Politica sulla sicurezza delle informazioni

Analisi del Contesto

Nome della società	Carol
Data di entrata in vigore	22/10/2024

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1.0	22/10/2024	-- N/D --	Daniele Berto	Lorenzo Granato

Scopo

Questa politica di sicurezza delle informazioni ha lo scopo di proteggere i dipendenti, i partner e l’azienda Carol da azioni illegali o dannose da parte di singoli individui, consapevolmente o inconsapevolmente. I sistemi relativi a Internet/ Intranet/ Extranet, inclusi ma non limitati a apparecchiature informatiche, software, sistemi operativi, supporti di memorizzazione, account di rete che forniscono posta elettronica, navigazione Web e trasferimenti di file, sono di proprietà dell’azienda. Questi sistemi devono essere utilizzati per scopi aziendali al servizio degli interessi dell'azienda e dei nostri clienti e clienti nel corso delle normali operazioni. Una sicurezza efficace è un lavoro di squadra che prevede la partecipazione e il sostegno di tutti i dipendenti o collaboratori dell’azienda che si occupano di informazioni e/o sistemi informativi. È responsabilità di ogni membro del team leggere e comprendere questa procedura e condurre le proprie attività di conseguenza.

Indice

- Attività di posta elettronica e comunicazione
- Conformità alle politiche
- Eccezioni
- Violazioni e applicazione

Scopo

Questa politica di sicurezza delle informazioni ha lo scopo di proteggere i dipendenti, i partner e l’azienda Carol da azioni illegali o dannose da parte di singoli individui, consapevolmente o inconsapevolmente.

I sistemi relativi a internet, inclusi ma non limitati a apparecchiature informatiche, software, sistemi operativi, supporti di memorizzazione, account di rete che forniscono posta elettronica, navigazione Web e trasferimenti di file, sono di proprietà dell’azienda. Questi sistemi devono essere utilizzati per scopi aziendali al servizio degli interessi dell'azienda e dei nostri clienti e clienti nel corso delle normali operazioni. Una sicurezza efficace è un lavoro di squadra che prevede la partecipazione e il sostegno di tutti i dipendenti o collaboratori dell’azienda che si occupano di informazioni e/o sistemi informativi. È responsabilità di ogni membro del team leggere e comprendere questa procedura e condurre le proprie attività di conseguenza.

Segnalazione di incidenti di sicurezza

Tutti i dipendenti sono tenuti a segnalare eventi o incidenti di sicurezza noti o sospetti, comprese le violazioni delle policy ed eventuali vulnerabilità di sicurezza osservate. Gli incidenti devono essere segnalati immediatamente o al più presto possibile alle persone di riferimento in base alla gravità. Gli incidenti critici (S1) vanno inviati a lorenzo@carol.health, mentre per gravità alta (S2) si può far riferimento a daniele.berto@carol.health o alternativamente a pietro.lerro@carol.health. Nell'inviare la segnalazione si prega di descrivere l'incidente o l'osservazione insieme a tutti i dettagli rilevanti.

Segnalazione di frodi

Le politiche sulla sicurezza delle informazioni hanno lo scopo di incoraggiare e consentire ai dipendenti e ad altri, di sollevare internamente eventuali preoccupazioni in modo da poter affrontare e correggere comportamenti/ azioni inappropriate. È responsabilità di tutte le parti interessate nella presente politica, segnalare dubbi circa violazioni del codice etico dell'azienda o sospette violazioni delle leggi/ regolamenti a cui l'azienda deve sottostare.

Va contro i valori di Carol chiunque effettui ritorsioni contro un dipendente o chi, in buona fede, segnali una violazione dell'etica o una sospetta violazione della legge, frode o sospetta violazione di qualsiasi regolamento. Un dipendente che effettua ritorsioni contro qualcuno che ha segnalato una violazione in buona fede è soggetto a sanzioni disciplinari, fino al possibile licenziamento.

Dispositivi mobili

Tutti i dispositivi mobili che rientrano tra gli asset aziendali ed assegnati ai dipendenti, collaboratori esterni o partner dell'azienda (ad esempio telefoni cellulari, tablet, laptop) devono essere conformi a quanto definito dal presente paragrafo. I dipendenti devono prestare la massima attenzione quando aprono allegati di posta elettronica ricevuti da mittenti sconosciuti, che potrebbero contenere malware.

Le password a livello di sistema e a livello utente devono essere conformi alla Politica di controllo degli accessi. È vietato fornire l'accesso ad un esterno sconosciuto, deliberatamente o attraverso la mancata messa in sicurezza di un dispositivo.

Tutti i dispositivi di proprietà dell'azienda assegnati all'utente finale, utilizzati per l'accesso ai sistemi informativi (ad esempio la posta elettronica) dell'azienda devono rispettare le seguenti regole e requisiti:

- **Riservatezza**: I dipendenti sono tenuti a mantenere la riservatezza delle informazioni e dei dati aziendali accessibili tramite questi dispositivi
- **Uso autorizzato**: I dispositivi devono essere utilizzati solo per scopi lavorativi e da personale autorizzato
- **Misure di sicurezza**: I dipendenti devono implementare misure di sicurezza come password forti e crittografia per proteggere le informazioni sensibili
- **Monitoraggio**: I dipendenti devono essere consapevoli che l'uso dei dispositivi aziendali può essere monitorato per garantire la conformità alle politiche aziendali
- **Segnalazione di problemi**: Qualsiasi perdita, furto o danno ai dispositivi deve essere segnalato immediatamente al dipartimento IT
- **Conformità software**: Solo i software autorizzati devono essere installati sui dispositivi aziendali
- **Protezione dei dati**: I dipendenti devono seguire le politiche di protezione dei dati, inclusa la gestione e la conservazione sicura delle informazioni sensibili.

Dispositivi mobili personali (BYOD - Bring Your Own Device)

Per tutti i dispositivi BYOD, ovvero di proprietà di dipendenti, partner o collaboratori dell'azienda, quali ad esempio telefoni cellulari, tablet, laptop e che, quindi, non rientrano tra gli asset aziendali, è necessario che gli utenti siano consapevoli di quanto indicato di seguito:

1. **Autenticazione e accesso:** I sistemi aziendali sono coperti da un'autenticazione a più fattori che richiede l'utilizzo di una Authenticator App
2. **Condivisione documenti:** La condivisione dei documenti aziendali è consentita solo tramite canali autorizzati e sicuri come Google Workspace o altre piattaforme aziendali approvate. È vietato l'utilizzo di piattaforme non autorizzate per evitare rischi di esposizione o compromissione dei dati

3. **Crittografia dei dati:** Tutti i dati aziendali memorizzati sui dispositivi personali devono essere protetti tramite crittografia, di conseguenza è d'obbligo fornire una evidenza in cui si dimostri l'attivazione di Bitlocker su dispositivi Windows o di Filevault su dispositivi Apple
4. **Protezione dalle minacce:** È obbligatorio l'utilizzo di un software antivirus aggiornato e la configurazione di un firewall sui dispositivi personali. Gli utenti devono fornire evidenze dell'utilizzo (screenshot) e assicurarsi che l'antivirus sia mantenuto aggiornato e operativo, con aggiornamenti automatici attivati
5. **Accesso ai dati sensibili:** L'accesso ai dati sensibili dei pazienti deve essere limitato solo ai soggetti autorizzati, in conformità con la normativa vigente e la ISO 27001
6. **Gestione delle applicazioni:** È vietata l'installazione di software non autorizzato che possa compromettere la sicurezza dei dati aziendali, in caso di dubbio è necessario consultare il reparto IT
7. **Aggiornamenti e patch di sicurezza:** I dispositivi devono essere mantenuti aggiornati con le ultime patch di sicurezza aggiornamenti del sistema operativo, il collaboratore ha l'obbligo di attivare gli aggiornamenti automatici del sistema operativo e di fornirne evidenza tramite screenshot
8. **Report di incidenti:** Qualsiasi incidente di sicurezza deve essere immediatamente segnalato a Support per una pronta gestione e risoluzione.
9. **Riservatezza:** È responsabilità dell'utente assicurarsi che i dati aziendali memorizzati sui dispositivi personali non siano accessibili a persone non autorizzate.
10. **Formazione:** L'utente sarà tenuto a seguire una formazione sulla security awareness fornita dall'azienda. La formazione verrà erogata in maniera graduale con moduli brevi durante tutto il corso della collaborazione.

Clean screen e clear desk

I dipendenti non dovranno lasciare materiali riservati non protetti sulla propria scrivania o spazio di lavoro e si assicureranno che gli schermi siano bloccati quando non vengono utilizzati seguendo le linee guida previste dal MdM adottato.

Lavoro e accesso da remoto

Il lavoro a distanza si riferisce a qualsiasi situazione in cui il personale organizzativo opera da luoghi esterni all'ufficio. Ciò include il telelavoro, il luogo di lavoro flessibile, gli ambienti di lavoro virtuali e la manutenzione remota. Laptop e altre risorse informatiche utilizzate per accedere alla rete aziendale devono essere conformi ai requisiti di sicurezza definiti nella Politica sulla sicurezza delle informazioni e aderire ai seguenti standard:

- È necessario seguire le regole aziendali durante il lavoro in remoto, inclusi protocolli di scrivania pulita, stampa, smaltimento di risorse e segnalazione di eventi di sicurezza delle informazioni per prevenire la gestione impropria o l'esposizione accidentale di informazioni sensibili.
- Per garantire che i dispositivi mobili non contengano virus che potrebbero compromettere la rete aziendale, si richiede l'installazione di software antivirus lato dipendente.
- Il software antivirus deve essere configurato per rilevare e prevenire o mettere in quarantena software dannoso, eseguire scansioni periodiche del sistema e abilitare gli aggiornamenti automatici.
- Quando il dipendente si collega da una rete domestica, si deve assicurare che le impostazioni del Wi-Fi predefinite siano modificate, come nome, password e accesso amministratore.
- I dipendenti non devono connettersi a nessuna rete esterna senza un firewall software sicuro e aggiornato configurato sul computer portatile.

- Ai dipendenti è vietato modificare o disattivare eventuali controlli di sicurezza organizzativi quali firewall personali, software antivirus sui sistemi utilizzati per accedere alle risorse aziendali.
- Le tecnologie di accesso remoto non autorizzate non possono essere utilizzate o installate su alcun sistema aziendale.

Utilizzo accettabile

Informazioni proprietarie e dei clienti archiviate su dispositivi elettronici e informatici, di proprietà o noleggiati dall'organizzazione, del dipendente o di un terzo, rimangono di proprietà esclusiva dell'azienda. I dipendenti e i collaboratori esterni devono garantire, attraverso mezzi legali o tecnici, che le informazioni proprietarie siano protette in conformità con la procedura di Politica di gestione delle informazioni. L'impiego di Google Drive per l'archiviazione di file aziendali è obbligatorio per i dipendenti che hanno laptop o dispositivi forniti dall'azienda.

Il dipendente ha la responsabilità di segnalare tempestivamente il furto, lo smarrimento o la divulgazione non autorizzata di informazioni o apparecchiature proprietarie dell'azienda. È possibile accedere, utilizzare o condividere informazioni proprietarie dell'azienda solo nella misura in cui è autorizzato e necessario per adempiere alle mansioni lavorative assegnate. I dipendenti sono tenuti ad esercitare il buon senso riguardo alla ragionevolezza dell'uso personale dei dispositivi forniti dall'azienda. Per scopi di sicurezza e manutenzione della rete, le persone autorizzate all'interno dell'azienda possono monitorare apparecchiature, sistemi e traffico di rete in qualsiasi momento. L'azienda si riserva il diritto di verificare periodicamente reti e sistemi per garantire il rispetto di questa procedura.

Utilizzo non accettabile

Le seguenti attività sono, in generale, vietate. I dipendenti possono essere esentati da queste restrizioni durante lo svolgimento delle loro legittime responsabilità lavorative, previa approvazione del Responsabile IT se adeguatamente documentata. In nessun caso un dipendente dell'organizzazione è autorizzato a impegnarsi in qualsiasi attività illegale ai sensi della legge locale, statale, o internazionale durante l'utilizzo di risorse di proprietà dell'azienda o mentre rappresentano l'azienda a qualsiasi titolo. L'elenco seguente non è esaustivo, ma tenta di fornire un quadro per le attività che rientrano nella categoria di uso inaccettabile.

Sono severamente vietate, senza eccezioni, le seguenti attività:

1. Violazioni dei diritti di qualsiasi persona o azienda protetta da copyright, segreto commerciale, brevetto o altra proprietà intellettuale, o leggi o regolamenti simili, inclusa, ma non limitata a, l'installazione o la distribuzione di prodotti software "pirata" o altri prodotti software che siano non adeguatamente concesso in licenza per l'uso da parte dell'organizzazione
2. Copia non autorizzata di materiale protetto da copyright inclusa, ma non limitata a, digitalizzazione e distribuzione di fotografie da riviste, libri o altre fonti protette da copyright, musica protetta da copyright e installazione di qualsiasi software protetto da copyright per il quale l'organizzazione oppure il dipendente non ha una licenza attiva
3. Accedere a dati, a un server o a un account per scopi diversi dalla conduzione dell'attività commerciale dell'organizzazione, anche se si dispone dell'accesso autorizzato
4. 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 gestione adeguata deve essere consultata prima dell'esportazione di qualsiasi materiale in questione
5. Introduzione di programmi dannosi nella rete o nei sistemi (ad es. virus, worm, trojan, email bomb, ecc.)
6. Rivelare la password del proprio account ad altri o consentire l'uso a terzi. Ciò include la famiglia e altri membri della famiglia quando il lavoro viene svolto a casa
7. Usare una risorsa informatica dell'organizzazione per impegnarsi attivamente nella fornitura o nella trasmissione di materiale che violi le molestie sessuali o le leggi ostili sul posto di lavoro
8. Fare offerte fraudolente di prodotti, articoli o servizi provenienti da qualsiasi account dell'organizzazione

9. Effettuare violazioni della sicurezza o interruzioni della comunicazione di rete. Le violazioni della sicurezza includono, ma non sono limitate a, l'accesso a dati di cui il dipendente non è il destinatario previsto o l'accesso a un server o account a cui il dipendente non è espressamente autorizzato ad accedere. Ai fini di questa sezione, "interruzione" include, ma non è limitato a, sniffing di rete, ping flood, spoofing di pacchetti, negazione del servizio e informazioni di routing contraffatte per scopi dannosi
10. La scansione delle porte o la scansione di sicurezza è espressamente vietata senza previa notifica all'azienda.
11. Esecuzione di qualsiasi forma di monitoraggio della rete che intercetti dati non destinati all'host del dipendente, a meno che questa attività non rientri nel normale lavoro/dovere del dipendente.
12. Eludere l'autenticazione dell'utente o la sicurezza di qualsiasi host, rete o account.
13. Introduzione di honeypot, honey-net o tecnologie simili sulla rete.
14. Interferire o negare il servizio a qualsiasi utente diverso dall'host del dipendente (ad esempio, attacco di negazione del servizio).
15. Utilizzo di programmi/ script/ comandi o invio di messaggi di qualsiasi tipo con l'intento di interferire o disabilitare la sessione di un utente con qualsiasi mezzo.
16. Fornire informazioni o elenchi di: dipendenti, appaltatori, partner o clienti a soggetti esterni all'organizzazione senza autorizzazione.

Attività di posta elettronica e comunicazione

Quando utilizzano le risorse aziendali per accedere e utilizzare Internet, i dipendenti devono rendersi conto di rappresentare l'azienda e agire di conseguenza.

Sono severamente vietate, senza eccezioni, le seguenti attività:

1. Invio di messaggi e-mail non richiesti, incluso l'invio di "posta indesiderata" o altro materiale pubblicitario a soggetti che non hanno richiesto espressamente tale materiale (e-mail spam).
2. Qualsiasi forma di molestia via e-mail, telefono o SMS
3. Uso non autorizzato o falsificazione delle informazioni dell'intestazione dell'e-mail
4. Sollecitazione di posta elettronica per qualsiasi altro indirizzo di posta elettronica, diverso da quello dell'account dell'autore con l'intento di molestare o raccogliere risposte.
5. Creazione o inoltro di "catene di sant'antonio", "ponzi" o altri schemi "piramidali" di qualsiasi tipo.
6. Utilizzo di e-mail non richieste provenienti dall'interno di reti o altri fornitori di servizi per conto di, o per pubblicizzare, qualsiasi servizio ospitato dell'organizzazione connesso tramite la rete dell'azienda.

Il personale è responsabile della lettura e del rispetto di tutte le politiche relative ai propri ruoli e responsabilità elencate sul documento aziendale.

Politica	**Scopo**
Politica dei ruoli e responsabilità in materia di sicurezza delle informazioni	Questa politica stabilisce e comunica i ruoli e le responsabilità all'interno dell'azienda. I ruoli sono necessari all'interno dell'organizzazione per fornire responsabilità chiaramente definite e una comprensione delle modalità di protezione delle informazioni. Il loro scopo è quello di chiarire, coordinare le attività e le azioni necessarie per diffondere la politica, gli standard e l'implementazione della sicurezza delle informazioni.
Politica delle risorse umane sulla sicurezza delle informazioni	Scopo della presente politica è quello di garantire che i dipendenti e gli appaltatori soddisfino i requisiti di sicurezza,

	comprendano le loro responsabilità e siano adatti ai loro ruoli.
Politica di controllo degli accessi	Limitare l'accesso alle informazioni e ai sistemi, alle reti e alle strutture di elaborazione delle informazioni alle parti autorizzate in conformità con gli obiettivi aziendali.
Politica di crittografia	Garantire un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni.
Politica di gestione del rischio della sicurezza delle informazioni	La seguente politica ha lo scopo di definire le azioni per affrontare i rischi di sicurezza delle informazioni e definire un piano per il raggiungimento degli obiettivi di sicurezza delle informazioni e della privacy.
Politica di gestione delle informazioni	Scopo della presente politica è quello di garantire che le informazioni siano classificate, protette, conservate e smaltite in modo sicuro in base alla loro importanza.
Politica di gestione delle terze parti	Per garantire la protezione dei dati e delle risorse dell'organizzazione condivisi con, accessibili o gestiti dai fornitori, comprese parti esterne o organizzazioni di terze parti come fornitori di servizi, venditori e clienti, e per mantenere un livello concordato di sicurezza delle informazioni e fornitura di servizi in linea con gli accordi con i fornitori.
Politica di gestione patrimoniale	Identificare le risorse organizzative e definire adeguate responsabilità di protezione.
Politica di progettazione e sviluppo sicuro	Garantire che la sicurezza delle informazioni sia progettata e implementata all'interno del ciclo di vita dello sviluppo di applicazioni e sistemi informativi.
Politica di sicurezza delle informazioni per gli ex dipendenti	Questa politica è stata redatta per garantire la sicurezza delle informazioni e la protezione dei beni aziendali dopo la cessazione del rapporto di lavoro di un dipendente. Gli ex dipendenti sono tenuti a seguire le indicazioni riportate in questo documento.
Politica di sicurezza fisica	Scopo della presente politica è quello di prevenire l'accesso fisico non autorizzato o danni alle strutture di elaborazione delle informazioni e delle informazioni dell’azienda.
Politica di sicurezza operativa	Garantire il funzionamento corretto e sicuro dei sistemi e delle strutture di elaborazione delle informazioni.

Conformità alle politiche

L’organizzazione misurerà e verificherà la conformità a questa procedura attraverso vari metodi, incluso ma non limitato al monitoraggio continuo e agli audit interni ed esterni.

Eccezioni

Le richieste di eccezione a questa procedura devono essere presentate al Responsabile del Sistema di Gestione o il Responsabile IT per l'approvazione.

Violazioni e applicazione

Qualsiasi violazione nota di questa procedura deve essere segnalata al Responsabile del Sistema di Gestione o il Responsabile IT. Le violazioni di questa procedura possono comportare il ritiro o la sospensione immediata dei privilegi del sistema e della rete e/o azioni disciplinari in conformità con le procedure aziendali fino al licenziamento.