POLITICA SULLA PRIVACY – ANNEX 1

INTEGRATED MANAGEMENT SYSTEM - POLICY

CREDIAMO IN UN MODO DI FARE SOFTWARE DIVERSO. VOGLIAMO CHE SIA CONDIVISO, PERSONALIZZABILE E IN CONTINUA EVOLUZIONE.

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

SOMMARIO

Document Information

Title	[Support]PrivacyPolicy – Annex 1			**Status**	Published
Type	*Standard*	**Version**	1.0	**Created**	28/11/2022
DocCode	*H_ST_003-IT*	**Language**	ITA	**Modified**	24/04/2021
Author	Chiara Savino	**Reviewer**	Vania Manzelli	**Approver**	Alice Magni

Document Control

Intended Audience	Employee, Auditor
Distribution List	Internal

Revision History

Ver.	Publish Date	Note
1.0	28/11/2022	First Release (Prima versione)

1. OBIETTIVI (PURPOSE)

Il presente documento funge da allegato alla Policy Privacy di Nuvyta e definisce il regolamento Privacy adottato dall'azienda.

2. CAMPO DI APPLICAZIONE (SCOPE)

La policy è rivolta a tutti i dipendenti, stagisti e collaboratori di Nuvyta

3. RESPONSABILITÀ (RESPONSABILITIES)

DPO

4. DEFINIZIONI E ABBREVIAZIONI (DEFINITIONS)

Acronino	Nome	Descrizione
DPO	Data Protection Officer	Responsabile della protezione dei dati

5. REGOLAMENTO (POLICY)

REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA

La valutazione delle misure di sicurezza da adottare deve essere vista nel contesto del rischio a cui è rivolta. Le misure di sicurezza pertanto vanno viste nel loro senso più ampio del termine partendo dal principio che l'art. 32 del Regolamento EU recita "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

Di seguito vengono riportate ad esempio alcune regole e principi di base per diverse misure di sicurezza implementate.

Misure	Regole / Principi da Osservare

Presenza di un sistema di allarme	E' importante che l'Ente si doti di impianto d'antifurto a tutela del patrimonio delle informazioni contenute al suo interno
Custodia dei dati sensibili in armadi chiusi a chiave	E' importante che gli uffici che trattano dati sensibili e giudiziari possano disporre di queste strutture per archiviare in modo consono tali informazioni
Digitazione password all'accensione del PC	Tutti i PC devono avere la password di Windows all'accensione del terminale, questo non vale solo come regola ma viene considerata una misura base di sicurezza
Manutenzione programmata degli strumenti	Come tutte le macchine che si rispettano anche il sistema informativo va sottoposto a manutenzione periodicamente sia attraverso l'aggiornamento dei suoi componenti sia con che la verifica periodica delle macchine stesse
Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente
Disattivazione delle credenziali di autenticazione nel caso di inutilizzo per 6 mesi	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Procedure di verifica sull'operato degli incaricati	È un compito ispettivo che il Responsabile della sicurezza dei dati personali può demandare anche a società esterne
Controllo degli accessi a siti internet non sicuri Protezione della posta elettronica	E' importante la conoscenza da parte degli operatori della navigazione in internet e dell'uso della posta elettronica. A questo proposito è stato introdotto il regolamento per l'uso del PC
Utilizzo di un antivirus	Per quanto precedentemente detto, è importante la presenza di un antivirus in ogni posto di lavoro, considerata misura di sicurezza e ovviamente che sia aggiornato
Aggiornamento periodico di programmi per il controllo della vulnerabilità	È importante che ogni pc sia periodicamente aggiornato sulle proprie vulnerabilità con gli appositi software
Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro	È importante che l'operatore conosca il regolamento per quanto concerne l'assenza dal posto di lavoro con il PC acceso
Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incarico	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia

Di seguito vengono riportate ad esempio alcune regole e principi di base per diverse misure di sicurezza che verranno implementate nel tempo.

Misure	Regole / Principi da Osservare
Utilizzo di un sistema firewall per la posta elettronica.	Obbligatorio viste le forme di attacco sempre più intelligenti.
Utilizzo di un filtro anti-spam	All'interno dello spam (posta indesiderata) si annidano spesso dei fenomeni di illegalità informatica. È importante dotare l'Ente di tale strumento

Aggiornamento periodico, con cadenza almeno annuale, della lista degli incaricati e dei profili di autorizzazione	Tutte le persone che operano all'interno degli uffici devono essere autorizzate dal Titolare
Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione	Rientra nel concetto della formazione del personale
Aggiornamento periodico delle credenziali di autenticazione	Spetta all'incaricato l'aggiornamento delle password quando richiesto dal sistema, secondo i requisiti di complessità adottati a livello aziendale
Formazione sugli aspetti principali della disciplina della privacy al momento dell'ingresso in servizio	Rientra nel concetto della formazione del personale
Formazione, periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione	Rientra nel concetto della formazione del personale
Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento	Rientra nel concetto della formazione del personale
Formazione professionale	Rientra nel concetto della formazione del personale
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati	Il backup deve essere metodico, non affidato alle singole volontà.
Definizioni di responsabilità e sanzioni disciplinari	Rientra nel concetto della formazione del personale nonché è necessario integrare il codice di comportamento includendo sanzioni disciplinari nei casi in cui ci sia un comportamento difforme da quando indicato dal presente Regolamento
Distruzione del cartaceo	È importante nel limite del possibile incentivare la distruzione del cartaceo rendendolo illeggibile usando dei comodi distruggi documenti

DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO CON STRUMENTI ANALOGICI E DIGITALI

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Autorizzati al trattamento dei dati personali debbono osservare le seguenti disposizioni.

Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.

L'Autorizzato al trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente

Ogni Autorizzato al trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non

consentito o non conforme alle finalità della raccolta.

Gli Autorizzati al trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.

Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.

Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'Autorizzato del trattamento non dovrà lasciarli mai incustoditi.

L'Autorizzato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.

Al termine dell'orario di lavoro l'Autorizzato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.

I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.

Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.

Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro Autorizzato debitamente autorizzato.

Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.

È inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.

Documenti contenenti dati personali che, per una qualunque ragione, siano da cestinare, devono assolutamente essere distrutti in modo da risultare illeggibili a soggetti terzi non autorizzati che ne potrebbero entrare in possesso (es. addetti alle pulizie).

Quando i documenti devono essere trasportati essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'Autorizzato del trattamento deve tenere sempre con sé la cartella o la

borsa, nella quale i documenti sono contenuti.

L'Autorizzato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.

È proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un autorizzato a potere trattare i dati in questione.

Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico o aperto al pubblico.

Oltre a quanto indicato nel presente documento si rimanda al contenuto dell'atto di designazione in riferimento ai principi in esso indicati.