



Sistema Gestione Sicurezza dei dati
SGSD ISO / IEC 27001

POLICY DI SISTEMA DI GESTIONE SICUREZZA DATI

POL- 15- POLITICA DI GESTIONE DEGLI INCIDENTI DI
SICUREZZA
Di TEXLINESRL

Rev. n°	Data	Descrizione della revisione	Redatto RSGSD	Approvato Legale Rappresentante
0	14/01/2026	Prima Stesura		

TEXLINE S.r.l. unipersonale
REA: 140477 - Cap. soc. € 20.000,00 int. vers.
sede legale: Fraz. Sant'Andrea
Stabilimento: Zona Ind. Villa Lempa - Via del Vecchio Mulino
64010 CIVITELLA DEL TRONTO (TE)
Tel. 0861.91.255 Fax 0861.920.294
C.F./P.I.: 01640120679

DISTRIBUZIONE

*Il presente documento controllato viene mantenuto sul server aziendale nella cartella destinata ai record del **Sistema di Gestione della Sicurezza dei dati** in modalità esclusiva di sola lettura.*

RISERVATEZZA

*Il presente documento è **strettamente riservato al personale aziendale**. Vietata ogni divulgazione all'esterno dell'azienda*

PUNTI DI CONTROLLO: ANNEX A NORMA ISO/IEC 27001

Rif. Controllo	Titolo
A.16	Gestione degli incidenti relativi alla sicurezza delle informazioni

1. Introduzione

TEXLINE è responsabile della sicurezza e dell'integrità di tutti i dati in suo possesso. TEXLINE deve proteggere questi dati utilizzando tutti i mezzi necessari per garantire in ogni momento che qualsiasi incidente che potrebbe causare danni al patrimonio e alla reputazione di TEXLINE sia impedito e/o ridotto al minimo. Esistono molti tipi di incidenti che potrebbero avere ripercussioni sulla sicurezza:

- Un incidente di sicurezza informatica è un evento che influisce negativamente sul trattamento dell'uso del computer. Questo include:

POLICY DI SISTEMA DI GESTIONE SICUREZZA DATI

1. Perdita di riservatezza delle informazioni
 2. Compromesso di integrità delle informazioni
 3. Diniego di servizio
 4. Accesso non autorizzato ai sistemi
 5. Uso improprio di sistemi o informazioni
 6. Furto e danneggiamento degli impianti
 7. Attacchi di virus
 8. Intrusione da parte degli esseri umani
- Altri incidenti includono:
 1. Perdita di badge/documenti identificativi
 2. Perdita di corrispondenza
 3. Esposizione di stampe non raccolte
 4. Supporti fuori posto o mancanti
 5. Trasmissione involontaria delle password

Garantire una segnalazione e una gestione efficaci degli incidenti di sicurezza contribuirà a ridurli e, in molti casi, a prevenirli.

2. Scopo

La gestione degli incidenti di sicurezza descritti in questa politica richiede che TEXLINE disponga di linee guida, politiche e procedure chiare. La promozione di una cultura della notifica e della registrazione proattive degli incidenti contribuirà a ridurre il numero di incidenti di sicurezza che spesso non vengono segnalati e non vengono notati, a volte, per un lungo periodo di tempo e spesso senza soluzione.

Lo scopo di questa politica è quello di:

- Descrivere i tipi di incidenti di sicurezza
- Dettagli sul modo in cui gli incidenti possono essere trattati e saranno trattati
- Identificare le responsabilità per la segnalazione e la gestione degli incidenti
- Procedure dettagliate per la notifica e l'elaborazione degli incidenti
- Fornire una guida

3. Campo di applicazione

Questa politica si applica a:

- dipendenti, agenzie partner, appaltatori e fornitori

POLICY DI SISTEMA DI GESTIONE SICUREZZA DATI

- Tutti i reparti, il personale e i sistemi (compreso il software) di TEXLINE che si occupano della memorizzazione, del recupero e dell'accesso ai dati.

4. Dichiarazione politica

La TEXLINE dispone di un chiaro meccanismo di segnalazione degli incidenti che descrive in dettaglio le procedure per l'identificazione, la segnalazione e la registrazione degli incidenti di sicurezza. Aggiornando e informando continuamente TEXLINE dipendenti, agenzie partner, appaltatori e fornitori dell'importanza dell'identificazione, della segnalazione e delle azioni necessarie per affrontare gli incidenti, TEXLINE può continuare ad essere proattiva nell'affrontare questi incidenti quando e quando si verificano.

Tutti i dipendenti di TEXLINE, le agenzie partner, gli appaltatori e i fornitori sono tenuti a segnalare quanto prima tutti gli incidenti, compresi quelli potenziali o sospetti, tramite le procedure di segnalazione degli incidenti di TEXLINE.

I tipi di Incidenti a cui questa politica si riferisce includono, ma non sono limitati a:

Computer lasciati sbloccati quando non sono presidiati

Gli utenti dei sistemi informatici di TEXLINE sono continuamente ricordati dell'importanza di bloccare i loro computer quando non sono in uso o quando lasciano i computer incustoditi per un certo periodo di tempo. Tutti i dipendenti e i collaboratori di TEXLINE, i partner, gli appaltatori e i fornitori devono assicurarsi di bloccare i propri computer in modo appropriato. Il rilevamento di un computer sbloccato che non è sorvegliato deve essere segnalato tramite le procedure di segnalazione degli incidenti di TEXLINE.

Informazioni sulla password

ID e password di account univoci vengono utilizzati per consentire l'accesso individuale a sistemi e dati. È imperativo che le singole password non vengano divulgate ad altri, indipendentemente dalla fiducia. Se una persona ha bisogno di accedere ai dati o a un sistema, deve passare attraverso le procedure corrette per l'autorizzazione - inizialmente attraverso il manager di linea della persona. Se qualcuno sospetta che la propria password o quella di un altro utente sia stata divulgata intenzionalmente, involontariamente o accidentalmente, il Servizio IT deve essere notificato tramite le procedure di segnalazione degli incidenti di TEXLINE. Per ulteriori informazioni, la policy Password di TEXLINE è disponibile sull'Intranet o tramite il Service Desk del reparto IT. In nessun caso un dipendente deve consentire a un altro dipendente di utilizzare i dettagli del proprio account utente dopo aver effettuato l'accesso a un sistema, anche sotto supervisione.

Avvertenze/allarmi antivirus

Tutti i computer desktop, portatili e tablet in uso in TEXLINE sono dotati di antivirus (incluso antispyware/malware). Per la maggior parte, l'interazione tra il computer e il software antivirus passerà inosservata agli utenti del computer. A volte, sullo schermo del computer potrebbe apparire un messaggio di avvertimento antivirus. Il messaggio potrebbe indicare la presenza di un virus che potrebbe causare perdita, furto o danneggiamento dei dati di TEXLINE. Il messaggio di avviso può indicare che il software antivirus potrebbe non essere in grado di risolvere il problema e quindi deve essere segnalato dall'utente al Servizio Clienti IT nel più breve tempo possibile.

Perdita di supporti portatili

L'uso di supporti portatili per la memorizzazione di dati (per es.: chiavette USB/unità disco) richiede all'utente di essere pienamente consapevole delle responsabilità derivanti dall'uso di tali dispositivi. L'uso di PC, laptop, tablet e molti altri dispositivi portatili aumenta la possibilità che i dati siano esposti e vulnerabili all'accesso non autorizzato. Qualsiasi utente autorizzato di un dispositivo portatile che abbia fuori posto o sospetti danni, furti intenzionali o accidentali di qualsiasi supporto portatile deve segnalarli immediatamente attraverso le procedure di segnalazione degli incidenti di TEXLINE.

Distintivi Personali

Per l'azienda è essenziale identificare gli individui presenti in ufficio e perciò è richiesto a chiunque abbia accesso agli uffici di segnalare la propria presenza e uscita dagli uffici per mezzo del sistema di rilevazione presenze. Il badge per la rilevazione delle presenze deve essere utilizzato per questo scopo da tutto il personale e dai fornitori che debbano accedere regolarmente agli uffici. I visitatori occasionali dovranno invece essere registrati in un apposito registro.

Perdita/divulgazione di dati

La potenziale perdita di dati può essere causata da diverse altre circostanze:

- trasmissione su una rete e destinati a un destinatario non intenzionale e non autorizzato (ad esempio, l'invio di dati sensibili per posta elettronica)
- Intercettazione su Internet attraverso canali non sicuri
- Inserimento di dati su Internet, accidentale o intenzionale
- Pubblicazione sul sito web di TEXLINE di dati identificati come imprecisi o inappropriati (questa eventualità deve essere segnalata)
- informazioni divulgate durante la conversazione
- divulgazione non autorizzata da parte dei dipendenti o di un rappresentante mal consigliato alla stampa o ai media

POLICY DI SISTEMA DI GESTIONE SICUREZZA DATI

- Dati che non possono più essere localizzati e che non sono più contabilizzati in un sistema informatico
- Copie cartacee di dati e informazioni non più localizzabili
- Copie cartacee di informazioni e dati accessibili da scrivanie e aree non presidiate

Tutti i dipendenti di TEXLINE, le agenzie partner, i contraenti e i fornitori devono agire in modo responsabile e professionale ed essere sempre consapevoli dell'importanza di mantenere la sicurezza e l'integrità dei dati di TEXLINE.

Qualsiasi perdita di dati e/o divulgazione, intenzionale o accidentale, deve essere segnalata immediatamente utilizzando le procedure di segnalazione degli incidenti di TEXLINE

Abuso di informazioni personali

Tutte le informazioni che consentono l'identificazione di una persona - ossia le informazioni che possono identificare una persona, come l'indirizzo di casa, le coordinate bancarie, ecc. - non devono essere divulgate, discusse o trasmesse ad alcuna persona che non sia in grado di visionarle, divulgarle o distribuirle.

Qualsiasi abuso/uso improprio di tali informazioni identificabili deve essere segnalato attraverso le procedure di segnalazione degli incidenti di TEXLINE

Sicurezza fisica

È di fondamentale importanza mantenere la sicurezza fisica degli uffici e delle stanze in cui i dati sono conservati, mantenuti, visualizzati o consultati. I locali o gli uffici che sono stati designati specificamente come zone in cui sono ubicate o conservate informazioni sicure devono disporre di un metodo per rendere fisicamente sicuro l'accesso a tali locali, ad esempio un meccanismo combinato di serratura a chiave. Le finestre del piano/livello inferiore potrebbero anche fornire l'accesso alla stanza/all'ufficio e devono essere bloccate in modo sicuro, in particolare quando la stanza viene lasciata incustodita. Le stanze che non sono state protette non devono essere utilizzate per memorizzare informazioni e dati sensibili e personali; le preoccupazioni relative alle stanze/uffici che devono essere chiuse in modo sicuro o l'accesso limitato devono essere segnalate al Servizio IT tramite le procedure di segnalazione degli incidenti di TEXLINE.

La continua enfasi e il rafforzamento della politica di scrivania sicura di TEXLINE contribuirà ulteriormente a ridurre il numero di incidenti di sicurezza.

Sicurezza logica / Controlli di accesso

POLICY DI SISTEMA DI GESTIONE SICUREZZA DATI

Controllare, gestire e limitare l'accesso alla rete, ai database e alle applicazioni della TEXLINE è una parte essenziale della sicurezza delle informazioni. È necessario garantire che solo i dipendenti autorizzati possano accedere alle informazioni elaborate e conservate elettronicamente.

Corrispondenza mancante

I dati o le informazioni inviati elettronicamente o fisicamente che non possono essere contabilizzati, ad esempio, non arrivano alla destinazione prevista tramite posta, inviati elettronicamente, inviati per la stampa ma non stampati ecc. devono essere segnalati tramite le procedure di segnalazione degli incidenti di TEXLINE.

Corrispondenza/media trovati

I dati memorizzati su qualsiasi supporto di memorizzazione o le informazioni fisicamente stampate che sono stati trovati in un luogo diverso da un luogo sicuro o un luogo dove la sicurezza e l'integrità dei dati / informazioni potrebbero essere compromesse dalla visualizzazione non autorizzata e / o l'accesso ad esempio stampe sbloccate, scartate CD (supporti), devono essere segnalati attraverso le procedure di segnalazione degli incidenti di TEXLINE

Perdita o furto di informazioni/informazioni informatiche

I dati o le informazioni che non possono più essere localizzati o contabilizzati, ad esempio, non possono essere trovati in un luogo in cui ci si aspetta che siano, archivi o altro, o che sono noti o sospettati di essere stati rubati, devono essere segnalati immediatamente attraverso le procedure di segnalazione degli incidenti di TEXLINE

5. Responsabilità

È responsabilità di tutti i dipendenti di TEXLINE, delle agenzie partner, dei contraenti e dei fornitori che lavorano per TEXLINE, all'interno o all'esterno della sede, essere proattivi nella segnalazione degli incidenti di sicurezza. Le procedure di segnalazione degli incidenti di NOME_AZIENDA sono in atto per prevenire e ridurre al minimo il rischio di danni all'integrità e alla sicurezza dei dati e delle informazioni di TEXLINE.

È inoltre responsabilità di tutti gli individui e i gestori di dati e informazioni di TEXLINE garantire che vengano seguite tutte le politiche e le procedure relative alla sicurezza e all'integrità delle informazioni e dei dati.

6. Adempimenti di obblighi legali e contrattuali

Reg. Ue 2016/679 e D.lgs. 101/2018

7. Violazioni della Politica

Le violazioni della presente politica e/o gli incidenti di sicurezza possono essere definiti come eventi che potrebbero causare perdite di dati o danni alle attività di TEXLINE, o come eventi che violano le procedure e le politiche di sicurezza di TEXLINE.

Tutti i dipendenti di TEXLINE, le agenzie partner, i contraenti e i fornitori hanno la responsabilità di segnalare incidenti di sicurezza e violazioni di questa politica il più presto possibile attraverso la Procedura di segnalazione degli incidenti di TEXLINE. Tale obbligo si estende anche a qualsiasi organizzazione esterna incaricata di supportare o accedere ai sistemi informativi di TEXLINE.

Nel caso di fornitori, consulenti o appaltatori terzi, il mancato rispetto può comportare l'immediata rimozione dell'accesso al sistema. Se dalla non conformità risultano danni o compromissioni ai sistemi ICT o alla rete di TEXLINE, TEXLINE prenderà in considerazione un'azione legale contro la terza parte. TEXLINE adotterà le misure appropriate per porre rimedio a qualsiasi violazione della politica attraverso i quadri normativi in vigore. Nel caso di un dipendente, la questione può essere trattata nell'ambito del processo disciplinare di TEXLINE.

La presente Politica fa riferimento ad altre politiche e linee guida di NOME_AZIENDA. Copie di queste dichiarazioni sono disponibili tramite la rete Intranet di NOME_AZIENDA o su richiesta al reparto IT, a seconda dei casi.

La presente Politica è mantenuta e revisionata dal team Sicurezza/Business Continuity di TEXLINE e ratificata dall'alta direzione di TEXLINE.

8. Gestione Documentale

Il presente documento è valido a partire dalla data di rilascio.

Il presente documento viene periodicamente riesaminato e comunque con cadenza almeno annuale al fine di garantire il rispetto dei seguenti criteri previsti.

- Conformità ai requisiti della norma ISO 27001
- Requisiti legislativi definiti dalla legge, se del caso