Politica per la sicurezza delle informazioni

1. PREMESSA

Il Gruppo CIDIU ha definito la presente politica per la sicurezza dei dati e delle informazioni, prevista dal Sistema di Gestione ISO/IEC 27001:2022.

In generale, il presente documento stabilisce che tutte le informazioni riguardanti CIDIU S.p.A. e CIDIU Servizi S.p.A. sono da considerarsi di proprietà di CIDIU S.p.A. e CIDIU Servizi S.p.A. stesse. Per questo motivo esse devono essere protette contro la diffusione non autorizzata, la modifica, la compromissione e la distruzione.

Queste protezioni sono implementate secondo il principio del "*need-to-know*", ovvero le informazioni classificate devono essere condivise solamente con chi ha una legittima necessità di business di accedere alle stesse.

I criteri per identificare secondo quale livello le informazioni siano da classificare, derivano direttamente:

- Dal rischio di generici danni nel caso di diffusione erronea o dolosa all'esterno delle società;
- Dalle leggi/norme sui segreti commerciali ed industriali;
- Dalle leggi/norme sulla protezione dei dati personali.

I dati aziendali sono classificati in base alla loro importanza e sensibilità.

Come riportato nelle apposite procedure, i dati e le informazioni di CIDIU sono classificate in quattro categorie distinte in base alla loro importanza.

- PUBBLICI
- USO INTERNO
- CONFIDENZIALI
- RISERVATI

La Politica di Sicurezza è basata su alcuni principi fondamentali, di seguito elencati:

- I dati Aziendali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati stessi, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (Integrità e Riservatezza) e resi disponibili laddove dove richiesto dal business di CIDIU S.p.A. e CIDIU Servizi S.p.A. (Disponibilità)
- L'accesso ai dati aziendali deve essere fornito in relazione all'attività ed al ruolo dell'utente;
- L'accesso agli utenti deve essere autorizzato dagli *Asset Owner* (responsabili di Processo e/o di Funzione);
- Tutte le normative legali, statutarie e contrattuali devono essere rispettate;
- Tutti gli utenti che accedono ai dati aziendali devono essere identificati.

Si precisa che il concetto di corretta conservazione dei dati e delle informazioni (*Data Retention*) è indissolubilmente legato al concetto di sicurezza dei dati e delle informazioni stesse.

La presente Politica, così come la procedura di riferimento (P 38 – Sicurezza delle Informazioni) e le relative Istruzioni Operative disciplinano le linee guida e le attività per la sicurezza delle informazioni applicate esclusivamente agli strumenti, asset (hardware e software) e processi approvati e gestiti dalle Società Cidiu S.p.A. e Cidiu Servizi S.p.A.

Sono vietati e non rientrano nell'ambito della presente Politica tutti gli strumenti e asset (hardware e software) che gli utenti possono scaricare, installare o utilizzare autonomamente (senza previa autorizzazione dell'azienda) o con l'aiuto di terzi mediante gli strumenti aziendali (notebook, smartphone, tablet), nonché eventuali software open source e dispositivi hardware (es. IoT, chiavette USB, hard disk, fotocamere) senza autorizzazione esplicita da parte dell'azienda, o di cui l'azienda non abbia conoscenza o che non siano stati formalmente censiti e approvati. L'azienda adotta comunque misure tecniche ed organizzative per rilevare e gestire tali asset non autorizzati, inclusi controlli periodici, monitoraggi dei sistemi e audit.

2. OBIETTIVI

L'obbiettivo principale della politica per la sicurezza delle informazioni è gestire i rischi legati alla sicurezza delle informazioni a un livello accettabile.

In pratica, la politica mira a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni, garantendo che siano al sicuro da minacce interne ed esterne, deliberate o accidentali.

Questa politica si applica quindi a tutti i dati aziendali creati, ricevuti o gestiti dall'azienda, inclusi documenti elettronici, e-mail, registrazioni cartacee e altri formati di dati.

CIDIU S.p.A. e CIDIU Servizi S.p.A. considerano la protezione del proprio patrimonio di informazioni elemento fondamentale per la tutela e la continuità del proprio business.

Altro obiettivo del presente documento è quello di definire i principi e le linee guida da adottare, nonché i ruoli, le funzioni e le responsabilità nella realizzazione di un efficace sistema di protezione delle informazioni, che devono essere rispettate da tutte le persone che operano all'interno di CIDIU S.p.A. e CIDIU Servizi S.p.A.

In questo ambito, la sicurezza dell'informazione è vista un tutt'uno come un insieme di processi e tecnologie, misure organizzative e comportamentali finalizzate alla garanzia degli aspetti di Riservatezza, Integrità e Disponibilità delle informazioni, ed alla loro corretta condivisione, in funzione del ruolo e del profilo dell'utente.

In ottica di *Data Retention* (conservazione dei dati e delle informazioni) ulteriore obbiettivo di questa politica è anche quello di definire le linee guida per la conservazione e l'eliminazione dei dati aziendali, garantendo la conformità alle normative legali e la protezione delle informazioni sensibili.

Nello specifico, le finalità del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) da conseguire sono:

a) assicurare l'evidenza dei processi autorizzativi e delle attività svolte a fini legali, fiscali ed operativi.

b) garantire la protezione delle informazioni aziendali e la continuità delle attività lavorative, assicurando che il livello di protezione previsto sia attuato in funzione della criticità delle informazioni da proteggere;
c) garantire l'attuazione pratica della Politica Aziendale per la Sicurezza e Protezione dei dati e del rispetto della Privacy integrando i requisiti del Sistema di Gestione per la Sicurezza delle informazioni nei processi dell'organizzazione con la finalità di soddisfare i requisiti stessi e fissando un quadro di riferimento per identificare e gestire i relativi obiettivi;
d) erogare i servizi nel rispetto dei contratti e dei Service Level Agreement (SLA) previsti;
e) garantire la confidenzialità, l'integrità e la disponibilità delle informazioni su tutto il ciclo di trattamento gestito;
f) garantire un'adeguata sicurezza logica e fisica nella gestione ed erogazione dei servizi salvaguardando i prodotti ed i relativi servizi contrastando nel contempo la criminalità informatica (virus, attacchi in rete, etc.);
g) garantire elevati livelli di affidabilità dei propri sistemi informativi al fine di minimizzare le potenziali indisponibilità dei servizi;
h) redigere, diffondere, organizzare e verificare procedure e risorse per affrontare eventi di natura disastrosa e garantire la continuità operativa;
i) promuovere i processi di innovazione tecnologica al fine di contrastare l'obsolescenza dei Sistemi al fine di incrementare l'efficienza e la sicurezza dei servizi;
j) individuare e gestire rischi e opportunità per assicurare il raggiungimento degli obiettivi minimizzando gli effetti indesiderati e massimizzando le ricadute positive.

Per quanto riguarda la *Data Retention* si possono identificare ulteriori obbiettivi che nel caso di CIDIU si possono riassumere con quelli sotto riportati:

k) *Conformità Legale*: Assicurare che l'azienda rispetti tutte le leggi e i regolamenti relativi alla conservazione dei dati, evitando sanzioni e responsabilità legali.
l) *Protezione dei Dati*: Salvaguardare le informazioni sensibili e personali da accessi non autorizzati, perdite o violazioni.
m) *Efficienza Operativa*: Ottimizzare la gestione dei dati, riducendo il volume di informazioni obsolete o non necessarie, migliorando così l'efficienza dei sistemi informatici.
n) *Recupero dei Dati*: Facilitare il recupero rapido e accurato dei dati necessari per le operazioni aziendali, le decisioni strategiche e le richieste legali.
o) *Riduzione dei Costi*: Minimizzare i costi associati alla conservazione e alla gestione dei dati, eliminando quelli non più necessari

Gli obiettivi sono gestiti e mantenuti sotto controllo dalla Direzione relativamente allo sviluppo e raggiungimento dei traguardi.
Tali obbiettivi possono essere monitorati mediante:

- Report periodici (semestrali / trimestrali)

- Riesame della Direzione
- KPI specifici
- Piano di miglioramento

La presente Politica è coerente con il Codice Etico aziendale e con il Codice di Comportamento Anticorruzione. Ogni scostamento dalla presente Politica, dal Codice Etico e dal Codice di Comportamento Anticorruzione non è riconosciuto come volontà della Direzione Aziendale ed è oggetto di indagine ed eventuale azione disciplinare.

3. PRINCIPI GUIDA

Di seguito vengono elencati e specificati i principi guida:

a) Tutti gli standard di sicurezza delle informazioni devono essere implementati e la loro adeguatezza ed affidabilità periodicamente verificata.

b) L'accesso ai sistemi, alle applicazioni ed alle informazioni deve avvenire tramite specifici meccanismi di autenticazione dell'utente. L'accesso deve essere autorizzato solo per quanto necessario al ruolo ricoperto dall'utente. Eventuali eccezioni e le relative modifiche devono essere registrate.

c) L'Asset Owner (responsabile di Processo e/o di Funzione) è responsabile per le autorizzazioni di accesso, assicurandone la rimozione nel caso in cui non siano più necessarie e verificandone periodicamente l'adeguatezza.

d) La responsabilità per l'amministrazione dei diritti di accesso deve essere chiaramente definita e mantenuta separata da quella degli utenti che otterranno l'autorizzazione all'accesso e che saranno soggetti a periodici review.

e) Devono essere implementati specifici meccanismi di controllo, di tipo fisico e logico, per gli accessi a tutti i sistemi/processi che ospitano/processano il patrimonio informativo di CIDIU S.p.A. e CIDIU Servizi S.p.A.

f) Tutti i sistemi e le applicazioni, opportunamente progettati, devono poter essere in grado di produrre opportuni log delle attività eseguite. I log devono essere attivati mediante opportune procedure e relative autorizzazioni.

g) Le caratteristiche dei meccanismi di controllo implementati dipendono dalla valutazione della criticità dei sistemi, delle applicazioni e dei dati aziendali. Un'elevata criticità si traduce necessariamente con l'implementazione di controlli caratterizzati da un alto livello di sicurezza.

h) Tutte le attività di gestione dei sistemi/applicazioni/informazioni devono essere svolte con il livello di *privilegio minimo* necessario per condurre l'attività.

i) Tutte le informazioni, le applicazioni ed i sistemi devono poter essere ripristinati in caso di malfunzionamento. Per quelli ritenuti critici per il Business, devono poter essere ripristinati in caso di disastro.

j) Connessioni di rete esterne possono essere realizzate solo da persone o Società autorizzate. Il contenuto delle trasmissioni deve rispettare i requisiti definiti da CIDIU S.p.A. e CIDIU Servizi S.p.A. in base al livello di criticità dei dati.

k) Tutti i Fornitori/Service Provider, nel caso trattino dati sensibili ai fini aziendali, devono sottoscrivere un NDA (Non Disclosure Agreement) che preveda l'obbligo di mantenere la riservatezza di tutte le informazioni, ad

essi non pertinenti, ottenute durante la realizzazione delle loro attività. Inoltre devono essere rispettate le norme e le leggi vigenti nei Paesi in cui sono realizzate le attività.

Collegno, li 09/03/2026

Il Direttore Generale
Dott. Silvio Barbiera
(firmato in originale)