cestaro rossi & c. s.p.a. - bari
capitale sociale € 1.000.000,00
sede legale:
70125 bari - via enrico toti, 62

Unità Tecnica/Amministrativa: 70125 Bari, via De Bellis 37 - Tel. 080.5421066 – 080.5573440 – 080.5574394
Unità Commerciale: 57023 Cecina (LI), Via Cavour 6 – Tel. 0586.15874 e-mail : commerciale@cestarorossi.com
Stabilimento: 70132 Bari, Via Zippitelli 8/A – Tel. 080.5621714 – 080.5050360

Politica di sicurezza informatica della Cestaro Rossi & C. S.p.a.

Scopo

La presente politica aziendale sulla sicurezza informatica delinea le nostre linee guida e relative disposizioni atte a preservare la sicurezza dei nostri dati e della nostra infrastruttura tecnologica. Più ci affidiamo alla tecnologia per raccogliere, archiviare e gestire le informazioni, più diventiamo vulnerabili a gravi violazioni di sicurezza. Errori umani, attacchi hacker e malfunzionamenti del sistema potrebbero causare gravi danni finanziari e mettere a repentaglio la reputazione della nostra azienda. Per questo motivo, abbiamo implementato una serie di misure di sicurezza e preparato delle istruzioni allo scopo di mitigare i rischi per la sicurezza informatica della nostra Società.

Ambito

Questa politica si applica a tutti i nostri dipendenti, fornitori e chiunque abbia accesso permanente o temporaneo ai nostri sistemi informatici.

Elementi della politica

Dati Confidenziali

I dati confidenziali sono da ritenersi preziosi. Esempi comuni sono:

- Informazioni finanziarie non pubblicate
- Dati di clienti/partner/fornitori
- Brevetti, formule o nuove tecnologie
- Elenchi clienti (esistenti e potenziali)

Tutti i dipendenti sono tenuti a proteggere questi dati. In questa politica, daremo ai nostri dipendenti istruzioni su come evitare violazioni della sicurezza.

Proteggi i dispositivi personali e aziendali

Quando i dipendenti usano i loro dispositivi digitali per accedere alle e-mail o agli account aziendali, introducono rischi per la sicurezza dei nostri dati. I PC aziendali sono forniti già protetti da password, con antivirus e con l'aggiornamento automatico delle app aziendali e del sistema operativo. Non vi è inoltre la possibilità di installare app se non con l'intervento diretto del Responsabile dei Sistemi Informativi Aziendali (IT Manager) tramite l'utente "Administrator", Chiediamo ai nostri dipendenti di proteggere sia i loro computer, tablet e cellulari personali che quelli forniti dall'azienda.

Si proteggono i propri dispositivi personali se:

- si proteggono tutti i dispositivi con password
- si sceglie e aggiorna un software antivirus completo
- non si lasciano i propri dispositivi esposti o incustoditi
- si installano gli aggiornamenti di sicurezza dei browser e dei sistemi non appena sono disponibili.

Chiediamo inoltre ai nostri dipendenti:

- di evitare di accedere ai sistemi e agli account interni dai dispositivi di altre persone o di prestare i propri dispositivi ad altri
- di accedere agli account e ai sistemi aziendali solo tramite reti sicure e private.

Quando i nuovi assunti ricevono l'attrezzatura fornita dall'azienda, vengono istruiti per gestirla in maniera corretta e garantire la sicurezza dei dati aziendali.

Chiediamo ai nostri dipendenti di rivolgersi all' IT Manager in caso di perplessità.

Mantieni le email al sicuro

Le E-mail spesso ospitano truffe e software/documenti dannosi. Per evitare infezioni da virus o furto di dati, chiediamo ai nostri dipendenti di:

- controllare l'email e i nomi delle persone da cui hai ricevuto un messaggio per assicurarti che siano corretti
- evitare di aprire allegati e di cliccare sui link quando il contenuto non è spiegato adeguatamente (ad esempio "guarda questo video, è fantastico")
- diffidare dei titoli strani (ad esempio quelli che propongono premi o consigli)

- Fare attenzione a incongruenze o elementi rivelatori (ad esempio errori grammaticali, lettere maiuscole, numero eccessivo di punti esclamativi).

Se un dipendente non è sicuro che un'e-mail ricevuta sia sicura, non deve assolutamente aprirla e può rivolgersi al nostro IT Manager.

Gestisci correttamente le password

Le perdite di password sono pericolose perché possono compromettere l'intera infrastruttura. Non solo le password devono essere sicure in modo che non possano essere facilmente hackerate, ma devono anche rimanere segrete. Per questo motivo, chiediamo ai nostri dipendenti di:

- scegliere password composte da almeno otto caratteri (inclusi lettere maiuscole e minuscole, numeri e simboli) ed evita informazioni facilmente indovinabili (ad esempio i compleanni)
- ricordare le password invece di scriverle. Se i dipendenti hanno bisogno di scrivere le proprie password, sono obbligati a mantenere riservato il documento cartaceo o digitale e a distruggerlo una volta terminato il lavoro
- non Scambiare mai le proprie credenziali con altri
- cambiare le password ogni sei mesi.

Trasferisci i dati in modo sicuro

Il trasferimento dei dati introduce rischi per la sicurezza. Chiediamo ai nostri dipendenti di:

- non utilizzare chiavette USB per trasferire dati
- evitare di trasferire dati sensibili (ad esempio informazioni sui clienti, registri dei dipendenti) ad altri dispositivi o account, a meno che non sia assolutamente necessario. Quando è necessario un trasferimento di massa di tali dati, chiediamo ai dipendenti di contattare il nostro IT Manager
- condividere i dati riservati tramite la rete/il sistema aziendale e non tramite Wi-Fi pubblico o connessioni private
- assicurarsi che i destinatari dei dati siano persone o organizzazioni debitamente autorizzate e che dispongano di adeguate politiche di sicurezza
- segnalare truffe, violazioni della privacy e tentativi di hacking

Il nostro IT Manager deve essere a conoscenza di eventuali tentativi di truffe, violazioni e malware in modo da poter proteggere meglio la nostra infrastruttura. Per questo motivo, chiediamo ai nostri dipendenti di segnalare attacchi percepiti, e-mail sospette o tentativi di phishing il prima possibile al nostro specialista. Il nostro IT Manager deve indagare

tempestivamente, risolvere il problema e inviare un avviso a tutta l'azienda quando necessario e consigliare i dipendenti su come rilevare le e-mail truffa. Incoraggiamo i nostri dipendenti a contattarlo per qualsiasi domanda o dubbio.

Navigazione in Internet

Il dispositivo abilitato alla navigazione in Internet costituisce strumento aziendale necessario allo svolgimento dell'attività lavorativa assegnata. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

Ai nostri dipendenti non è consentito:

- accedere a siti INTERNET evitando o superando o comunque tentando di superare o disabilitando i sistemi adottati dalla società per bloccare l'accesso ad alcuni siti ed in ogni caso utilizzare siti o altri strumenti (es. CRACKING PROGRAMS) che realizzino tale fine
- accedere a siti INTERNET che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

Il servizio di connessione internet aziendale non deve essere utilizzato per commettere azioni punibili o reprensibili quali ad esempio infrangere i diritti di proprietà intellettuale e visitare siti pornografici. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti, anche filmati e musica, provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato l'IT Manager)
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o dall'IT Manager) e comunque nel rispetto delle normali procedure di acquisto
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa

- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale
- l'accesso ai Social Media (es. Linkedin, Facebook, Instagram, X, TikTok etc.) se non espressamente autorizzati dal Responsabile d'ufficio

Misure aggiuntive

Per ridurre la probabilità di violazioni della sicurezza, diamo inoltre chiediamo ai nostri dipendenti di:

- spegnere gli schermi e bloccare i dispositivi quando si allontanano dalla scrivania
- segnalare il prima possibile all' IT Manager l'attrezzatura rubata o danneggiata
- cambiare contemporaneamente tutte le password degli account quando un dispositivo viene rubato
- segnalare una minaccia percepita o una possibile debolezza della sicurezza nei sistemi aziendali
- astenersi dallo scaricare software sospetti, non autorizzati o illegali sulle apparecchiature aziendali
- astenersi dall'accedere a siti web sospetti

Il nostro IT Manager:

- installa firewall, software anti-malware e sistemi di autenticazione degli accessi
- organizza la formazione sulla sicurezza per tutti i dipendenti
- informa regolarmente i dipendenti sulle nuove e-mail fraudolente o sui virus e sui modi per contrastarli
- Indaga approfonditamente sulle violazioni della sicurezza.

La nostra azienda disporrà di tutti i sistemi fisici e digitali per proteggere le informazioni.

Azioni disciplinari

Ci aspettiamo che tutti i nostri dipendenti seguano sempre questa politica: coloro che causano violazioni della sicurezza saranno soggetti a misure disciplinari.

Fornitori

Il nostro Fornitore garantisce che i propri sistemi informatici, includendo i sistemi utilizzati per la fornitura dei servizi/prodotti oggetto dei nostri rapporti contrattuali , rispettano i requisiti di

Cyber Security richiesti dalla nostra Società e dal Cliente Finale, e che sono in linea con gli standard internazionali di riferimento (es: NIST, sistemi di gestione della sicurezza delle informazioni ISO/IEC 27000, ecc.). In particolare, il nostro Fornitore, con riferimento ai sistemi di cui sopra, garantisce:

- di aver adottato e di adottare tutte le misure necessarie a garantire il puntuale rispetto delle disposizioni di legge in materia di trattamento dei dati personali e la conformità a standard e normative in materia di cyber security;
- di aver ottenuto le eventuali certificazioni di sicurezza necessarie per ottemperare a obblighi di conformità a standard e normative;
- che tali sistemi siano esenti da vulnerabilità di sicurezza e codice malevolo quale, a titolo indicativo e non esaustivo, virus, trojan, e backdoor, in grado di compromettere la riservatezza, disponibilità e integrità dei dati o comunque mettere a rischio la sicurezza dei sistemi informatici della nostra Società

Qualora si verifichino situazioni quali, a titolo esemplificativo e non esaustivo, non conformità e/o vulnerabilità di sicurezza rilevate nelle attività di auditing/monitoraggio condotte dalla nostra Società, direttamente e/o tramite terze parti, fattori di rischio cyber correlati al nostro rapporto e segnalati dalla nostra Società, Il nostro Fornitore è tenuto a formulare un piano contenente le azioni operative per la risoluzione o, in subordine, la mitigazione, di tali criticità, che deve essere sottoposto all'approvazione dalla nostra Società. Tutte le attività correlate a tale piano sono a carico del nostro Fornitore, senza alcun onere per la nostra Società e saranno oggetto di monitoraggio da parte dalla nostra Società. Qualora nel corso del nostro rapporto intervengano modifiche normative (nazionali, comunitarie o internazionali) o di prassi di settore (a titolo esemplificativo standardizzazioni) che comportino l'adozione di misure di Cyber Security, organizzative e/o tecniche, aggiuntive e/o diverse rispetto a quanto definito in precedenza, il nostro Fornitore dovrà curare l'integrazione e l'aggiornamento dei requisiti di Cyber Security relativi al nostro rapporto al fine di ottemperare agli obblighi di compliance. Il nostro Fornitore, in caso di Incidenti Cyber e/o Data Breach che dovessero interessare direttamente le applicazioni e/o i sistemi informatici, i prodotti e i dati oggetto del nostro rapporto o, indirettamente, i sistemi informatici e le informazioni dalla nostra Società e/o del Cliente Finale, è tenuto ad allertarci tempestivamente, comunicando quali siano i dati e/o i sistemi coinvolti e assicurando una risposta e un ripristino tempestivi senza alcun onere per dalla nostra Società e saranno oggetto di monitoraggio da parte nostra.

Prendi sul serio la sicurezza

Tutti, dai nostri clienti e partner, ai nostri dipendenti e fornitori, dovrebbero sentire che i loro dati sono al sicuro. L'unico modo per ottenere la loro fiducia è proteggere in modo proattivo i nostri sistemi e database. Possiamo tutti contribuire a questo essendo vigili e tenendo la sicurezza informatica al primo posto.

Firmato digitalmente da Fabio Dalla Serra
ND: cn=Fabio Dalla Serra, o=Cestaro Rossi &c. S.p.A., ou=Presidente, email=f.dallaserra@cestarorossi.com, c=IT
Data: 2024.11.12 13:00:00 +01'00'