

Cyber Security Policy

24.04.2024

CONTESTO

Step S.p.A. ("Azienda") si impegna a salvaguardare la riservatezza di tutti gli accessi e le risorse applicative disponibili e a rispettare le leggi, i regolamenti, le linee guida e le migliori pratiche attuali per proteggere i suoi dipendenti, parti interessate, funzionari, affiliati e azionisti dai pericoli del mondo cibernetico dovuti ai suoi progressi tecnologici e ai conseguenti vari tipi attività quali phishing, fuga di dati, minacce, hacking non etico e ransomware.

SCOPO E OBIETTIVI

Lo scopo di questa policy è garantire la sicurezza delle informazioni sensibili dell'organizzazione, proteggendo i sistemi informatici e i dati dai rischi di accesso non autorizzato, perdita, danneggiamento o furto.

Gli obiettivi principali includono:

- Proteggere l'integrità, la riservatezza e la disponibilità dei dati
- Assicurare la conformità alle leggi e ai regolamenti pertinenti sulla protezione dei dati
- Minimizzare il rischio di violazioni della sicurezza informatica
- Educare e sensibilizzare i dipendenti sui rischi di sicurezza informatica.

TERMINI E DEFINIZIONI

Cyber Security:

Conosciuta anche come Sicurezza Informatica si riferisce alla pratica di proteggere computer, hardware, software, server, dispositivi mobili, sistemi elettronici e dati da attacchi dannosi che possano compromettere l'efficienza della Società, per salvaguardare la riservatezza e l'integrità di tutti gli accessi e applicazioni.

Information Technology:

Fa riferimento all'uso di computer e internet per accedere e scambiare ogni tipologia d'informazioni.

Accessi Non Autorizzati:

Fa riferimento a soggetti che provano a guadagnare l'accesso a specifiche applicazioni o informazioni senza un preventivo consenso o permesso da parte di un utente autorizzato o dell'azienda.

Cybercrime:

Fa riferimento all'attività non etica che coinvolge computer e reti, volta a commettere un reato online con il solo scopo di danneggiare qualcuno o la sicurezza di un'azienda, specialmente la sua condizione finanziaria.

Step s.p.a.

Via Senato, 3 – 20121 Milano – Italy

Via Zaccarini, 1 – San Nicolò – 29010 Rottofreno (PC) – Italy

Cap.Soc. € 3.640.000 i.v. C.F. e P.IVA 00103350336 C.c.i.a.a. Rea Piacenza 4722 Reg. Soc. Trib. (PC) n° 611

Tel. +39 0523 765111 – e-mail info@step.it

Cyber-criminali:

Fa riferimento a un individuo o un gruppo di persone che ingaggiano attività di cybercrime.

Phishing:

Si riferisce ad un'attività fraudolenta che si maschera da entità ufficiale e rispettabile in tutte le forme di comunicazione. Questi criminali informatici, ad esempio, potrebbero inviare un'e-mail con un aggiornamento apparentemente ufficiale della banca attraverso gli allegati e i collegamenti distribuiti che li aiuteranno ad accedere, se compilato correttamente, all'account della vittima.

Ransomware:

Si riferisce a un tipo di malware ("software dannoso") che blocca l'accesso dell'utente alla sua applicazione o ai suoi file. Di solito avviene in ambiente aziendale o organizzativo nella forma di una richiesta di pagamento, spesso mediante criptovalute, necessaria per sbloccare l'utente o le informazioni compromesse.

RESPONSABILITÀ

La responsabilità della sicurezza informatica è attribuita al team di sicurezza informatica dell'organizzazione, che opera sotto la supervisione della direzione IT.

Ogni dipendente è responsabile della sicurezza delle informazioni a cui ha accesso e deve aderire a questa policy.

Tutti i soggetti (dipendenti, stakeholder, funzionari, affiliati e azionisti) devono essere consapevoli e informati sulla sicurezza informatica, partecipando a tutti i corsi di formazione e certificazione e rispettando i processi e le procedure dell'azienda. Tutti i soggetti sono tenuti ad attenersi alle seguenti direttive:

- Tutti i dispositivi forniti dall'Azienda (smartphone, computer e laptop) sono strettamente destinati all'uso aziendale per evitare qualsiasi possibile accesso dalla rete esterna. Sono forniti al solo scopo di svolgere il proprio ruolo per l'Azienda e i suoi Clienti.
- Occorre sempre disconnettersi correttamente dai sistemi e dai dispositivi dopo l'orario di lavoro.
- Le credenziali di accesso, in particolare le password dei diversi sistemi e database, devono essere conservate nel sistema di gestione delle password protetto, come prescritto dall'Azienda.
- Chiudere a chiave i dispositivi informatici o portatili quando il personale non si trova nel proprio posto di lavoro o nella propria area di lavoro per un periodo prolungato.
- Evitare di condividere i dati o le informazioni aziendali, soprattutto con persone che non fanno parte della cerchia aziendale o che non sono a conoscenza del problema.
- Tutti i soggetti devono attenersi scrupolosamente a non cercare mai di connettersi a un Wi-Fi pubblico, sempre e ovunque, nei centri commerciali, nelle catene di fast food, nelle caffetterie e in qualsiasi altro luogo ad alto rischio di violazione della sicurezza.

Step s.p.a.

Via Senato, 3 – 20121 Milano – Italy

Via Zaccarini, 1 – San Nicolò – 29010 Rottofreno (PC) – Italy

Cap.Soc. € 3.640.000 i.v. C.F. e P.IVA 00103350336 C.c.i.a.a. Rea Piacenza 4722 Reg. Soc. Trib. (PC) n° 611

Tel. +39 0523 765111 – e-mail info@step.it

- Bloccare i dispositivi informatici o portatili quando il personale non si trova sul posto di lavoro o nell'area di lavoro.
- Essere sempre vigili nell'area circostante al di fuori dei locali dell'azienda per proteggere voi stessi, i vostri oggetti essenziali, il vostro cellulare e i vostri dispositivi portatili.
- Essere sempre consapevoli della propria sicurezza informatica.

CLASSIFICAZIONE DEI DATI

Tutti i dati dell'organizzazione devono essere classificati in base al loro livello di sensibilità e crittografia in conformità con le linee guida interne.

La classificazione dei dati deve essere rivista periodicamente e aggiornata secondo necessità.

ACCESSO E CONTROLLO

L'accesso ai sistemi e ai dati deve essere limitato solo ai dipendenti autorizzati e deve essere basato sul principio del "bisogno di sapere".

Le credenziali di accesso devono essere gestite in modo sicuro e non devono essere condivise con altri dipendenti.

SICUREZZA FISICA

Tutti i dispositivi informatici e i server devono essere fisicamente protetti per impedire l'accesso non autorizzato.

Le misure di sicurezza fisica includono l'installazione di serrature, sistemi di allarme e videosorveglianza.

FORMAZIONE E CONSAPEVOLEZZA

I dipendenti devono ricevere formazione regolare sulla sicurezza informatica, compresi i rischi di phishing, malware e altre minacce.

Deve essere promossa una cultura della sicurezza informatica in tutta l'organizzazione, incoraggiando la segnalazione tempestiva di incidenti di sicurezza.

L'Azienda fornirà una formazione sulla sicurezza informatica con un professionista certificato in materia di sicurezza informatica per i suoi dipendenti, stakeholder, funzionari, affiliati e azionisti per aiutarli a discernere tutte le loro attività che coinvolgono reti, computer e l'uso di Internet per la loro sicurezza e per quella dell'azienda.

La formazione e la sensibilizzazione sulla sicurezza informatica possono riguardare i seguenti argomenti:

- Come riconoscere gli attacchi di phishing
- Criteri di scelta delle password e autenticazioni uniche
- Uso corretto dei supporti rimovibili
- Sicurezza dei dispositivi: Cellulari, portatili e computer

Step s.p.a.

Via Senato, 3 – 20121 Milano – Italy

Via Zaccarini, 1 – San Nicolò – 29010 Rottofreno (PC) – Italy

Cap.Soc. € 3.640.000 i.v. C.F. e P.IVA 00103350336 C.c.i.a.a. Rea Piacenza 4722 Reg. Soc. Trib. (PC) n° 611

Tel. +39 0523 765111 – e-mail info@step.it

- Lavoro a distanza e sicurezza a casa
- I pericoli del Wi-Fi pubblico
- Sicurezza fisica all'interno e all'esterno dei locali dell'azienda
- I social media

GESTIONE DEGLI INCIDENTI

Deve essere istituito un processo per la gestione degli incidenti di sicurezza, che include la notifica tempestiva, l'indagine e la mitigazione del danno.

Gli incidenti di sicurezza devono essere registrati e analizzati per identificare le cause radici e prevenire futuri incidenti simili.

CONFORMITÀ E REVISIONE

Questa policy deve essere periodicamente rivista e aggiornata per garantire la conformità alle normative e agli standard di sicurezza informatica.

Devono essere condotti regolarmente audit sulla sicurezza informatica per valutare l'efficacia delle misure di sicurezza e identificare eventuali aree di miglioramento.

APPLICAZIONE DELLA POLICY

La violazione di questa policy può comportare provvedimenti disciplinari, inclusa la revoca dei privilegi di accesso e il licenziamento.

I dipendenti sono tenuti a segnalare qualsiasi violazione o sospetta violazione di questa policy al team di sicurezza informatica (Cyber Security Team).

SECURITY OFFICER E CYBER SECURITY TEAM

L'Azienda ha nominato un proprio Responsabile della Sicurezza Informatica (Cyber Security Manager), il Chief Information Officer del Dipartimento di Information Technology, Alessio Mangano, che guida anche il Cyber Security Team.

Il Responsabile della sicurezza informatica è responsabile dell'implementazione e dell'esecuzione dell'intero processo relativo alla sicurezza informatica. Il Responsabile ha inoltre l'autorità esclusiva di prendere e discernere tutte le decisioni relative alla sicurezza informatica. Tutti i soggetti sono tenuti a seguire le indicazioni del Cyber Security Manager e del Cyber Security Team.

Questi funzionari fungono da organo responsabile della sicurezza informatica e sono di grande aiuto nell'attuazione e nell'esecuzione di questa policy per tutta l'organizzazione.

APPROVAZIONE E REVISIONE DELLA POLICY

Step s.p.a.

Via Senato, 3 – 20121 Milano – Italy

Via Zaccarini, 1 – San Nicolò – 29010 Rottofreno (PC) – Italy

Cap.Soc. € 3.640.000 i.v. C.F. e P.IVA 00103350336 C.c.i.a.a. Rea Piacenza 4722 Reg. Soc. Trib. (PC) n° 611

Tel. +39 0523 765111 – e-mail info@step.it

Questa policy è stata approvata dal CIO e sarà soggetta a revisione annuale o quando vi siano cambiamenti significativi nell'ambiente operativo.

Firma

Alessio Mangano (CIO)


Step s.p.a.

Via Senato, 3 – 20121 Milano – Italy

Via Zaccarini, 1 – San Nicolò – 29010 Rottofreno (PC) – Italy

Cap.Soc. € 3.640.000 i.v. C.F. e P.IVA 00103350336 C.c.i.a.a. Rea Piacenza 4722 Reg. Soc. Trib. (PC) n° 611

Tel. +39 0523 765111 – e-mail info@step.it