MÉRIEUX NUTRISCIENCES

COMPLIANCE POLICY

DATA SECURITY

(Ottobre 2020 - V.1)

1. OBIETTIVI

Questa Policy mira ad individuare gli obblighi e le responsabilità degli Utenti per garantire un uso appropriato delle risorse IT e la protezione dei dati aziendali e personali all'interno della Società.

Questa Policy si applica all'uso delle Risorse IT per condurre l'attività della Società o interagire con le reti interne e i sistemi aziendali, siano essi di proprietà o affittati dalla Società, dall'Utente o da terzi.

La presente Data Security Policy si applica a tutti i dipendenti, amministratori e funzionari della Società. È responsabilità dei manager condividere queste linee guida e raccomandazioni con tutti i dipendenti della Società.

2. DEFINIZIONI

Dati personali indica qualsiasi informazione che identifica, direttamente o indirettamente, una persona fisica.

Dati aziendali indica qualsiasi informazione riservata elaborata per conto della Società o di uno dei suoi partner o clienti.

Legislazione sulla protezione dei dati indica il Regolamento Europeo (UE) 2016/679 sulla protezione dei Dati Personali e ogni altra normativa nazionale relativa alla protezione dei Dati Personali applicabile alla presente informativa.

Risorse IT includono :

- Hardware informatici che forniscono accesso a: server, computer, stampanti, tablet, smartphone, reti, canali e altre apparecchiature informatiche;
- Software installati sul computer dell'Utente o accessibile da remoto sui server della Società (Intranet) o su server esterni (Internet).

Utente si intende qualsiasi persona, qualunque sia il suo stato, che utilizza le risorse IT dell'azienda.

3. PRINCIPIO GENERALE

Tutte le risorse IT appartengono alla Società e sono fornite agli Utenti al solo scopo di essere utilizzate per scopi aziendali legittimi e in conformità con le politiche, le procedure, le linee guida e le istruzioni della Società.

L'uso personale delle risorse IT, compreso l'accesso alle reti (Internet o locale), è consentito fintanto che rimane appropriato, limitato, legale, non interrompe il funzionamento della Società e non ne danneggia la reputazione.

4. RISERVATEZZA E PROTEZIONE

Protezione delle informazioni

È responsabilità di ciascun Utente gestire, mantenere e proteggere adeguatamente la sicurezza delle Risorse IT aziendali e dei dati aziendali a cui ha accesso o controllo in conformità con le linee guida sulla sicurezza globale delle informazioni della Società disponibili su MXNS Connect.

Le informazioni e i processi utilizzati per trasmettere, archiviare e accedere alle Risorse IT aziendali e ai dati aziendali possono essere confidenziali, commercialmente sensibili o soggetti a diritti di proprietà intellettuale.

Ogni Utente deve inoltre proteggere le informazioni appartenenti a terzi, come clienti, partner e fornitori, dalla divulgazione non autorizzata o da altri danni.

Impostazioni di accesso

Account, logins, password, licenze o qualsiasi altro key device del personal computer rilasciato all'Utente sono informazioni personali.

Le password sono associate ad un accesso specifico dell'Utente e, se utilizzate correttamente, impediscono l'accesso non autorizzato. Le password devono essere mantenute strettamente riservate e non devono mai essere divulgate, nemmeno al manager o al supporto IT. Le password non devono essere ovvie e devono contenere lettere, numeri e / o punteggiatura.

Per garantire una buona sicurezza, la Società consiglia vivamente a ciascun Utente di modificare le proprie password ogni 120 giorni.

L'Utente modifica o richiede il rinnovo dei propri mezzi di autenticazione non appena sospetta la loro divulgazione.

L'Utente deve utilizzare i propri diritti di accesso solo per accedere a informazioni o servizi necessari per lo svolgimento dei compiti a lui affidati e per i quali è autorizzato.

L'Utente deve garantire la riservatezza della sua postazione computer bloccando il suo display durante la sua assenza. Si impegna inoltre a garantirne il corretto funzionamento ed in particolare a riavviare il suo computer almeno una volta alla settimana collegandolo alla rete interna per consentire l'installazione degli aggiornamenti di sicurezza aziendale. Il riavvio regolare è necessario anche per tablet e telefoni.

L'Utente deve prendersi cura delle apparecchiature portatili della Società e garantirne la protezione sia all'interno della Società che al di fuori di essa. Se, al di fuori dell'orario di lavoro, l'Utente lascia il dispositivo portatile in loco, si impegna a riporlo in una scatola o in un mobile chiuso a chiave. Se l'Utente porta con sé il dispositivo portatile, si impegna a non lasciarlo in un luogo incustodito.

5. CONTROLLO DELLE ATTIVITÀ

Controlli automatizzati

Tutte le azioni eseguite dalle Risorse IT aziendali possono essere soggette a supervisione. Ogni Utente è considerato responsabile delle azioni eseguite sotto la sua identità informatica.

Procedura di controllo manuale

In caso di malfunzionamento rilevato dalla Direzione IT, potrà essere effettuata una verifica manuale e una verifica delle eventuali operazione eseguite da uno o più Utenti.

Se una Risorsa IT presenta anomalie, l'Utente deve informare immediatamente il reparto IT tramite ssp.mxns.com.

6. E-MAIL

La posta elettronica (nominativa o meno) è messa a disposizione dell'Utente per scopi aziendali e sotto la propria responsabilità.

Uso personale della posta elettronica

L'Utente ha il diritto di utilizzare occasionalmente la sua posta elettronica per scopi personali. Tuttavia, tali messaggi devono essere chiaramente identificati come messaggi privati e personali (aggiungendo la parola "PERSONALE" o "PRIVATO" nella riga dell'oggetto o creando una directory specifica dedicata a questo contenuto). Si presume che tutti i messaggi non identificati come personali siano messaggi aziendali.

I diritti della società

Sebbene la Società si impegni a proteggere sempre i dati dei dipendenti, la Società avrà comunque il diritto di consultare le e-mail di qualsiasi Utente in circostanze specifiche e critiche e per scopi legittimi come garantire la continuità aziendale, proteggere le risorse IT o in caso di indagini di polizia o amministrative .

In tali situazioni eccezionali, l'accesso alla casella di posta elettronica dell'Utente sarà consentito solo ai pochissimi responsabili della Società o esperti esterni che necessitano realmente di essere coinvolti nella risoluzione della situazione critica. I diritti di consultazione estesi a terzi alla casella di posta elettronica dell'Utente non consentiranno mai alla Società di utilizzare in altro modo l'indirizzo di posta elettronica dell'Utente. La Società dovrà, nella misura migliore possibile, informare l'Utente prima di estendere qualsiasi diritto di accesso alla sua casella di posta elettronica a terzi. Se tali informazioni non possono essere fornite in anticipo per motivi confidenziali od operativi, l'Utente verrà informato il prima possibile successivamente. Accedendo alla posta elettronica degli Utenti, la Società si impegna a non

consultare messaggi chiaramente identificati come “personali” come descritti nella precedente sottosezione.

Cessazione dell’Utente

Prima di lasciare la Società, è responsabilità dell'Utente rimuovere tutti i suoi messaggi personali e impostare un messaggio di fuori sede che indichi la sua cessazione del rapporto con la Società. L'accesso alla posta dell'Utente verrà cessata al termine del suo contratto di lavoro.

Dopo la cessazione dell'Utente, la Società potrà accedere alle sue e-mail per un periodo di tempo limitato se necessario nell'ambito delle attività aziendali. La Società non potrà utilizzare l'indirizzo email dell'Utente e vi accederà solo per consultazione. La Società si impegna a non consultare messaggi chiaramente identificati come personali.

7. PROTEZIONE RETI E SCAMBI

Uso delle reti

L'Utente accetta di non scaricare o utilizzare per scopi aziendali, software o pacchetti software i cui canoni di licenza non siano stati pagati, da siti sospetti o proibiti dalla Società. Si impegna a non interrompere deliberatamente il corretto funzionamento delle risorse e delle reti IT. Se gli Utenti desiderano installare software o pacchetti software o qualsiasi applicazione sulle Risorse IT disponibili, accettano di fare una richiesta al servizio di supporto IT tramite ssp.mxns.com.

È vietato collegare risorse informatiche diverse da quelle dell'Azienda alla rete cablata delle sedi dell'Azienda. Se necessario, dovranno essere utlizzate connessioni Wi-Fi "Guest" per apparecchiature personali o di terze parti . Il Supporto IT ha facoltà di interrompere la connessione in caso di rischio per la Società o abuso.

Scambi inrete

L'Utente dovrà vigilare sulle informazioni inviate e ricevute (disinformazione, virus informatici, tentativi di frode, catene, phishing, ...) e sui siti web ai quali si collega. Qualsiasi sospetto o informazione ricevuta in merito a un problema di sicurezza del computer deve essere segnalata al reparto di supporto IT tramite ssp.mxns.com. È vietato inviare, trasmettere, scaricare, importare, creare o visualizzare e-mail, allegati o elementi trovati su Internet che siano inappropriati e costituiscano una violazione dei valori politici, delle procedure, delle direttive o delle istruzioni della Società.

Le informazioni scambiate elettronicamente con terze parti possono, in termini legali, costituire un contratto a determinate condizioni o essere utilizzate come prove legali. L'Utente deve, quindi, fare attenzione al tipo di informazioni che scambia elettronicamente oltre che per posta tradizionale. L'Utente è informato che la posta elettronica è un documento amministrativo riconosciuto come prova in caso di contenzioso.

Utilizzo dello spazio di archiviazione

Lo spazio di archiviazione dell'azienda è Google Drive. La Società si impegna solo a recuperare i dati archiviati su Google Drive.

Qualsiasi archiviazione di file aziendali su server o altre applicazioni diverse da Google Drive deve essere discussa e approvata a monte dal reparto IT.

Dispositivi di memorizzazione (es .: chiave USB, disco rigido esterno) di origine sconosciuta non devono essere collegati ai computer e alle apparecchiature aziendali. L'utilizzo dei dispositivi di archiviazione deve essere temporaneo per limitare qualsiasi rischio di perdita di dati. I file memorizzati su questi dispositivi devono essere eliminati dopo l'uso.

Il trasferimento di file tra gli Utenti dell'Azienda avviene tramite link dinamici a Google Drive le cui condivisioni devono essere gestite con cura e non come allegati di posta elettronica.

Archiviazione di file e informazioni private

Tutti i dati sono considerati aziendali ad eccezione dei dati chiaramente contrassegnati dall'Utente come privati (aggiungendo la parola "PERSONALE" o "PRIVATO"). L'archiviazione privata di file e informazioni è tollerata sul computer e su Google Drive fintanto che rimane limitata. Non dovrebbe occupare server e altre applicazioni.

Procedura di controllo in caso di smarrimento o furto

In caso di smarrimento, furto di apparecchiature o utilizzo fraudolento, l'Utente deve informare immediatamente il Dipartimento IT tramite ssp.mxns.com e riferire al Local Data Champion / DPO tramite il collegamento MXNS Connect di violazione dei dati. Il Data Champion valuterà la necessità di segnalare la violazione della sicurezza alle autorità locali.

Il Dipartimento IT può cancellare da remoto tutti i dati dell'Azienda presenti sul dispositivo e, in qualsiasi momento, procedere alla cancellazione dei dati dell'Azienda in caso di utilizzo sospetto di un dispositivo mobile.

8. TELEFONIA

Uso personale della telefonia per viaggi d'affari

L'uso personale del telefono è tollerato durante i viaggi di lavoro, purché giustificato dalle normali esigenze della vita familiare e utilizzato entro limiti ragionevoli. L'Utente è informato che la Società può avere accesso alla cronologia delle attività del dipendente, sia su rete fissa che su dispositivi mobili, solo per un motivo legittimo come di seguito indicato. Tale cronologia verrà utilizzata per fini statistici, di controllo interno e di verifica nei limiti previsti dalla legge.

9. REGOLAMENTI LOCALI CHE FORNISCONO REGOLE DIVERSE DA QUESTA POLICY

Questa Policy ha lo scopo di fornire uno standard minimo da seguire. Nella misura in cui qualsiasi legge applicabile fornisce standard superiori o aggiuntivi, tali standard devono essere seguiti in aggiunta a questa Policy. Tuttavia, se il rispetto di questa Policy è in conflitto con qualsiasi legge applicabile, è necessario attenersi alla legge e informare il dipartimento Affari legali e compliance del conflitto.

10. SANZIONI

Il mancato rispetto dei requisiti della presente Policy o delle sue procedure comporterà un'azione disciplinare fino alla cessazione del rapporto di lavoro.

11. PORRE DOMANDE O COMUNICARE RISCHI IDENTIFICATI

Questa Policy non affronta tutte le situazioni che potresti incontrare sul lavoro. Se c'è una situazione che pensi possa rappresentare un rischio e non sei sicuro di come gestirla, dovresti chiedere consiglio. Il supporto è disponibile presso il tuo team IT, dal tuo manager e dal tuo dipartimento Affari legali e compliance.

È possibile contattare l'Ufficio Affari legali e compliance tramite e-mail all'indirizzo compliance@mxns.com. Le tue domande o dubbi rimarranno confidenziali nella massima misura possibile e riceveranno un riscontro rapido e appropriato.

* *

*