SHARP

Sharp Electronics (Italia) S.p.A.

Via Ettore Bugatti, 12
20142 Milano
T: +39 02 893488 1
F: +39 02 893488 244
W: www.sharp.it

Politica per la sicurezza delle informazioni

Per tematiche non trattate nella presente,

ci si rimetta alle politiche Aziendali della Sharp Corporation

Indice dei contenuti

1 Campo di applicazione

Questa politica si applica a tutte le informazioni (rif. digitali, cartacee, verbali) ai sistemi, alle reti, alle applicazioni e ai dispositivi gestiti e utilizzati da SHARP Electronics Italia S.p.A. (di seg. SEIS), nonché a tutto il personale (rif. dipendenti, collaboratori, consulenti, stagisti) e a terze parti che hanno accesso alle informazioni o ai sistemi informativi di SEIS.

La presente politica si applica come tale a SEIS e si colloca in accordo alle omologhe politiche della SHARP Corporation, applicabili all'interno del mondo SHARP ed armonizzate alla presente.

2 Principi e obiettivi della sicurezza delle informazioni

2.1 Principi

2.1.1 Terminologia

SEIS argomenta nel seguito la propria politica per la sicurezza delle informazioni, e si impegna a garantire la sicurezza delle informazioni nonchè promuovere un uso sicuro ed appropriato dei sistemi informativi.

Sicurezza informativa si riferisce alle modalità secondo cui sono ricondotti ad un livello accettabile i rischi di sicurezza in relazione agli obiettivi aziendali di **Confidenzialità, Integrità e Disponibilità**, per tutte le informazioni e le tecnologie informative.

Oltre alla sicurezza dei sistemi informatici e dei dati che risiedono in essi, la sicurezza delle informazioni comprende anche la sicurezza delle informazioni NON processate e immagazzinate elettronicamente.

Definizioni:

- **Confidenzialità:**
  Dati, informazioni e programmi riservati e confidenziali devono essere protetti contro il possibile accesso NON autorizzato e contro la propria divulgazione. Sono fatti oggetto della protezione il contenuto dei messaggi archiviati o inviati. Sono presenti nel Sistema di Sicurezza delle Informazioni, a proposito del processo di ricezione e invio, dettagli ulteriori circa i processi comunicativi (es. chi, quando, per quanto tempo, con chi…ecc.)
- **Integrità:**
  Il termine integrità si riferisce al singolo dato, ad un patrimonio informativo, all'intero sistema IT aziendale: integrità di una informazione significa la sua completezza e correttezza. Completezza significa che ogni parte della informazione è disponibile. L'informazione è corretta se riproduce i fatti senza falsificazione. Infine il termine Integrità si riferisce inoltre ai sistemi IT aziendali, poiché l'integrità della informazione può essere assicurata unicamente nel caso che essa sia adeguatamente trattata e trasmessa.
- **Disponibilità:**
  Le funzionalità hardware e software, cosi' come tutte le informazioni necessarie, devono essere disponibili agli utenti al momento giusto e nel posto giusto.

2.1.2 Sicurezza delle informazioni nei processi IT

Lo scopo dichiarato di SEIS è assicurare la disponibilità, l'integrità e la confidenzialità delle informazioni, durante la pianificazione e la implementazione del processo di business aziendale.

La sicurezza delle informazioni è un aspetto prestazionale dei processi IT che deve essere individuato e tenuto in considerazione.

La sicurezza delle informazioni deve essere tenuta in considerazione durante i processi di:

- Implementazione delle procedure IT.
- L'operatività e la manutenzione dei processi IT.
- Acquisto, rimozione e smaltimento dei prodotti IT.
- Uso di servizi di terze parti.

Le misure di sicurezza effettivamente intraprese devono essere economicamente giustificabili in relazione al rischio.

Tutti i dipendenti, collaboratori, fornitori e subfornitori e partners di SEIS, nonché tutto il Management aziendale, sono al corrente della propria responsabilità circa la sicurezza delle informazioni e devono seguire la presente politica di sicurezza delle informazioni.

Lo scopo delle presenti linee guida è duplice: proteggere SEIS e i soggetti collegati da danno reputazionale, interruzione della continuità operativa, perdita di patrimonio informativo aziendale, e allo stesso tempo aiutare i dipendenti ad accrescere la propria consapevolezza circa la propria responsabilità a proteggere il patrimonio informativo aziendale.

2.1.3 Sicurezza delle informazioni come performance organizzativa e gestionale

Le misure di sicurezza tecniche ed organizzative devono essere concepite in maniera da essere parte integrante di tutti i processi organizzativi e gestionali. Ciò è specialmente rilevante a proposito dei dati personali e dei dati sensibili.

Le questioni di sicurezza delle informazioni devono essere necessariamente tenute in conto nelle seguenti situazioni:

- Nella progettazione della Organizzazione e dei flussi di lavoro.
- Nella creazione ed assegnazione delle funzioni e dei ruoli.
- Nella gestione del personale.
- Nella informazione/formazione delle persone coinvolte.
- Nella collaborazione con i partners e i soggetti esterni.
- Nella selezione e nell'uso di risorse ausiliarie.

2.1.4 Sostenibilità economica

Le misure di sicurezza delle informazioni devono essere economicamente giustificate in relazione al rischio. Ciò è definito tramite il valore della informazione da proteggere, i sistemi IT coinvolti, la probabilità che il rischio si materializzi, l'impatto dell'accadimento rischioso.

Generalmente, nel processo di identificazione del rischio, devono essere tenuti in conto gli effetti sulla integrità materiale e immateriale delle persone, i danni finanziari, i danni reputazionali, le conseguenze di violazioni di legge.

2.1.5 Sicurezza prioritaria rispetto a disponibilità

Nel caso venissero conosciuti minacce o attacchi effettivi alla sicurezza della infrastruttura IT di SEIS, la disponibilità ai dati o alle reti aziendali può essere temporaneamente ristretta in accordo ai livelli di rischio e minaccia.

2.1.6 Formazione e sensibilizzazione di impiegati, partner e terze parti

SEIS fornisce regolarmente informazione, formazione e addestramento a tutti i propri dipendenti, sulla sicurezza dell'informazione e sulla consapevolezza dei rischi, così da renderli capaci di contribuire alla garanzia di sicurezza delle informazioni.

2.2 Obiettivi della sicurezza delle informazioni

2.2.1 Disponibilità dei processi IT e delle informazioni

L'obiettivo dichiarato di SEIS è garantire che i sistemi e le informazioni siano accessibili e utilizzabili quando necessario.

Per tutte le procedure ed i programmi IT, viene indicato l'orario in cui esse devono essere disponibili. Le interruzioni ai processi di business su tali piattaforme devono essere il più possibile evitate durante tali fasce orarie, nonchè limitate in numerosità e durata.

I fermi programmati saranno stabiliti sistematicamente, in maniera tale da consentire riparazione, manutenzione preventiva e aggiornamenti dei diversi Sistemi ed applicativi.

2.2.2 Riservatezza e confidenzialità

I dati raccolti, immagazzinati, processati e transitati tramite le procedure IT devono essere trattati in modo riservato o confidenziale e devono essere protetti contro accessi non autorizzati, in ogni momento.

A tale fine, deve essere sempre preordinato il gruppo degli utenti ai quali è autorizzato l'accesso. L'accesso ai sistemi IT, alla applicazioni di IT, nonché ai relativi dati ed informazioni, devono essere ristretti al minimo numero possibile di utenti, per tutti i dati presenti in SEIS.

Ogni dipendente riceve unicamente le autorizzazioni di accesso ai dati che egli deve utilizzare per svolgere i compiti affidati.

2.2.3 Integrità

SEIS si è data l'obiettivo di mantenere l'accuratezza e la completezza delle informazioni, proteggendole contro ogni alterazione, sia involontaria sia volontaria.

Tutti i processi IT devono sempre fornire informazioni aggiornate e complete, prevenendo modifiche non autorizzate.

2.2.4 Garantire la conformità legislativa e contrattuale

SEIS agisce in accordo alle leggi ed ai regolamenti applicabili (es. GDPR, NIS2, ecc.), nonché agli accordi contrattuali circa la sicurezza delle informazioni, così che partners esterni e terze parti devono essere messi a conoscenza degli aspetti di sicurezza delle informazioni, così come altresì devono essere richieste da tutte le persone di SEIS le appropriate qualifiche ed attestazioni di conformità.

3 Ruoli e responsabilità

3.1 Responsabilità della Direzione

La Direzione emette regole cogenti circa la Sicurezza della Informazione di SEIS, e si preoccupa che tali regole siano chiaramente comunicate a tutti i dipendenti.

La Direzione istituisce misure e policy al fine di assicurare che solamente i soggetti autorizzati abbiano accesso ai dati sui sistemi aziendali e ai dati aziendali.

Le violazioni della sicurezza delle informazioni devono essere immediatamente riportate all'apposito responsabile (Responsabile Sicurezza Informazione).

Le violazioni includono, in particolare, azioni che divergono dalle prescrizioni della presente politica, o altre policies di Gruppo a proposito della sicurezza delle informazioni, e che:

- Causino danno materiale o immateriale a SEIS.
- Permettano accesso non autorizzato, diffusione o alterazione di tale informazione.
- Utilizzino informazioni per azioni illegali.
- Compromettano la reputazione di SEIS.

3.2 Responsabilità dei dipendenti

Tutti i dipendenti contribuiscono a favorire e ad assicurare la sicurezza delle informazioni, tramite il loro agire responsabile e in accordo con le regole di sicurezza delle informazioni, con le linee guida, con le direttive e gli obblighi contrattuali.

3.3 Responsabilità dei fornitori esterni

Personale ed aziende, che non appartengono a SEIS, ma che svolgono servizi per SEIS devono muoversi in conformità alle regole e alle linee guida di sicurezza delle informazioni specificate da SEIS.

Le funzioni di SEIS che contrattualizzano un fornitore devono renderlo edotto circa le regole in essere e devono obbligarlo a rispettare tali regole, secondo la modalità più appropriate per ciascun caso. Ciò include il fatto che il fornitore deve informare il cliente di anomalie riscontrate o rischi di sicurezza delle misure messe in atto (vd seg.pt.5).

4 Organizzazione

SEIS ha individuato le figure del Responsabile della Protezione dei Dati (DPL) e del Responsabile della Sicurezza dell'Informazione (RSI) che sono responsabili per la sicurezza delle informazioni.

Il Responsabile della Protezione dei Dati viene supportato dalle funzioni responsabili della protezione dei dati a livello Europeo, cosi' da assicurare la presenza di un esperto in loco per la protezione dei dati, nonché al fine di costituire un punto di contatto per gli interni e per gli esterni a proposito della questione della protezione dei dati.

Tale responsabile della protezione dei dati viene supportato dal personale del reparto IT, che si assume la responsabilità operativa delle attività, e fornisce consulenza IT specializzata.

5 Attuazione della Politica per la Sicurezza delle informazioni

La presente politica è il caposaldo per la creazione di ulteriori linee guida, classificazione di asset informativi, concetti di sicurezza e regole di dettaglio riguardanti la sicurezza delle informazioni, incluse linee guida tecniche, regole e istruzioni di dettaglio.

6 Assicurazione e miglioramento della Sicurezza delle Informazioni

La presente politica, la sicurezza IT, la sicurezza delle informazioni e i principi di sicurezza delle informazioni sono regolarmente verificati circa la loro adeguatezza ed efficacia.

In particolare, devono essere regolarmente controllate le suddette misure al fine di assicurare che esse siano note, implementabili e integrabili nel processo di business.

La Direzione supporta il miglioramento continuo dell'efficacia delle misure di sicurezza delle informazioni.

Anche i Dipendenti sono incentivati a suggerire miglioramenti e a render conto di eventuali debolezze del sistema alle appropriate funzioni aziendali.

Amministratore Delegato
Corrado Righetti