LAPTOP & MOBILE DEVICE SECURITY

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_Laptop&MobileDeviceSecurityPolicy			Status	Published
Type	*Policy*	Version	1.0	Created	29/12/2022
DocCode	*IT_P_008 -IT*	Language	ITA	Modified	29/12/2022
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	29/12/2022	First Release

1 OBIETTIVI (PURPOSE)

Nuvyta fa affidamento sull'utilizzo di laptop, eventualmente di tablet e altri dispositivi di elaborazione mobili in tutte le sue aree di business: l'utilizzo di dispositivi mobili ha facilitato la flessibilità lavorativa dell'Azienda. La presente policy ha l'obiettivo di definire e normare la sicurezza dei dispositivi mobili che sono attualmente in uso.

Lo scopo di questa procedura è quello di garantire che laptop, eventuali tablet e altri dispositivi di mobile computing siano utilizzati, configurati e gestiti in modo sicuro e protetto, e che vengano identificate e descritte le azioni da effettuare per garantirlo.

Nuvyta, pur riconoscendo che laptop, eventuali tablet e altri dispositivi di mobile computing, sono strumenti utili che consentono di lavorare in modo flessibile e "smart", impone che tali dispositivi debbano essere controllati, configurati e utilizzati nel modo più sicuro possibile utilizzando standard e procedure per prevenire danni sia alle proprie risorse che alla propria reputazione.

2 CAMPO DI APPLICAZIONE (SCOPE)

I destinatari della presente policy sono:

- Tutti i dipendenti dell'azienda;
- Tutti i visitatori che utilizzano le postazioni desk dell'organizzazione.

La policy si applica a tutto il personale nella sede dell'organizzazione o presso le sedi dei clienti nel caso di permanenza prolungata, indipendentemente dall'area di lavoro o dalla tipologia di attività che utilizzano dispositivi mobile.

3 RESPONSABILITÀ (RESPONSABILITIES)

La protezione delle informazioni non è solo una responsabilità aziendale, è anche una responsabilità di tutto il personale che lavora per l'azienda.

L'azienda adotterà le misure appropriate per porre rimedio a qualsiasi violazione della policy. Nel caso di violazioni da parte dei dipendenti, la questione può essere trattata nel processo disciplinare dell'azienda secondo quanto previsto dal CCNL.

4 DEFINIZIONI E ABBREVIAZIONI (DEFINITIONS)

Dati personali: le informazioni personali sono informazioni che possono identificare una persona e che collega quell'individuo a dettagli che sarebbero considerati come privati, ad es. Nome, indirizzo privato, numero di telefono di casa, codice fiscale etc...;

5 POLITICA (POLICY)

5.1 Laptop & Tablet Devices

5.1.1 Generalità

Tutti i laptop e gli eventuali tablet dovranno avere le seguenti configurazione al fine di garantire che siano applicate i corretti livelli di sicurezza:

- utilizzo del sistema operativo previsto dall'Azienda (Windows);
- i nuovi laptop / tablet verranno preconfigurati da Nuvyta – dall'IT Manager - per le figure amministrative, mentre per le figure con alte specializzazioni informatiche verrà effettuata indicazione delle modalità di configurazione;
- i Laptop sono protetti da virus e malware mediante l'utilizzo di prodotti autorizzati. Questo viene automaticamente mandato in esecuzione su tutti i laptop durante l'avvio e viene regolarmente aggiornato con la definizione dei virus / minacce più recenti;
- i laptop si bloccano automaticamente dopo 5 minuti di inoperatività.

Altri dispositivi mobili utilizzati per lo sviluppo del business di Nuvyta devono essere utilizzati principalmente come uno strumento per attivare e facilitare l'accesso alle informazioni dell'organizzazione ospitate su siti Web, intranet e siti di risorse.
La connessione di qualsiasi dispositivo di elaborazione mobile alla rete di Nuvyta deve essere valutata dal servizio IT e soggetta agli standard e alle procedure di configurazione esistenti previa autorizzazione.

5.1.2 Uso Accettabile

I laptop, i tablet e altri dispositivi di elaborazione mobile possono essere utilizzati solo da persone autorizzate per attività o scopi autorizzati in conformità alle policy aziendali.

I dipendenti di Nuvyta devono essere consapevoli della possibilità di accesso e visualizzazione non autorizzato a dati ed informazioni dell'organizzazione ed adottare le misure appropriate per evitare ed impedire ciò.

Tutti gli utilizzatori di laptop, tablet e altri dispositivi mobili devono garantire in ogni momento che:

- L'accesso al dispositivo avvenga previa autenticazione, l'account debba essere inserito nell'active directory aziendale;
- l'account e la password di accesso al dispositivo siano tenute private e non vengano condivise, visualizzate o comunicate ad altri;
- in nessuna circostanza i dati sensibili e personali vengano salvati su alcun dispositivo mobile;
- i dati che non sono sensibili o personali possono essere archiviati su dispositivi informatici mobili solo quando non è disponibile la connettività verso la rete aziendale, non appena la connettività viene ripristinata i dati dovranno essere trasferiti verso il sistema informativo aziendale e le copie locali devono essere eliminate;

- gli utenti devono essere consapevoli del fatto che i dati memorizzati localmente sui dispositivi mobili non verranno salvati e rischiano di essere persi;
- i dispositivi mobili non devono essere usati come dispositivi di memorizzazione di dati;
- non è ammesso l'utilizzo di chiavette USB o altri dispositivi per il passaggio di informazioni e dati da un dispositivo e un altro;
- apparecchiature non autorizzate, non standard o personali non devono essere collegate in alcun modo ad un dispositivo mobile.
- qualsiasi dispositivo mobile non venga lasciato incustodito o distrutto in luoghi pubblici;
- non è consentito l'accesso a reti pubbliche che possano esporre a rischio il contenuto del PC;
- vengono prese tutte le misure ragionevoli per garantire che durante il trasporto, qualsiasi dispositivo informatico mobile sia bloccato e non accessibile al sistema da parte di utenti non autorizzati e posizionato in modo sicuro. Per motivi assicurativi, i dispositivi portatili non devono essere mai lasciati incustoditi nei veicoli;
- tutti i dispositivi siano adeguatamente protetti da danni fisici;
- è possibile attivare la crittografia su PC e dispositivi mobile;
- qualsiasi dispositivo mobile, che non sia più necessario o che abbia raggiunto la fine del suo ciclo di vita, deve essere restituito al responsabile degli asset per essere smaltito utilizzando la procedura di dismissione di Nuvyta. A tale regola può essere fatta apposita deroga tramite assegnazione personale del pc all'utente. Nel caso di specie, al fine di tutelare i dati aziendali, il team IT effettua verifica che in locale sul dispositivo non ci siano informazioni/file;
- tutti i dispositivi mobili devono essere restituiti al responsabile degli asset, alla cessazione del rapporto di lavoro o quando non siano più necessari al lavoro abituale;
- tutti i dispositivi mobili debbano essere resi disponibili su richiesta della direzione o da chi è autorizzato per essere sottoposti alle politiche di manutenzione e di revisione di conformità;
- venga prestata attenzione quando si utilizzano connessioni remote, inclusi i punti di rete wireless, che queste siano "attendibili" e adeguatamente protette.

N.B. La perdita di qualsiasi dispositivo mobile deve essere immediatamente segnalata al IT Manager e denunciata alle autorità competenti.

5.1.3 Installazioni software

Tutte le attività di installazione di applicazioni/software o volte ad apportare modifiche alla configurazione del sistema dei dispositivi mobili deve essere effettuata da personale autorizzato. Una configurazione di base standard è installata su tutti i dispositivi laptop
In particolare:

- su laptop, tablet o dispositivi mobili, il software non deve essere installato da personale non autorizzato a meno che non sia prevista formale autorizzazione;
- è accettato l'aggiornamento dei soli aggiornamenti software / patch automaticamente proposte dal sistema operativo o dal software pre-installato sui PC;
- qualsiasi software installato deve essere compreso nell'elenco dei software dell'organizzazione;
- i dispositivi mobili non devono essere maneggiati in maniera errata, danneggiati intenzionalmente o manomessi in alcun modo;

Eventuali variazioni o installazione di nuovi software devono essere concordate con il Responsabile IT e con il Responsabile della sicurezza delle informazioni. Laptop/tablet devono essere protetti da codice dannoso in conformità alla procedura anti-virus in essere. Tutti i dispositivi mobili devono essere gestiti in conformità con tutte le politiche e le procedure di Nuvyta.

5.1.4 Dismissioni PC

Nuvyta procede allo smaltimento dei dispositivi attraverso la formattazione completa dei dispositivi stessi e archiviazioni di questi, sotto la responsabilità dell'IT Manager, in armadi sotto chiave.

6 RIFERIMENTI (REFERENCES)

Elenco dei riferimenti normativi ISO 27001

Riferimento Controllo	Titolo
A.6.2.1	Politica per i dispositivi portatili
A.8.1.3	Utilizzo accettabile degli asset
A.8.2.3	Trattamento degli asset
A.8.3.1	Gestione dei supporti rimovibili
A.8.3.2	Dismissione dei supporti
A.9.4.4	Uso di programmi di utilità privilegiati
A.9.4.5	Controllo degli accessi al codice sorgente dei programmi
A.11.2.1	Disposizione delle apparecchiature e loro protezione
A.11.2.4	Manutenzione delle apparecchiature
A.11.2.6	Sicurezza delle apparecchiature e degli asset all'esterno delle sedi
A.11.2.7	Dismissione sicura o riutilizzo delle apparecchiature
A.11.2.8	Apparecchiature incustodite degli utenti
A.12.5.1	Installazione del software sui sistemi di produzione
A.16.1.2	Segnalazione degli eventi relativi alla sicurezza delle informazioni