PAPER MANAGEMENT, SECURITY DESK & SCREEN POLICY

IT MANAGEMENT - POLICY

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

SOMMARIO

Sommario 1
1 Obiettivi (Purpose) 3
2 Campo di applicazione (Scope) 3
3 Responsabilità (Responsabilities) 3
4 Definizioni e abbreviazioni (Definitions) 4
5 POLITICA (POLICY) 4
5.1 Politica delle scrivanie 4
5.2 Stampanti, fotocopiatrici e fax 5
5.3 Schemi puliti 5
6 Riferimenti (References) 5

Document Information

Title	IT_P_ITManagement_PaperManagement&SecurityDesk&Screen			Status	Published
Type	*Policy*	Version	1.1	Created	07/06/2022
DocCode	*IT_P_004 -IT*	Language	ITA	Modified	28/12/2022
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	07/06/2022	First Release
1.1	28/12/2022	Aggiunto paragrafo 5.3 Schemi puliti

1 OBIETTIVI (PURPOSE)

Lo scopo di questa policy è garantire che tutti i documenti cartacei contenenti informazioni personali o qualsiasi altra informazione riservata / sensibile (comprese informazioni aziendali o commercialmente sensibili siano adeguatamente protette quando non utilizzate, lasciate incustodite o visibili su una scrivania fuori orario di lavoro).

Questa policy si applica in particolare alle aree di lavoro, come scrivanie che non devono contenere informazioni riservate, sensibili o identificabili della persona mentre sono incustodite per un periodo prolungato.

I principi chiave per aderire alla policy di Secure Desk sono elencati di seguito:

- ridurre il rischio di violazione della sicurezza o furto di informazioni;
- ridurre il rischio di furto o accesso a informazioni o documenti riservati da parte di persone non autorizzate che potrebbero danneggiare l'integrità aziendale;
- essere conformi al GDPR come previsto nella Privacy Policy;
- disincentivare la stampa di documenti per cui non è necessaria la conservazione in formato cartaceo;
- creare una cultura della responsabilità del personale in relazione alla gestione e alla cura dei dati personali e di altre informazioni riservate.

L'informazione, in qualsiasi forma, è un bene prezioso per l'organizzazione e di conseguenza deve essere adeguatamente protetta.

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.

La policy si applica a scrivanie, tavoli, schermi di computer o laptop, aree per fotocopiatrici, fax e stampanti.

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:

- tutti i dipendenti sono tenuti a rispettare la politica di Secure Desk;
- la direzione ed il responsabile della sicurezza delle informazioni sono responsabile della conformità, dell'attuazione e forniscono guida al personale sull'attuazione della policy;

- tutti i dipendenti e il personale che opera all'esterno presso le sedi dei clienti hanno la responsabilità di segnalare gli incidenti di sicurezza e le violazioni di questa politica il più rapidamente possibile al responsabile della sicurezza delle informazioni tramite la procedura di segnalazione e gestione degli incidenti.

L'azienda adotterà le misure appropriate per porre rimedio a qualsiasi violazione della policy di Secure Desk. 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...;

Categorie particolari di dati personali: le informazioni personali sensibili sono quelle in cui le informazioni contengono dettagli di quella persona come ad esempio:

- Condizioni fisiche o mentali;
- Vita sessuale;
- Origine etnica;
- Credenze religiose;
- Visioni politiche:
- Condanne penali;
- Appartenenza a un sindacato.

Informazioni classificate come "riservate": Informazioni la cui divulgazione non autorizzata (anche all'Interno dell'organizzazione) causerebbe gravi danni in termini di perdite finanziarie, perdita di know how, azioni legali perdite di reputazione e mancata tutela di dati tutelati dal GDPR

Informazioni classificate come "ad uso interno": informazioni generalmente disponibili a chiunque all'Interno di NUVYTA e che abbiano "valore aziendale" per l'organizzazione, o che richiedano protezione in considerazione dei dati personali.

5 POLITICA (POLICY)

5.1 Politica delle scrivanie

- Le scrivanie devono essere ordinate alla fine di ogni giornata lavorativa da qualsiasi informazione confidenziale o identificativa della persona;
- gli oggetti personali (ad es. chiavi, borsette, portafogli ecc.) devono essere chiusi a chiave in sicurezza. È responsabilità del proprietario dell'oggetto assicurarsi che vengano prese tutte le precauzioni;
- è consentito riprodurre i documenti con informazioni personali in un numero di copie strettamente necessarie ed eventualmente distribuirle solo a chi ne abbia comprovata necessità;

- il collaboratore deve distruggere le copie non necessarie e quelle difettose, in modo che le informazioni personali registrate non siano più utilizzabili;
- quando un documento con informazioni personali è scaduto, si è tenuti a provvedere alla sua eliminazione, avendo cura che il contenuto non sia comunque più leggibile (ad esempio utilizzando uno shredder oppure ricorrendo ad una procedura di invio al macero);
- scrivanie e altri spazi di lavoro devono essere sufficientemente in ordine alla fine di ogni giornata lavorativa per consentire al personale delle pulizie di svolgere le proprie mansioni.

5.2 Stampanti, fotocopiatrici e fax

- Per evitare di stampare accidentalmente su un dispositivo di rete non intenzionale, gli utenti devono verificare che la loro stampante predefinita sia corretta prima di stampare qualsiasi documento;
- è vietato lasciare documenti incustoditi sulla stampante, per evitare che informazioni personali possano essere conosciute da chi non è autorizzato a quel trattamento;
- i dati a cui si applica la presente policy devono essere cancellati immediatamente dalle stampanti, dalle fotocopiatrici e dagli eventuali fax;
- è responsabilità della persona che invia le informazioni da stampare assicurarsi che raccolgano i propri documenti e non li lascino incustoditi. Se le informazioni sono di natura confidenziale / sensibile e sono malriposte o mancanti, questo dovrebbe essere registrato come incidente di sicurezza.

5.3 Schemi puliti

- Non lasciare collegati computer o comunque devono essere protetti da PW se ci si allontana dalla scrivania: è obbligatorio verificare, ogniqualvolta ci si allontana dalla scrivania, che il PC sia bloccato e sia accessibile solo tramite autenticazione
- È vietato ai dipendenti conservare su desktop documentazione relativa all'attività operativa aziendale

6 RIFERIMENTI (REFERENCES)

Elenco dei riferimenti normativi ISO 27001

Riferimento Controllo	Titolo
A.6.1.1	Ruoli e responsabilità della sicurezza delle informazioni
A.9.3.1	Utilizzo delle informazioni segrete di autenticazione
A.11.2.8	Apparecchiature incustodite degli utenti
A.11.2.9	Politica di schermo e scrivania puliti
A.16.1.2	Segnalazione degli eventi relativi alla sicurezza delle informazioni
A.18.1.4	Privacy e protezione dei dati personali