POLITICA DI SICUREZZA DELLE

INFORMAZIONI DI

PHOENIX TOWER INTERNATIONAL

Revisionata il 10 maggio 2021

Indice

Scopo

Phoenix Tower US Holdings, LP e le sue consociate e affiliate in tutto il mondo (collettivamente "PTI", "Phoenix Tower" o "Società"), si impegnano a proteggere la sicurezza delle informazioni e ad apprendere e migliorare continuamente, come stabilito nella presente Politica di sicurezza delle informazioni (la "Politica"). L'ambito di questa Politica vuole essere globale e includerà i requisiti della Società per la sicurezza e la protezione delle risorse PTI, comprese le informazioni di identificazione personale ("PII"), in tutta la Società e i suoi fornitori approvati sia all'interno che all'esterno dei locali di lavoro. Tutti i dipendenti devono esaminare e seguire le informazioni contenute in questa politica.

Ambito

Questa politica si applica a tutti i dipendenti e fornitori di Phoenix Tower che supportano o interagiscono con Phoenix Tower e le sue risorse informative. Ciascuna sezione di questa Politica si applica ad aspetti specifici del programma di sicurezza delle informazioni di PTI.

Definizioni

- **Informazioni riservate:** tutte le informazioni materiali, non pubbliche, relative all'attività commerciale, scritte o orali, contrassegnate o meno come tali, relative a questioni quali strategia aziendale, processi, dati finanziari, piani di marketing, contratti e/o tecnologia. Esempi inclusi:
  - Contratti, sia eseguiti che in bozza;
  - Materiali di marketing in fase di sviluppo; o
  - Proiezioni di vendite o entrate.
- **Sicurezza delle informazioni:** i processi e le metodologie progettati e implementati per proteggere la stampa, l'elettronica o qualsiasi altra forma di informazioni o dati riservati, privati o sensibili da accesso, uso, uso improprio, divulgazione, distruzione, modifica o interruzione non autorizzati.
- **Dipendente:** una persona fisica identificata o identificabile che agisca in qualità di direttore, funzionario, membro del team di PTI, dipendente, appaltatore o consulente, a tempo pieno o part-time, su base temporanea o permanente.
- **Dispositivi interattivi per l'utente finale:** qualsiasi strumento o dispositivo tecnologico utilizzato da un dipendente PTI per archiviare informazioni o accedere ai sistemi PTI, inclusa la posta elettronica. Esempi di dispositivi rivolti agli utenti finali includono computer, laptop, smartphone, dischi rigidi esterni e dispositivi di archiviazione USB.
- **Informazioni di identificazione personale ("PII"):** qualsiasi dato che potrebbe potenzialmente identificare un individuo specifico, come nome, e-mail, informazioni finanziarie, numero di previdenza sociale, numero di passaporto, ecc.

Supervisione delle politiche

Phoenix Tower considera la sicurezza delle informazioni uno degli aspetti più importanti della sua attività.

- L'alta dirigenza di Phoenix Tower darà il buon esempio assicurando che la sicurezza delle informazioni abbia un'elevata priorità in tutte le attività e iniziative aziendali attuali e future.

- La presente Politica e ciascuna delle sue appendici saranno riviste annualmente dal Consulente generale globale per garantire che siano pertinenti, aggiornate e riviste, se necessario, per garantire che siano adeguate alla luce dell'evoluzione degli obblighi legali, della tecnologia e delle esigenze aziendali.
- La direzione comunicherà le revisioni della politica a tutto il personale con vari mezzi, come aggiornamenti elettronici, briefing, formazione, newsletter, ecc.

Per raggiungere o superare questi obiettivi, sono state messe in atto le seguenti pratiche:

- I dipendenti firmano un avviso di ricezione, revisione e riconoscimento della politica di sicurezza delle informazioni quando vengono assunti.
- La consapevolezza del personale sarà periodicamente rafforzata affinché le questioni di sicurezza delle informazioni siano al centro dell'attenzione.
- La formazione individuale in Sicurezza delle informazioni è obbligatoria a partire dall'inserimento dei dipendenti, con qualsiasi formazione tecnica adeguata alle responsabilità della funzione lavorativa. Quando il personale cambia lavoro o funzione, le sue esigenze in materia di sicurezza delle informazioni devono essere rivalutate e qualsiasi nuova formazione fornita come priorità.

1. Informazioni di identificazione personale

Questa sezione ha lo scopo di guidare la protezione delle informazioni di identificazione personale raccolte da locatori, locatari, potenziali clienti e dipendenti e aiuterà i dipendenti a determinare quali informazioni possono essere divulgate a persone non dipendenti, nonché la relativa sensibilità delle informazioni che non saranno divulgate al di fuori di Phoenix Tower senza adeguata autorizzazione.

Definizioni

Phoenix Tower riconosce la necessità di mantenere la riservatezza delle PII e comprende che tali informazioni sono uniche per ogni individuo e sono generalmente limitate ai dati che sono rilevanti e necessari per i suoi scopi. Le PII coperte dalla presente Politica possono provenire da vari tipi di individui che svolgono attività per conto della Società e includono Dipendenti, candidati, appaltatori indipendenti e qualsiasi PII mantenuta sulla sua base di clienti. Le PII includono tutte le informazioni identificabili su locatori, locatari, potenziali clienti e dipendenti:

- Informazioni di contatto personali (numeri di telefono, indirizzi, ecc.);
- Numeri di previdenza sociale (o equivalenti emessi da enti governativi al di fuori degli Stati Uniti);
- Numeri di identificazione del contribuente (o equivalenti emessi da enti fiscali governativi al di fuori degli Stati Uniti);
- Numeri di identificazione del datore di lavoro (o equivalenti emessi da enti governativi al di fuori degli Stati Uniti);
- Numero di patente di guida statale o straniera o copie di carte d'identità;
- Numeri di passaporto o copie di passaporti;
- Date di nascita;
- Numeri di carte di credito o di debito aziendali o detenuti individualmente (inclusi PIN o numeri di accesso) conservati nei registri dell'organizzazione o dei fornitori approvati; o
- Informazioni sul conto bancario di PTI o di partner commerciali.

Le PII possono trovarsi in copia cartacea o in record elettronici; entrambe le forme di PII rientrano nell'ambito di applicazione della presente Politica.

Archiviazione e gestione delle informazioni che contengono PII

PII elettroniche

Le PII possono essere salvate elettronicamente con una varietà di metodi e su una varietà di dispositivi rivolti agli utenti finali, inclusi ma non limitati a quanto segue:

- Dispositivi mobili (ad esempio laptop, smartphone, tablet, computer, palmari (PDA), ecc.).
- E-mail, Internet e programmi di messaggistica istantanea che archiviano, elaborano o trasmettono dati.
- Supporti elettronici rimovibili, come unità USB, unità CD, dischi rigidi esterni, ecc., devono essere utilizzati solo per informazioni personali non sensibili. PII sensibili, come numeri di previdenza sociale, informazioni sul passaporto e dati bancari o altri dati finanziari non devono essere salvati su supporti elettronici rimovibili.
- Server locali e di proprietà di Cloud PTI.
- Server basati su cloud di terze parti.

Questa sezione della politica stabilisce i requisiti e il processo di approvazione per i dispositivi rivolti agli utenti finali di proprietà, gestiti o concessi in leasing da PTI. Qualsiasi Dispositivo rivolto all'utente finale che non sia di proprietà, concesso in locazione o gestito da PTI non potrà accedere o rimuovere alcun server locale contenente PII, a meno che non sia autorizzato, per iscritto, dal Consulente generale globale.

- **Dispositivi mobili (ad es. laptop, smartphone, tablet, palmari (PDA), ecc.)**: le PII possono essere salvate su dispositivi mobili, ma tali dispositivi devono essere protetti da password, crittografati e avere funzionalità di cancellazione remota. Questo non è un metodo preferito per memorizzare le PII e le informazioni archiviate su dispositivi mobili dovrebbero essere considerate come una posizione di archiviazione temporanea e le PII dovrebbero essere spostate su un server PTI il prima possibile.
- **E-mail, Internet e programmi di messaggistica istantanea**: la Società sconsiglia la trasmissione di PII tramite Internet o programmi di messaggistica istantanea. Quando le PII devono essere trasferite tramite e-mail, è necessario eseguire le seguenti operazioni per garantire una trasmissione sicura e ridurre al minimo il rischio di violazione dopo che è stato confermato che tali PII sono state salvate sul server locale:
    1. Proteggere con password il documento, sia pdf, word o excel. Se il documento è in un formato non facilmente protetto (es. gif o jpeg), convertire il documento in un file pdf, proteggerlo con password in questo formato e salvarlo di nuovo. A questo punto può essere eliminato e rimosso dal cestino il formato "originale".
    2. Inviare il documento tramite posta elettronica con la dicitura "**RISERVATO**" come etichetta dopo il nome dell'oggetto nella riga dell'oggetto.
    3. Contattare il destinatario per telefono per la conferma della ricezione dell'email e per fornirgli la password. ***NON INVIARE MAI LA PASSWORD NELLA E-MAIL***
    4. Eliminare l'allegato dall'e-mail inviata.

  PII sensibili, come numeri di previdenza sociale, informazioni sul passaporto e dati bancari o altri dati finanziari **non** devono essere trasmessi tramite e-mail.

  Se una PII viene ricevuta da PTI tramite Internet o programmi di messaggistica istantanea o qualsiasi altro mezzo non sicuro, le informazioni devono essere trasferite immediatamente al server PTI (prima preferenza) o spostate nella memoria di un dispositivo mobile e quindi eliminate definitivamente dal programma in cui sono state ricevute.
- **Supporti elettronici rimovibili:** è possibile salvare le PII su supporti elettronici rimovibili, come le unità USB, allo scopo di trasportare le informazioni tra i supporti. I dispositivi multimediali rimovibili devono essere protetti da password e crittografati. Questo non è un metodo preferito per archiviare le PII. Le informazioni memorizzate su un supporto elettronico rimovibile devono essere considerate come una posizione di archiviazione temporanea e le PII dovrebbero essere spostate su un server PTI il prima possibile e rimosse dal supporto rimovibile. PII sensibili, come numeri di previdenza sociale, informazioni sul passaporto e dati bancari o altri dati finanziari **non** devono essere salvati su supporti elettronici rimovibili.
- **Server di proprietà PTI locale o cloud**: il luogo preferito per l'archiviazione di tutte le PII è su server locali o basati su cloud di proprietà di PTI e questo metodo di archiviazione deve essere sempre utilizzato per primo quando disponibile. Tutte le cartelle e i dati contenenti PII devono essere chiaramente etichettati come tali e l'accesso a queste cartelle sarà limitato solo a quei Dipendenti che devono avere accesso nella funzione quotidiana del loro lavoro.

- **Archiviazione cartacea (in loco)**: le PII archiviate negli uffici devono essere protette in cassetti chiusi a chiave e preferibilmente dietro porte chiuse, se possibile. L'accesso a questi luoghi dovrebbe essere limitato a quei Dipendenti che richiedono le informazioni nello svolgimento delle loro funzioni lavorative quotidiane. Le chiavi di tali luoghi protetti devono essere conservate solo dal capo dipartimento e qualsiasi accesso fornito ai dipendenti deve essere documentato in formato registro. In nessun caso ordinario i documenti contenenti PII devono essere portati fuori dall'ufficio e tali casi che richiedono la rimozione di PII dall'ufficio richiederanno l'approvazione dell'amministratore delegato. Tutte le informazioni, i dati e i documenti contenenti PII devono essere chiaramente etichettati in modo che tutti gli utenti siano consapevoli della proprietà, della classificazione e del valore delle informazioni. Informazioni, dati e documenti contenenti PII saranno trasportati in modo sicuro e distrutti in modo sicuro, per proteggerli dalla divulgazione involontaria. Informazioni, dati e documenti contenenti PII verranno archiviati in modo sicuro quando non vengono utilizzati.
- **Archiviazione cartacea (fuori sede)**: l'archiviazione di PII in formato cartaceo fuori sede non è generalmente consentita senza l'approvazione scritta dell'amministratore delegato. I dati contenenti PII in formato cartaceo non devono essere inviati a strutture di archiviazione fuori sede come parte dei file del sito e in nessun caso tali dati devono essere archiviati nelle case dei Dipendenti. Tutte le informazioni, i dati e i documenti contenenti PII devono essere chiaramente etichettati in modo che tutti gli utenti siano consapevoli della proprietà, della classificazione e del valore delle informazioni. Informazioni, dati e documenti contenenti PII saranno trasportati in modo sicuro e distrutti in modo sicuro, per proteggerli dalla divulgazione involontaria. Informazioni, dati e documenti contenenti PII verranno archiviati in modo sicuro quando non vengono utilizzati.
- **Trasporto cartaceo:** quando le PII devono essere trasportate fuori dai locali dell'ufficio in situazioni approvate, ciò deve essere effettuato solo dai dipendenti diretti di PTI. È necessario prestare sufficiente attenzione per garantire che i dati contenenti PII siano protetti (valigetta chiusa a chiave, ecc.) e che tali dati siano sempre in possesso del Dipendente durante il trasporto.
- **Stampe cartacee:** la stampa di dati contenenti PII e archiviati elettronicamente dovrebbe essere evitata il più possibile. In situazioni in cui ciò non è possibile, il Dipendente che stampa i dati dovrà ricevere l'approvazione preventiva del capo reparto, indicando quali materiali vengono stampati e per quale motivo. Il Dipendente sarà inoltre responsabile della distruzione delle stampe cartacee e fornirà al capo reparto una dichiarazione contenente la data di distruzione, la descrizione del materiale distrutto e il metodo utilizzato.

Accesso alle PII da parte dei dipendenti

Ogni capo reparto è responsabile dell'identificazione e del mantenimento di un elenco di utenti nel proprio reparto che dovrebbero avere accesso ai file (elettronici o cartacei). L'elenco dovrebbe essere aggiornato come richiesto e come minimo dovrebbe essere rivisto annualmente e in occasione di un evento del personale (ad esempio, assunzione, separazione, licenziamento, promozione). L'elenco verrà fornito al reparto IT che a sua volta sarà responsabile di garantire che l'accesso ai file in copia digitale contenenti PII sia limitato in conformità con l'elenco. Ogni capo reparto sarà responsabile di garantire che l'accesso ai file cartacei contenenti PII sia limitato in conformità con l'elenco. I capi reparto e/o i manager da loro designati devono rivedere l'accesso degli utenti in caso di modifiche ai ruoli e alle responsabilità di un individuo interessato, o allo stato di dipendente/appaltatore indipendente (incluso ma non limitato alla risoluzione) e comunicare tempestivamente eventuali modifiche all'IT.

Requisiti normativi

È politica della Società rispettare gli statuti e le normative internazionali, federali o statali in materia di accesso, utilizzo, archiviazione e conservazione delle PII. Gli uffici legali e/o di conformità di Phoenix Tower devono supervisionare tutti i problemi di conformità normativa. Se una qualsiasi disposizione della presente Politica è in conflitto con un requisito legale della legge internazionale, federale o statale che disciplina le PII, le disposizioni della Politica in conflitto saranno sostituite.

Formazione

A tutti i nuovi assunti che entrano nella Società viene fornita una formazione introduttiva sulla corretta gestione e protezione delle PII e viene fornita una copia della presente Politica e delle procedure di attuazione per il dipartimento a cui sono assegnati (se presenti). I dipendenti in posizioni con accesso regolare e continuativo alle PII o quelli trasferiti in tali posizioni ricevono una formazione che rafforza la presente Politica e le procedure per il mantenimento dei dati PII e riceveranno una formazione in merito alla sicurezza e alla protezione dei dati PII e dei dati di proprietà dell'azienda almeno una volta all'anno. La formazione sarà guidata dal dipartimento IT e farà parte del nuovo orientamento dei dipendenti nel caso di nuovi dipendenti. Se un Dipendente esistente viene aggiunto all'elenco di accesso PII, il Dipendente riceverà una formazione separata sulle disposizioni di questa Politica.

Conferma di riservatezza

Tutti i dipendenti della società devono mantenere la riservatezza delle informazioni personali e delle informazioni riservate dell'azienda a cui possono avere accesso e comprendere che tali informazioni personali devono essere limitate solo a coloro che hanno necessità di conoscerle.

Violazioni dei dati PII/incidenti di sicurezza

Se un Dipendente viene a conoscenza di qualsiasi utilizzo, accesso o trasferimento di PII in conflitto con questa Politica o qualsiasi incidente di sicurezza, il Dipendente deve segnalarlo immediatamente all'ufficio legale di Phoenix Tower. Database o set di dati che includono PII possono essere violati inavvertitamente o attraverso intrusioni illecite. Si prega di consultare la sezione 6 di questa politica per ulteriori informazioni.

Violazioni delle politiche e procedure PII

Phoenix Tower considera la protezione dei dati PII della massima importanza. Le infrazioni alla presente Politica o alle sue procedure comporteranno azioni disciplinari, che possono includere la sospensione o la risoluzione in caso di violazioni gravi o ripetute.

Monitoraggio dell'utilizzo dei sistemi informatici

La Società ha il diritto e la capacità di monitorare le informazioni elettroniche create e/o comunicate da persone che utilizzano i sistemi e le reti informatiche della Società, inclusi i messaggi di posta elettronica e l'utilizzo di Internet. Non è politica o intenzione della Società monitorare continuamente l'utilizzo del computer da parte dei dipendenti o di altri utenti dei sistemi informatici e della rete della Società. Tuttavia, gli utenti dei sistemi devono essere consapevoli del fatto che la Società può monitorare l'utilizzo, inclusi, a titolo esemplificativo ma non esaustivo, i modelli di utilizzo di Internet (ad esempio, accesso al sito, durata on-line, l'ora di accesso

giornaliero) e i file e i messaggi elettronici dei dipendenti nella misura necessaria per garantire che Internet e altre comunicazioni elettroniche vengano utilizzate in conformità con la legge e con la politica aziendale. L'utilizzo dei sistemi e delle reti informatiche della Società sarà considerato come riconoscimento e consenso affermativo del monitoraggio sopra descritto.

2. Uso accettabile

Lo scopo di questa sezione è garantire un uso accettabile delle apparecchiature informatiche di proprietà, affittate o gestite da Phoenix Tower. Un utilizzo inappropriato espone Phoenix Tower a rischi quali attacchi di virus, compromissione di sistemi e servizi di rete, danni alla reputazione e problemi legali.

Uso generale e proprietà

- Gli utenti saranno consapevoli che i dati che creano o le applicazioni che utilizzano i dati sui sistemi aziendali rimangono di proprietà di Phoenix Tower. I dipendenti non devono avere alcuna aspettativa di privacy per le loro attività durante l'utilizzo di apparecchiature informatiche PTI e nessuna aspettativa di proprietà, anche in caso di separazione dalla Società.
- Per motivi di sicurezza e manutenzione della rete, le persone autorizzate all'interno di Phoenix Tower possono monitorare le apparecchiature, i sistemi e il traffico di rete in qualsiasi momento.
- Phoenix Tower si riserva il diritto di controllare reti e sistemi su base periodica per garantire la conformità a questa Politica.

Sicurezza e informazioni proprietarie

- Le informazioni conservate sui sistemi Phoenix Tower che contengono PII saranno chiaramente etichettate come tali in conformità con la sezione Informazioni di identificazione personale di questa Politica. Gli utenti si adopereranno per mantenere queste informazioni al sicuro.
- Proteggere le password e non condividere gli account. Gli utenti autorizzati sono responsabili della sicurezza e dell'integrità delle proprie password e account.
- I dipendenti devono prestare la massima attenzione quando aprono allegati di posta elettronica ricevuti da mittenti sconosciuti, che potrebbero contenere virus o malware.
- I sistemi che archiviano informazioni riservate della Phoenix Tower o che vengono utilizzati per l'elaborazione delle informazioni non devono essere rimossi dai locali della Phoenix Tower senza l'approvazione ufficiale della direzione.
- I dipendenti non devono utilizzare le funzionalità di compilazione automatica del browser Web o altre funzionalità che salvano le informazioni sull'ID utente e sulla password in applicazioni aziendali online.

Attività vietate

- Il coinvolgimento in qualsiasi attività illegale ai sensi del diritto locale, statale, federale o internazionale utilizzando risorse di proprietà della Phoenix Tower.
- L'esportazione di software, informazioni tecniche, software di crittografia o tecnologia, in violazione delle leggi internazionali o regionali sul controllo delle esportazioni, è illegale. La direzione appropriata sarà consultata prima dell'esportazione di qualsiasi materiale in questione.
- L'utilizzo di una risorsa informatica della Phoenix Tower per impegnarsi attivamente nell'acquisizione o nella trasmissione di materiale che violi le molestie sessuali o le leggi sull'ambiente di lavoro ostile.

- L’elusione dell'autenticazione dell'utente o la sicurezza di qualsiasi host, rete o account. L'uso non autorizzato di un ID di rete diverso dal proprio è severamente vietato.
- I tentativi non autorizzati di aggirare la sicurezza della rete, la protezione dei dati, la sicurezza delle password o l'installazione/l'utilizzo di software progettato per aggirare qualsiasi sicurezza o politica creata e implementata da Phoenix Tower.
- Il tentativo di manomettere o manipolare la comunicazione o i file di rete di un altro dipendente.
- La violazione delle leggi sul copyright e delle loro disposizioni sull'uso corretto, tra cui la copia o la "pirateria" di software o la violazione di licenze/accordi software.
- L’installazione di applicazioni non ufficiali su qualsiasi risorsa di Phoenix Tower senza previo consenso dell'IT.
- La divulgazione di informazioni riservate e/o segreti commerciali.
- Gli utenti non devono impegnarsi intenzionalmente ad ottenere l'accesso ai sistemi aziendali per i quali non dispongono dell'autorizzazione o per necessità aziendale di conoscere.

3. **Utilizzo della posta elettronica**

Questa sezione ha lo scopo di fornire linee guida per un uso accettabile della posta elettronica e delineare le procedure di conservazione della posta elettronica.

Uso consentito

- La posta elettronica e i sistemi di posta elettronica aziendali devono essere utilizzati solo per scopi aziendali e devono essere coerenti con le politiche e le procedure di PTI per la condotta etica, la sicurezza e la conformità alle leggi e alle pratiche aziendali applicabili. Qualsiasi comunicazione personale sull'e-mail aziendale deve essere limitata.
- I dipendenti non devono avere alcuna aspettativa di privacy in tutto ciò che archiviano, inviano o ricevono sul sistema di posta elettronica della Società. PTI può monitorare i messaggi senza preavviso.
- I dipendenti devono presentare reclamo per l'autenticazione a più fattori.

E-mail contenente informazioni personali

- Se le PII devono essere trasferite tramite e-mail, è necessario eseguire le seguenti operazioni per garantire una trasmissione sicura e ridurre al minimo il rischio di una violazione dopo che è stato confermato che tali PII sono state salvate nel server locale:
    1. Proteggere con password il documento, sia pdf, word o excel. Se il documento è in un formato non facilmente protetto (es. gif o jpeg), convertire il documento in un file pdf, proteggerlo con password in questo formato e salvarlo di nuovo. A questo punto può essere eliminato e rimosso dal cestino il formato "originale”.
    2. Inviare il documento tramite posta elettronica con la dicitura "**RISERVATO**" come etichetta dopo il nome dell'oggetto nella riga dell'oggetto.
    3. Contattare il destinatario per telefono per la conferma della ricezione dell’email e per fornirgli la password. ***NON INVIARE MAI LA PASSWORD NELLA STESSA EMAIL DELLE PII***
    4. Eliminare l'allegato dall'e-mail inviata.

PII sensibili, come numeri di previdenza sociale, informazioni sul passaporto e dati bancari o altri dati finanziari **non** devono essere inviati tramite e-mail.

- Se una PII viene ricevuta da PTI tramite e-mail, Internet o programmi di messaggistica istantanea, le informazioni devono essere trasferite immediatamente al server locale (prima preferenza) o spostate nella memoria di un dispositivo mobile e quindi eliminate definitivamente dal programma in cui sono state ricevute.

E-mail e attività di comunicazione vietate

- Utilizzo dell'e-mail PTI per usi commerciali non correlati a PTI o per uso personale frequente.
- Inoltro automatico della posta elettronica PTI a sistemi o piattaforme di posta elettronica di terze parti.
- Eliminazione o alterazione del messaggio di esclusione di responsabilità legale generato dal sistema allegato a ogni e-mail PTI.
- Invio di messaggi di posta elettronica non richiesti, incluso l'invio di "posta indesiderata" o altro materiale pubblicitario o di sollecitazione a soggetti che non hanno richiesto specificamente tale materiale (posta indesiderata).
- La creazione o la distribuzione di messaggi di disturbo o offensivi. I dipendenti che ricevono messaggi di posta elettronica con questo contenuto da qualsiasi dipendente della Phoenix Tower segnaleranno immediatamente la questione al proprio supervisore.
- Utilizzo di account di posta elettronica non Phoenix Tower (Hotmail, Gmail, et. al.) per attività ufficiali di Phoenix Tower o inoltro di e-mail ricevute in account e-mail Phoenix Tower ad account e-mail personali o non Phoenix Tower (Hotmail, Gmail, et. al.).
- Abbonamento a servizi elettronici o altri contratti che utilizzano indirizzi e-mail PTI senza un valido motivo aziendale.

Dispositivi mobili

- I dipendenti devono ottenere l'approvazione preventiva del proprio manager o supervisore prima di tentare di accedere all'e-mail PTI tramite dispositivi mobili personali.
- Phoenix Tower fornisce l'accesso alla posta elettronica tramite dispositivi mobili personali in conformità con questa politica. Phoenix Tower non è responsabile per la perdita di dati nel caso in cui un dispositivo venga cancellato (a causa di un errore dell'utente o delle funzionalità di sicurezza implementate). Questa politica si applica a tutti i dispositivi palmari dell'utente finale e a qualsiasi altro dispositivo che può accedere ai servizi di posta elettronica di Phoenix Tower e/o ai dati protetti di Phoenix Tower. La conformità a questa politica è un requisito per tutti i dispositivi palmari che archiviano o accedono ai dati protetti di Phoenix Tower.
- Gli utenti che utilizzano un dispositivo palmare per accedere a e-mail, dati, record o documenti di Phoenix Tower devono implementare le seguenti funzionalità di sicurezza nella misura in cui sono disponibili sul dispositivo:

- Essere configurato per disconnettersi o spegnersi non più di dieci (10) minuti dopo l'ultima attività dell'utente.
- Richiedere una password o un codice di accesso all'accensione.
- Richiedere una lunghezza minima della password di quattro (4) caratteri o chiavi.
- Fornire un ripristino del dispositivo (cancellazione dei dati) se viene inserita una password errata per più di otto (8) volte consecutive, se tecnicamente fattibile.
- Il dispositivo deve essere crittografato.

- Utenti che utilizzano un dispositivo palmare per accedere a posta elettronica, dati, record o documenti di Phoenix Tower devono portare il proprio dispositivo all'IT per garantire che queste funzionalità di sicurezza siano implementate.

Smaltimento dell'attrezzatura

Prima dello smaltimento o del trasferimento, tutti i dispositivi palmari e le schede di memoria associate devono essere completamente cancellati da tutti i dati della Phoenix Tower. Al termine dell'accesso di un dipendente ai sistemi Phoenix Tower, l'individuo porterà il proprio dispositivo palmare all'IT in modo che l'IT possa rimuovere tutti i dati della Phoenix Tower dal dispositivo.

Segnalazioni

- La perdita, il furto o qualsiasi utilizzo non autorizzato di un Dispositivo dell'utente finale palmare che è stato utilizzato per archiviare o accedere a informazioni protette di Phoenix Tower costituisce una divulgazione e deve essere segnalato a Phoenix Tower IT.

- L'IT si coordinerà con l'ufficio legale e il supervisore dell'utente per determinare la misura in cui un dispositivo dell'utente finale di proprietà o personale di PTI deve essere cancellato o eliminato in caso di perdita o furto e al termine del rapporto di lavoro dell'utente con PTI. Se viene stabilito che una cancellazione remota è necessaria e possibile, l'IT tenterà di limitare i dati cancellati alle sole informazioni di Phoenix Tower nella misura tecnicamente possibile sui dispositivi di proprietà di PTI e/o sui dispositivi in cui si applicano i rimborsi.

4. Uso di Internet

La Società fornirà l'accesso a Internet a dipendenti e appaltatori che sono collegati alla rete interna e che hanno una necessità aziendale di tale accesso.

Internet è uno strumento aziendale per l'Azienda. Deve essere utilizzato per scopi aziendali quali: comunicazione tramite posta elettronica con fornitori e partner commerciali, acquisizione di informazioni commerciali utili e ricerca di argomenti tecnici e commerciali rilevanti.

Il servizio Internet non può essere utilizzato per la trasmissione, il recupero o l'archiviazione di comunicazioni di natura discriminatoria o molesta o che siano dispregiative per qualsiasi individuo o gruppo, oscene o pornografiche, o diffamatorie o di natura minacciosa per "catene di Sant'Antonio" o qualsiasi altro scopo illegale o per guadagno personale.

5. **Personale**

Lo scopo di questa sezione è ridurre il rischio di errore umano, furto, frode o uso improprio delle strutture. Poiché la sicurezza delle nostre risorse informative è una componente fondamentale del nostro modello di business, è fondamentale che tutti i dipendenti di Phoenix Tower siano soggetti a determinati standard per garantire credibilità e sicurezza.

Memorizzazione di informazioni personali sui sistemi aziendali

- Nonostante il rispetto di Phoenix Tower per la privacy dei Dipendenti sul posto di lavoro, si riserva il diritto di avere accesso a tutte le informazioni create e archiviate sui sistemi di Phoenix Tower.
- Phoenix Tower ha il diritto di monitorare tutte le informazioni ricevute, archiviate, trasmesse e/o create sui sistemi di Phoenix Tower.

Condivisione di informazioni riservate

- Le informazioni riservate saranno condivise solo con altre persone autorizzate.
- Le informazioni sull'organizzazione hanno i propri livelli di sensibilità individuali e non devono essere divulgate al personale che non dispone dell'autorizzazione per accedere a tali informazioni.
- Tutti i dati e le informazioni non di dominio pubblico, relativi all'attività di Phoenix Tower e ai suoi dipendenti, devono rimanere sempre riservati.
- Le informazioni riservate non devono essere divulgate ai familiari che non hanno l'autorizzazione a ricevere tali informazioni.

6. Sicurezza fisica

Questa sezione vieta l'accesso fisico non autorizzato ai locali e alle informazioni di Phoenix Tower e previene danni o interferenze con le normali operazioni aziendali. Questa politica copre anche tutta la sicurezza fisica degli ingressi, delle strutture di lavoro degli uffici e di altre aree critiche che devono essere protette per proteggere le risorse.

Sicurezza fisica

- Per proteggere le aree con informazioni critiche sono in uso porte di sicurezza, lettori di badge e tastiere con PIN. Solo i dipendenti autorizzati possono accedere a queste aree protette.
- Il personale sarà monitorato elettronicamente in base alle aree a cui è stato concesso l'accesso. Questo per mitigare i pericoli di furto, vandalismo e uso non autorizzato dei sistemi.
- Le aree in cui vengono gestite le informazioni protette (inclusi l'elaborazione delle informazioni e le strutture informatiche) saranno soggette a severi controlli di accesso per garantire che non sia consentito l'accesso a dipendenti non autorizzati o persone esterne all'organizzazione.

Protezione delle postazioni di lavoro e delle strutture di lavoro incustodite

- L'attrezzatura deve essere sempre adeguatamente protetta, soprattutto se lasciata incustodita.
- Prima di lasciare la scrivania, se la scrivania sarà fuori vista, il computer deve essere disconnesso o bloccato per impedire l'accesso non autorizzato.
- Le stampanti e i fax verranno ripuliti quotidianamente dai dati sensibili. I documenti sensibili inviati a stampanti o fax devono essere protetti non appena vengono stampati.

Prestito di chiavi, codici di sicurezza o badge di accesso di sicurezza ad altri

- L'utilizzo delle chiavi, sia fisiche che elettroniche, per accedere ad aree protette deve essere strettamente limitato al dipendente a cui sono state assegnate le chiavi. È vietato il prestito di chiavi, codici di sicurezza o badge di accesso di sicurezza a dipendenti non PTI e/o persone esterne.
- Il mancato rispetto di questa Politica potrebbe essere visto come una violazione della sicurezza ed è soggetto ad azione disciplinare.

Gestione degli estranei nei locali

- Se un estraneo non è accompagnato da un dipendente di Phoenix Tower, i dipendenti ne metteranno in dubbio la presenza nei locali dell'organizzazione.

7. Controllo di accesso

Una componente fondamentale della nostra politica di sicurezza delle informazioni è il controllo dell'accesso alle risorse di informazioni critiche che richiedono protezione dalla divulgazione o modifica non autorizzata. Il significato fondamentale del controllo degli accessi è che le autorizzazioni vengono assegnate a individui o sistemi autorizzati ad accedere a risorse specifiche. I controlli di accesso esistono a vari livelli del sistema, inclusa la rete. Il controllo degli accessi è implementato dall'ID di accesso e dalla password. A livello di applicazione e database, è possibile implementare altri metodi di controllo dell'accesso per limitare ulteriormente l'accesso. L'applicazione e i sistemi di database possono limitare il numero di applicazioni e database disponibili per gli utenti in base ai loro requisiti di lavoro.

Sistema utente e accesso alla rete - Identificazione utente normale

A tutti gli utenti verrà richiesto di disporre di un ID di accesso e di una password univoci per l'accesso ai sistemi. La password dell'utente deve essere mantenuta riservata e NON DEVE essere condivisa con il personale di gestione e supervisione e/o qualsiasi altro dipendente. Tutti gli utenti devono rispettare le seguenti regole relative alla creazione e al mantenimento delle password:

- La password deve essere complessa, cioè, non utilizzare alcun nome, nome, verbo, avverbio o aggettivo comune. Queste semplici password possono essere facilmente violate utilizzando gli "strumenti hacker" standard.
- Le password non devono essere pubblicate su o vicino ai terminali dei computer o comunque essere facilmente accessibili nel terminale.
- La password deve essere modificata ogni 60 giorni.
- Gli account utente verranno congelati dopo 5 tentativi di accesso non riusciti.
- Gli ID di accesso e le password verranno sospesi dopo 20 giorni di inattività.

Agli utenti non è consentito accedere ai file delle password su alcun componente dell'infrastruttura di rete. I file delle password sui server verranno monitorati per l'accesso da parte di utenti non autorizzati. È severamente vietato copiare, leggere, eliminare o modificare un file di password su qualsiasi sistema informatico.

Agli utenti non sarà consentito accedere come amministratore di sistema. Gli utenti che necessitano di questo livello di accesso ai sistemi di produzione devono richiedere un account di accesso speciale come descritto altrove in questo documento.

Gli ID di accesso e le password dei dipendenti verranno disattivati il prima possibile se il dipendente viene separato, ha cessato di prestare servizio, viene licenziato, sospeso, messo in congedo o lascia in altro modo l'ufficio della Società.

I supervisori / manager devono contattare immediatamente e direttamente il dipartimento IT della Società per segnalare qualsiasi cambiamento nello stato dei dipendenti che richieda la cessazione o la modifica dei privilegi di accesso dei dipendenti.

I dipendenti che dimenticano la password devono chiamare il reparto IT o seguire gli strumenti forniti per l'IT per ottenere una nuova password assegnata al proprio account. Il dipendente deve identificarsi tramite (ad esempio, il numero del dipendente) al reparto IT.

I dipendenti saranno responsabili di tutte le transazioni che si verificano durante le sessioni di accesso avviate utilizzando la password e l'ID del dipendente. I dipendenti non devono accedere a un computer e quindi consentire a un'altra persona di utilizzare il computer o condividere in altro modo l'accesso ai sistemi informatici.

Accesso dell'amministratore di sistema

Gli amministratori di sistema, gli amministratori di rete e gli amministratori della sicurezza avranno accesso con privilegi elevati a sistemi host, router, hub e firewall come richiesto per svolgere i compiti del loro lavoro.

Tutte le password dell'amministratore di sistema verranno **ELIMINATE** immediatamente dopo che qualsiasi dipendente che ha accesso a tali password viene separato, ha cessato di prestare servizio, viene licenziato o altrimenti interrompe il rapporto di lavoro con l'azienda. Le password dei dipendenti in congedo amministrativo o disciplinare saranno sospese fino al ripristino dello status di lavoratore attivo.

Accesso speciale

Gli account di accesso speciale vengono forniti alle persone che richiedono privilegi temporanei di amministratore di sistema per svolgere il proprio lavoro. Questi account sono monitorati dalla Società e richiedono l'autorizzazione dell'IT aziendale dell'utente. Il monitoraggio degli account ad accesso speciale avviene inserendo gli utenti in una specifica area e generando periodicamente rapporto alla direzione. I rapporti mostreranno chi ha attualmente un account di accesso speciale, per quale motivo e quando scadrà. Gli account speciali scadranno dopo 2 giorni e non verranno rinnovati automaticamente senza autorizzazione scritta.

Connessione a reti di terze parti

Questa politica è stabilita per garantire un metodo di connettività sicuro fornito tra la Società e tutte le società di terze parti e altre entità richieste per lo scambio elettronico di informazioni con la Società.

"Terze parti" si riferisce a fornitori, consulenti e partner commerciali che fanno affari con la Società e altri partner che hanno la necessità di scambiare informazioni con la Società. Le connessioni di rete di terze parti devono essere utilizzate solo dai dipendenti della terza parte, solo per gli scopi aziendali della Società. La Società di terze parti garantirà che solo gli utenti autorizzati potranno accedere alle informazioni sulla rete della Società. La terza parte non consentirà al traffico Internet o ad altro traffico di rete privata di fluire nella rete aziendale. Una connessione di rete di terze parti è definita come una delle seguenti opzioni di connettività:

- Una connessione di rete verrà terminata su un firewall e la terza parte sarà soggetta alle regole di autenticazione aziendale standard.

Questa politica si applica a tutte le richieste di connessione di terze parti e a tutte le connessioni di terze parti esistenti. Nei casi in cui le connessioni di rete di terze parti esistenti non soddisfino i requisiti delineati in questo documento, verranno ridisegnate secondo necessità.

Tutte le richieste di connessioni di terze parti devono essere effettuate inoltrando una richiesta scritta ed essere approvate dal reparto IT.

Collegamento dei dispositivi alla rete

Solo i dispositivi autorizzati possono essere collegati alle reti aziendali. I dispositivi autorizzati includono PC e workstation di proprietà dell'Azienda conformi alle linee guida di configurazione dell'Azienda. Altri dispositivi autorizzati includono i dispositivi dell'infrastruttura di rete utilizzati per la gestione e il monitoraggio della rete.

Gli utenti non devono collegarsi alla rete: computer non aziendali non autorizzati, posseduti e/o controllati dalla Società. Agli utenti è espressamente vietato collegare dispositivi non aziendali come laptop, computer, dischi rigidi esterni, telefoni, tablet alla rete aziendale.

NOTA: gli utenti non sono autorizzati a collegare alcun dispositivo che altererebbe le caratteristiche della topologia della rete o qualsiasi dispositivo di archiviazione non autorizzato (ad esempio, pen drive e CD scrivibili).

Accesso remoto

Solo le persone autorizzate possono accedere da remoto alla rete aziendale. L'accesso remoto viene fornito a quei dipendenti, appaltatori e partner commerciali della Società che hanno una legittima esigenza aziendale di scambiare informazioni, copiare file o programmi o accedere ad applicazioni informatiche. Le connessioni autorizzate possono essere un PC remoto alla rete o una rete remota alla connessione di rete aziendale. L'unico metodo accettabile per connettersi in remoto alla rete interna è l'utilizzo di un ID protetto.

Accesso remoto non autorizzato

Il collegamento di hub al PC o alla stazione di lavoro di un utente che è connesso alla rete locale (LAN) aziendale è vietato senza l'autorizzazione scritta della Società. Inoltre, gli utenti non possono installare software personale progettato per fornire il controllo remoto del PC o della workstation. Questo tipo di accesso remoto aggira i metodi di accesso remoto altamente sicuri autorizzati e rappresenta una minaccia per la sicurezza dell'intera rete.

8. **Risposta agli incidenti e segnalazione di violazione dei dati**

In caso di incidente di sicurezza, è importante che i dipendenti di Phoenix Tower siano in grado di identificarsi e rispondere in modo appropriato. Ogni potenziale incidente sarà indagato a un livello ritenuto appropriato dall'ufficio legale e dall'IT. Rispondere in modo appropriato e tempestivo agli incidenti di sicurezza delle informazioni aiuterà a proteggere le risorse di Phoenix Tower.

Segnalazioni

- Ogni Dipendente è responsabile della segnalazione immediata di tutte le debolezze della sicurezza delle informazioni identificate o sospette, incluse, a titolo esemplificativo ma non esaustivo, violazioni dei dati PII potenziali o effettive, all'IT e/o all'ufficio legale/conformità:
    - Hotline: 1-844-348-5247 o https://secure.ethicspoint.com
    - E-mail: security@phoenixintnl.com
- Anche una violazione della riservatezza o la divulgazione non autorizzata delle Informazioni riservate di Phoenix Tower è considerata un incidente di sicurezza delle informazioni e deve essere segnalata come descritto sopra.

- L'IT registrerà gli incidenti di sicurezza segnalati per monitorare sia i tipi di incidenti di sicurezza che il volume degli incidenti che si verificano a Phoenix Tower.
- Le prove relative a una violazione della sicurezza delle informazioni devono essere adeguatamente raccolte come indicato dal responsabile del reparto IT e inoltrate al reparto IT. Devono essere raccolte per adempiere ad obblighi di legge, regolamentari o contrattuali ed evitare violazioni di diritto penale o civile?
- Dopo aver condotto un'indagine iniziale, il responsabile del reparto IT determinerà se l'evento è effettivamente un incidente di sicurezza delle informazioni. Se si è verificato un incidente di sicurezza, l'Ufficio legale determinerà se l'incidente costituisce una violazione dei dati per la quale è richiesta la segnalazione e delle violazioni dei dati che coinvolgono PII.
- L'ufficio legale manterrà un registro degli incidenti di sicurezza segnalati che costituiscono una violazione dei dati.
- Le informazioni relative agli incidenti di sicurezza delle informazioni possono essere rilasciate solo da persone autorizzate. I dipendenti non possono rilasciare alcuna informazione riguardante un incidente di sicurezza al di fuori di PTI senza l'espressa autorizzazione del team legale.
- In seguito all'incidente o alla violazione dei dati, il reparto IT sarà responsabile della conduzione di una riunione con tutti i dipendenti e le parti interessate/ applicabili per esaminare i risultati dell'indagine e per discutere la causa principale dell'incidente. Tutti i dipendenti coinvolti nella scoperta o nell'indagine di un incidente di sicurezza sono tenuti a partecipare a questa riunione.
- I dipendenti di Phoenix Tower o appaltatori di terze parti coinvolti in un incidente di sicurezza o che abbiano violato la Politica di sicurezza delle informazioni di Phoenix Tower, indipendentemente dalle intenzioni, dovranno affrontare un comitato disciplinare, che determinerà la colpa, la correzione e altre azioni appropriate.