Kettydo+

Politica per la sicurezza delle informazioni

Indice dei contenuti

Kettydo+ S.r.l.

Sede Legale
Via Francesco De Sanctis 34
20141 Milano - IT

Phone: +39 02 87393636
Fax: +39 02 87394018
Web: www.kettydo.com
Email: info@kettydo.com

1 Campo di applicazione

Questa politica si applica a Kettydo+ S.r.l. (di seg. Anche K+) e ai soggetti che detengono, forniscono o accedono ai sistemi informativi di K+.

La politica include:

- Informazioni immagazzinate elettronicamente, trasmesse attraverso le reti e le linee telefoniche, nonchè le informazioni discusse e stampate come copia fisica;
- Tutte le risorse direttamente associate con la fornitura di servizi informativi e i sistemi informativi di K+.

La presente politica si applica come tale a Kettydo+ S.r.l. e si colloca in accordo alle omologhe politiche del Gruppo cui K+ appartiene, applicabili all'interno del mondo K+ ed armonizzate alla presente.

2 Principi ed obiettivi della sicurezza delle informazioni

2.1 Principi

2.1.1 Terminologia

Kettydo+ S.r.l. 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 apporpriato 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, così come tutte le informazioni necessarie, devono essere disponibili agli utenti al momento giusto e nel posto giusto.

2.1.2 Importanza della sicurezza delle informazioni nell'uso delle apparecchiature IT

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

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

Tutti gli impiegati, fornitori e subfornitori e partners di Kettydo+ S.r.l., nonché tutto il Management aziendale, sono al corrente della propria responsabilità circa la sicurezza delle informazioni e devono seguire la presente politica di sicurezza.

Lo scopo delle presenti linee guida è duplice: proteggere Kettydo+ S.r.l. 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 caratteristica delle procedure IT

La sicurezza delle informazioni è un aspetto prestazionale dei processi IT che deve essere individuato e tenuto in conto in sede di progetto globale/specifica del sistema di sicurezza IT.

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

- Sviluppo e 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.

2.1.4 Sicurezza delle informazioni come caratteristica prestazionale della Organizzazione di Kettydo+ S.r.l.

Le misure di sicurezza tecniche ed organizzative devono essere concepite in maniera da essere parte integrante di tutti i processi gestionali. Ciò è specialmente rilevante a prosito 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.
- Nella creazione ed assegnazione delle funzioni e dei ruoli.
- Nella gestione del personale.
- Nell'addestramento e nella successive formazione.
- Nella progettazione dei flussi di lavoro.
- Nella cooperazione con i partners e i soggetti esterni.
- Nella selezione e nell'uso di risorse ausiliarie.

2.1.5 Sostenibilità economica

Le misure di sicurezza 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 psichica e fisica delle persone, il diritto alla autodeterminazione informativa, i danni finanziari, i danni reputazionali, le conseguenze di violazioni di legge.

2.1.6 Sicurezza prioritaria rispetto a disponibilità

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

2.1.7 Informazione di impiegati, partner e terze parti

Kettydo+ S.r.l. fornisce regolarmente addestramento e formazione a tutti i Manager e gli impiegati, così da renderli capaci di contribuire alla garanzia di sicurezza delle informazioni.

Kettydo+ S.r.l. si pone in accordo alle leggi ed ai regolamenti applicabili, nonché agli accordi 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 unità di business di Kettydo+ S.r.l. le appropriate qualifiche ed attestazioni di conformità.

2.2 Scopi della sicurezza delle informazioni

2.2.1 Disponibilità

Per tutte le procedure ed i programmi IT, deve essere specificato 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.

La descrizione della disponibilità richiesta include:

- Orario di operatività regolare.
- Orari con requisiti di disponibilità supplementare.
- La durata massima delle indisponibilità tollerate.

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

2.2.2 Confidenzialità

I dati raccolti, immagazzinati, processati e transitati tramite le procedure IT devono essere trattati confidenzialmente 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 permesso 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 Kettydo+ S.r.l.

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

2.2.3 Integrità

Le informazioni devono essere protette contro ogni alterazione, sia essa involontaria sia essa deliberata falsificazione.

Tutte le procedure IT devono sempre fornire informazioni aggiornate e complete. Deve essere documentata ogni restrizione dovuta al processo o alla gestione di informazioni.

3 Ruoli e responsabilità

3.1 Responsabilità della Direzione

La Direzione emette regole cogenti circa la Sicurezza della Informazione di Kettydo+ S.r.l., e si preoccupa che tali regole siano chiaramente communicate agli impiegati.

La Direzione istituisce misure e linee guida 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 (rif. Information Security Manager).

Le violazioni includono, in particolare, azioni che sono discostanti dalle prescrizioni della presente politica, o altre linee guida a proposito della sicurezza delle informazioni, e che:

- Causino danno materiale o immateriale a Kettydo+ S.r.l.
- Permettano accesso non autorizzato, rivelando alterazione di tale informazione.
- Utilizzino informazioni per azioni illegali.
- Compromettano la reputazione di Kettydo+ S.r.l.

3.2 Responsabilità del dipendente

Tutti i dipendenti contribuiscono ad aiutare 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 Kettydo+ S.r.l. ma che svolgono servizi per K+ devono muoversi in accordo con le specifiche di K+ per la conformità alle regole e alle linee guida rivolte alla sicurezza delle informazioni.

La funzione di Kettydo+ S.r.l. che contrattualizza un fornitore deve renderlo edotto circa le regole in essere e deve obbligarlo a rispettare tali regole, secondo la modalità più appropriate per il 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

Kettydo+ S.r.l. individua le figure del responsabile della protezione dei dati (rif. DPO) e del responsabile della sicurezza informatica (rif. IT Manager) che è responsabile per la sicurezza delle informazioni.

Il responsabile della protezione dei dati viene supportato dalle funzioni responsabili della protezione dei dati a livello delle varie entità aziendali, così 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 da personale del reparto IT, che si assume la responsabilità operativa delle attività, e fornisce consulenza IT specializzata.

5 Implementazione

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

6 Assicurazione e miglioramento della Sicurezza delle Informazioni

Le politiche per la sicurezza, la sicurezza IT, la sicurezza delle informazioni e i concetti di sicurezza delle informazioni sono regolarmente controllati circa la loro adeguatezza ed efficacia.

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

Il Management supporta il miglioramento continuo dell’efficacia delle misure di sicurezza. Anche i Dipendenti sono incentivati a suggerire miglioramenti e a render conto di eventuali debolezze del sistema alle appropriate funzioni aziendali.

Federico Rocco
CEO

DocuSigned by:
818B21BAD2C74B9...