natura devono essere protetti sia per motivi di riservatezza sia per motivi di sicurezza. La presente procedura definisce le modalità di crittografia dei dati gestiti da Nuvyta.

2 CAMPO DI APPLICAZIONE (SCOPE)

La procedura si applica a tutti i dati di lavoro gestiti da Nuvyta. Sono ritenuti dati da proteggere:

- i dati personali di dipendenti e collaboratori;
- i dati personali degli utenti dei servizi che l'azienda eroga sia per proprio conto sia per conto dei clienti;
- i dati di business dell'azienda, dei clienti e dei fornitori;
- i dati relativi al servizio fornito dall'azienda.

3 RESPONSABILITÀ (RESPONSABILITIES)

CTO, Responsabile IT

4 DEFINIZIONI E ABBREVIAZIONI (DEFINITIONS)

Nessuna

5 POLICY (POLICY)

5.1 Trasferimento Dati

Tutti i dati scambiati attraverso la rete Internet, che si tratti di sistemi ad uso interno o di servizi erogati per conto di clienti, sono scambiati utilizzando protocolli di comunicazione basati su crittografia SSL/TLS: HTTPS, SSH, SCP, etc.

Nuvyta ha adottato un approccio completamente cloud per la gestione delle informazioni e non ha un sistema informatico centralizzato presso le proprie sedi di lavoro. Il sistema identificato per l'archiviazione e la condivisione dei dati è Office365 con le componenti Teams Sharepoint e Onedrive.

Lo scambio di dati fra l'Infrastruttura IT dell'azienda in cloud e i PC del personale avviene utilizzando protocolli di comunicazione protetti con la crittografia TLS (Transport Layer Security). È consentito solo l'accesso sicuro. Non verranno consentite connessioni autenticate tramite HTTP, ma verrà invece eseguito il reindirizzamento a HTTPS.

5.2 Memorizzazione Dati

I dati contenuti all'interno dei DMS (Sharepoint-Teams-OneDrive) sono salvati utilizzando la crittografia Advanced Encryption Standard (AES) con chiavi a 256 bit ed è conforme ai criteri FIPS (Federal Information Processing Standard) 140-2.

I pc aziendali sono dotati di tecnologia bitlocker o similare per garantire crittografia del disco.

Le credenziali di accesso ai sistemi database vengono salvate in modo cifrato.

5.3 Chiavi per la Crittografia

Per la crittografia dei dati presenti nei pc aziendali viene adottata tecnologia bitlocker con algoritmi AES 256 con chiave pubblica RSA a 2048 bit. Il Responsabile IT provvede alla disattivazione nei casi di:

- uscita del dipendente dall'azienda;
- smarrimento del PC;
- compromissione del PC;

Sono implementati meccanismi di rotazione delle chiavi di bitlocker per i pc aziendali gestiti dal responsabile IT.

6 RIFERIMENTI (REFERENCES)

Norma UNI CEI ISO/IEC 27001:2017

Regolamento UE n. 679/2016 – GDPR

<https://learn.microsoft.com/it-it/sharepoint/safeguarding-your-data>

<https://learn.microsoft.com/it-it/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide>

<https://support.microsoft.com/it-it/office/in-che-modo-onedrive-protegge-i-dati-dell-utente-nel-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1>

<https://www.microsoft.com/it-it/trust-center/privacy?rtc=1>

<https://learn.microsoft.com/it-it/mem/intune/protect/encrypt-devices>

