# Sistema di gestione per la sicurezza delle informazioni

## Politica della sicurezza delle informazioni

Assotherm
Servizi associati per la termoidraulica

## 1. Introduzione

Per il conseguimento dei suoi obiettivi di business, la società ASSOTHERM SRL, (di seguito indicata come "ASSOTHERM SRL" o la "Società") sono impegnate nello sviluppo di azioni di miglioramento strutturale, in particolare anche curando l'evoluzione dei sistemi informativi nel rispetto degli standard di qualità e di sicurezza. In quest'ottica, la sicurezza delle informazioni è di fondamentale importanza: una corretta gestione deve prevedere la protezione delle informazioni da un'ampia gamma di minacce, assicurando la continuità del business aziendale, minimizzando i danni in caso di incidenti e massimizzando le opportunità di miglioramento.
Il principale obiettivo del presente documento è migliorare il governo della sicurezza delle informazioni di ASSOTHERM SRL, contribuendo in particolare a:

- regolamentare gli ambiti e le misure di governo della sicurezza delle informazioni;
- recepire e garantire l'applicazione e il rispetto del principio RID (Riservatezza, Integrità e Disponibilità) delle informazioni;
- prevenire la perdita di capitale intellettuale o dati critici per il business;
- promuovere la consapevolezza e le capacità di gestione del rischio aziendale legato all'ICT;
- favorire il raggiungimento della conformità ai requisiti normativi sia nazionali che internazionali;
- aumentare il vantaggio competitivo mediante una gestione più efficiente ed efficace delle risorse ICT e strumenti di sicurezza a supporto.

## 2. Scopo e Ambito del Documento

La presente policy definisce l'approccio di ASSOTHERM SRL e i principi generali che devono essere adottati da tutto il personale, nel governo dei sistemi informatici, dai processi e dalle procedure che operano al suo interno, al fine di garantire la protezione e la sicurezza delle informazioni.

La politica per la sicurezza delle informazioni è finalizzata al conseguimento dei seguenti obiettivi:

- Riservatezza: garantire che un determinato dato di cui ASSOTHERM SRL è titolare/proprietario sia reso disponibile soltanto ai processi che lo devono elaborare e al personale che è legittimato al suo utilizzo. Salvaguardare la riservatezza dell'informazione significa proteggerla da accessi volontari o involontari da parte di entità senza autorizzazione;
- Integrità: garantire che l'informazione sia completa e accurata e non sia alterata a seguito di modifiche intenzionali non autorizzate o accidentali. Salvaguardare l'integrità dell'informazione significa proteggerla da cancellazioni o modifiche a seguito di interventi da parte di entità non autorizzate o del verificarsi di fenomeni non controllabili;
- Disponibilità: garantire che l'informazione sia fruibile da parte di tutte le persone autorizzate nel momento in cui è richiesta, in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione. Salvaguardare la disponibilità dell'informazione significa proteggerla da un mancato accesso all'informazione a seguito del verificarsi di eventi sia dolosi che accidentali che compromettono la fruibilità del dato;
- Conformità: garantire un costante rispetto delle normative, degli accordi contrattuali e degli standard di riferimento.

Questo documento si applica alle Funzioni di ASSOTHERM SRL coinvolte nella fornitura di servizi che effettuano trattamenti sui dati e sulle informazioni di proprietà dell'azienda o in ogni modo da essa gestite; sono altresì compresi i dati personali soggetti alla normativa sulla protezione dei dati. È responsabilità di tutti gli interessati proteggere il patrimonio informativo aziendale in coerenza con le norme di legge in vigore e con le procedure aziendali previste.

La presente politica si applica a tutte le informazioni nelle sue diverse forme (scritte, orali, registrate o stampate elettronicamente), raccolte o mantenute da o per conto di ASSOTHERM SRL e a tutti i sistemi informativi utilizzati o gestiti da ASSOTHERM SRL o da qualsiasi organizzazione per conto di ASSOTHERM SRL.

## 3. Glossario Termini e definizioni

| Termine | Definizione |
|---|---|
| **Rischio informatico (o ICT)** | Il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (ICT). |
| **Dati personali** | Tutte le informazioni relative a persone fisiche che consentano l'identificazione, diretta o indiretta, degli individui a cui i dati si riferiscono. Ad esempio, sono dati personali oggetto di tutela, oltre ai dati anagrafici ed economici, anche le immagini ed i codici identificativi riconducibili ad un individuo. |
| **Abilitazione** | Possibilità per un utente di accedere alle funzionalità di una risorsa informatica. Rappresenta l'insieme delle transazioni/informazioni/dati cui un utente autorizzato può accedere e dei relativi privilegi di accesso (es. lettura, modifica, esecuzione). |
| **Credenziali di accesso/autenticazione** | Parametri, composti generalmente da una sequenza di caratteri (alfanumerici o simboli), che vengono utilizzati come forma di autenticazione per ottenere l'accesso ad un sistema informatico, con le abilitazioni concesse all'utente che si autentica. |
| **Profilo utente** | Insieme di abilitazioni aggregate secondo un criterio funzionale (per esempio in base al ruolo o alle mansioni aziendali) ed attribuite ad una classe di utenti. |
| **Utenza** | Identificativo assegnato ad un utente informatico che gli permette di accedere ad un sistema IT in base alle proprie abilitazioni. |
| **Utenze privilegiate (super-user)** | Utenze applicative o infrastrutturali a cui sono assegnati profili abilitativi che permettono di compiere operazioni non consentite ad utenti standard. Tali utenze, ad esempio, possono installare aggiornamenti al sistema operativo, o creare utenze in un dato applicativo o sistema. |
| **Utenze di dominio** | Utenze assegnate a tutti i dipendenti e collaboratori esterni al fine di permetterne l'accesso a strumenti informatici di base (accesso al dominio, alla intranet e alla posta elettronica). |
| **Asset ICT** | Server, apparati di comunicazione, postazioni di lavoro, dispositivi mobili, cablaggi, infrastrutture logistiche, supporti dati rimovibili, sistemi di stampa, di proprietà o utilizzati dalla Banca (per esempio tramite leasing, affitto o licenza). |
| **Apparati ICT** | Apparati che costituiscono elementi infrastrutturali sistemici del sistema informatico, ovvero il cui malfunzionamento può pregiudicare il regolare e sicuro funzionamento del sistema informatico (per esempio i data server, gli apparati di rete, ecc.). |
| **Locali ICT** | Armadi di piano che ospitano o che sono destinati ad ospitare apparati ICT. |
| **Data Center** | Locale dove vengono collocate le apparecchiature e i servizi di gestione dei dati. Anche definito solo Centro di Elaborazione Dati (CED), Data Center o Sala Server. |

## Normativa esterna

La presente Policy tiene in considerazione i seguenti riferimenti alla normativa esterna:

- Regolamento UE 2016/679 (General Data Protection Regulation);

## Standard e Best Practice

La presente Policy tiene in considerazione i seguenti riferimenti ai seguenti standard di sicurezza e best practice:

| Titolo Norma | Descrizione | Fonte normativa | Indirizzo web |
|---|---|---|---|
| **ISO/IEC 27001:2022** | Standard internazionale per la gestione della sicurezza delle informazioni. | ISO/IEC | iso.org |
| **ISO/IEC 27002:2022** | Information technology - Security techniques - Code of practice for Information Security controls | ISO/IEC | iso.org |
| **ISO/IEC 27005:2011** | Information technology - Security techniques - Information Security risk management | ISO/IEC | iso.org |
| **ISO/IEC 27035:2011** | Information technology - Security techniques - Information security incident management. | ISO/IEC | iso.org |
| **ISO 27701:2021** | Tecniche di sicurezza – Estensione a ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni in ambito privacy – Requisiti e linee guida | ISO/IEC | iso.org |
| **ISO 22301:2019** | Sicurezza e resilienza – Sistemi di gestione per la continuità operativa – Requisiti | ISO | Iso.org |
| **ISO/IEC 27017:2015** | Linee guida per la sicurezza delle informazioni nei servizi cloud. | ISO/IEC | iso.org |
| **ISO/IEC 27018:2019** | Codice di condotta per la protezione delle informazioni personali nei servizi cloud pubblici. | ISO/IEC | iso.org |
| **GDPR (Regolamento UE 2016/679)** | Regolamento generale sulla protezione dei dati personali. | Unione Europea | gdpr.eu |
| **D.Lgs. 196/2003 (Codice della Privacy)** | Normativa italiana sulla protezione dei dati personali. | Italia | garanteprivacy.it |
| **D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale)** | Normativa italiana per la digitalizzazione della pubblica amministrazione e la sicurezza informatica. | Italia | agid.gov.it |
| **Regolamento eIDAS (Regolamento UE 910/2014)** | Regolamento europeo sull'identificazione elettronica e servizi fiduciari per le transazioni elettroniche. | Unione Europea | ec.europa.eu |
| **Legge 48/2008 (Recepimento Convenzione di Budapest)** | Normativa italiana sulla criminalità informatica. | Italia | normattiva.it |
| **Direttiva NIS (Direttiva UE 2016/1148)** | Direttiva europea sulla sicurezza delle reti e dei sistemi informativi. | Unione Europea | ec.europa.eu |

| | | | |
|---|---|---|---|
| **Regolamento UE 2018/1807 (Libera Circolazione dei Dati Non Personali)** | Regolamento europeo per la libera circolazione dei dati non personali nell'UE. | Unione Europea | eur-lex.europa.eu |

# 4. Ruoli e responsabilità

ASSOTHERM SRL è impegnata nell'assicurare una corretta gestione del processo di sicurezza delle informazioni sin dalla definizione del modello organizzativo nonché dei ruoli e delle responsabilità che ne derivano, con l'obiettivo di favorire il continuo esercizio dei requisiti e l'accountability.

## Consiglio di Amministrazione

Con riferimento al governo della sicurezza delle informazioni di ASSOTHERM SRL, al Consiglio di amministrazione (o C.d.A.) sono attribuite le responsabilità di:

- Approvare gli orientamenti strategici, il profilo e i livelli di rischio accettabili di ASSOTHERM SRLin materia di sicurezza delle informazioni.
- Approvare le policy dell'information security management system, che definiscono le responsabilità delle funzioni aziendali in materia di sicurezza delle informazioni.
- Fornire risorse sufficienti per definire, implementare, monitorare, rivedere, mantenere e migliorare la strategia di sicurezza delle informazioni promuovere con tempestività idonee misure correttive in caso di riscontro di criticità.

## Amministratore Delegato (AD)

All'Amministratore Delegato spetta il compito di supportare il Consiglio di amministrazione nei relativi processi decisionali. In particolare, l'AD ha in carico le responsabilità di:

• Assicurare che le politiche aziendali, le procedure e i regolamenti legati alla sicurezza delle informazioni siano tempestivamente comunicati a tutto il personale interessato.

• Approvare le misure necessarie nel caso in cui emergano carenze o anomalie dall'insieme delle verifiche svolte sul sistema dei controlli interni.

## Funzione Risk Management

La funzione di Risk Management è preposta all'individuazione e identificazione delle metriche di misurazione e mitigazione dei vari rischi a cui è esposta l'organizzazione.

La funzione svolge le seguenti attività:

- Definire, in collaborazione con la funzione Information Security & IT Compliance, le modalità di integrazione delle fattispecie di rischio operativo con gli scenari di rischio informatico in coerenza con quanto riportato nella Policy di gestione del Rischio ICT e di Sicurezza.
- Definire la propensione al rischio legato ai requisiti di sicurezza.

## Internal Audit

La funzione svolge le seguenti attività:

- Valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli Organi aziendali i possibili miglioramenti al processo di gestione dei rischi, nonché agli strumenti di misurazione e controllo degli stessi.

- Verificare la regolarità delle diverse attività aziendali incluse quelle esternalizzate, il rispetto dei limiti previsti dai meccanismi di delega, l'adeguatezza, l'affidabilità complessiva e la sicurezza del sistema informativo (IT audit).
- Formulare, a seguito della rilevazione di particolari criticità, eventuali raccomandazioni ed effettua delle attività di follow-up sulle stesse.

## Information Security & IT Compliance

La funzione Information Security & IT Compliance, presidiata dal DPO, governa la sicurezza delle informazioni e dei beni aziendali di ASSOTHERM SRL e costituisce il riferimento in azienda per la prevenzione, raccoltadati, analisi e gestione degli eventi e incidenti di sicurezza informatica.

La funzione svolge le seguenti attività:

- Definire la strategia di sicurezza delle informazioni della Società, garantendo allineamento alle esigenze di business e monitorando che i presidi di sicurezza siano conformi alla normativa vigente e in linea con il profilo di rischio IT.
- Definire, nel più ampio contesto di gestione dei rischi aziendali, politica e metodologie di valutazione del rischio ICT e di sicurezza, eseguire l'analisi del rischio ICT, compartecipare alla predisposizione del relativo piano di trattamento e produrre la reportistica sullo stato del rischio ICT e di sicurezza assicurando, nella definizione delle misure di mitigazione, il corretto bilanciamento tra i costi e benefici
- Definire la politica di sicurezza delle informazioni aziendale e governare la normativa interna di sicurezza (processi e modelli operativi), assicurandone l'allineamento alle normative di riferimento e agli obiettivi aziendali e di business.
- Definire e indirizzare le misure procedurali e tecnologiche di sicurezza, verificandone l'adeguatezza in termini di protezione del patrimonio informativo aziendale.
- Tenere i contatti con gli Stakeholder esterni e verificare la congruità delle misure poste in essere con le aspettative di questi ultimi. Definire i piani di miglioramento al fine di mantenere la capacità di soddisfare i requisiti del mercato.
- Presidiare gli incidenti di sicurezza delle informazioni, valutarne la gravità, definire e coordinare la strategia di rientro dall'incidente, di concerto con le altre funzioni coinvolte (DPO, IT, Funzioni di Business, altro), al fine di minimizzarne gli impatti e di ripristinare nel più breve tempo possibile la capacità normale operatività dei servizi coinvolti;
- Promuovere lo sviluppo, con il supporto della funzione competente, dei programmi di formazione e sensibilizzazione sulle tematiche di propria competenza.
- Identificare, nel più ampio contesto di gestione dei rischi di conformità, i rischi di conformità legati alla sicurezza delle informazioni, compresi i rischi legati allo sviluppo di nuovi prodotti e servizi (Security by Design).
- Individuare le diverse azioni di mitigazione e controllo, al fine di poter fornire idonea informativa alle funzioni di business, oltre che agli altri attori del Sistema dei Controlli Interni, all'Organizzazione e ai soggetti esterni coinvolti (nelle casistiche necessarie).
- Implementare e mantenere un piano per assicurare la continuità operativa dei processi di Business e dei servizi IT critici in caso di scenari di crisi.

## Information Technology

La funzione Information Technology, presidiata dal Resp. IT, si occupa della gestione ordinaria, del monitoraggio continuo e della conduzione proattiva delle attività legate alla sicurezza dell'infrastruttura IT (rete, sistemi ed applicazioni), allo scopo di migliorare il livello di protezione dell'organizzazione.

La funzione svolge le seguenti attività:

- Gestire operativamente l'aderenza alla normativa e la sicurezza informatica, implementando e mantenendo le misure di protezione e i controlli di primo livello in accordo con le policy e le procedure aziendali.
- Monitorare le attività di pianificazione in ambito IT, valutando i rischi e gli impatti di sicurezza, in collaborazione con la Funzione Information Security & IT Compliance, dei sistemi informativi legati alle evolutive di prodotti e servizi.
- Garantire il presidio delle attività esternalizzate di pertinenza, con particolare riferimento al monitoraggio dei requisiti di sicurezza;
- Gestire le impostazioni/configurazioni di sicurezza legate all'infrastruttura IT (rete, sistemi ed applicazioni).
- Definire, progettare, aggiornare e condividere con la Funzione Information Security & IT Compliance le soluzioni atte alla rilevazione di eventi di sicurezza o vulnerabilità.
- Monitorare l'infrastruttura IT in tempo reale al fine di supportare nell'individuazione tempestiva dei tentativi di intrusione e di attacco;
- Eseguire analisi infrastrutturali atte a identificare vulnerabilità.
- Segnalare le vulnerabilità di sicurezza rilevate all'interno del perimetro monitorato.
- Analizzare gli eventi di sicurezza rilevati all'interno del perimetro monitorato.
- Segnalare gli incidenti di sicurezza rilevati all'interno del perimetro monitorato.
- Supportare le altre strutture aziendali durante il processo di gestione degli incidenti di sicurezza.
- Supportare nell'analisi delle cause (root cause) degli incidenti di sicurezza e condividere le informazioni di dettaglio con la Funzione Information Security & IT Compliance in caso di incidenti rilevanti.

# 5. Sicurezza delle informazioni

Al fine di garantire la riservatezza, l'integrità e la disponibilità delle informazioni, ASSOTHERM SRL definisce i principi generali e li articola in un insieme di controlli di sicurezza (di tipo organizzativo, logico e fisico), i quali costituiscono la prassi corrente per garantire la sicurezza delle informazioni e dei dati personali.

Si specifica che le informazioni come da standard ISO/IEC 27001 sono "l'insieme di dati che hanno valore per un individuo o un'organizzazione", mentre i dati personali come da definizione di cui all'art. 4 del GDPR sono "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

## 5.1. Aspetti organizzativi della sicurezza

Al fine di garantire un'adeguata protezione del patrimonio informativo è fondamentale valutare e indirizzare opportunamente gli aspetti di sicurezza, pertanto nell'ambito dell'organizzazione della Società:

- Sono chiaramente definite e formalizzate le responsabilità in materia di sicurezza delle informazioni.
- Il Sistema di Gestione della Sicurezza delle Informazioni, il cui riferimento è rappresentato dallo Standard ISO/IEC 27001, viene sviluppato adottando il modello iterativo del "Plan-Do-Check-Act" (PDCA), al fine di garantirne il continuo miglioramento e l'integrazione con altri sistemi di gestione adottati da ASSOTHERM SRL. Le componenti di questo modello sono descritte di seguito:
  - Plan: redazione di politiche, linee guida, procedure, struttura organizzativa e processi aziendali relativi alla sicurezza delle informazioni, che garantiscano l'identificazione, l'analisi e il trattamento dei rischi e che permettano di raggiungere gli obiettivi di sicurezza e di business dell'azienda.
  - Do: implementare, gestire e monitorare l'insieme dei requisiti identificati nella prima fase.
  - Check: misurare e verificare l'efficacia dei controlli e l'adeguatezza dei processi implementati.
  - Act: mantenere e migliorare la maturità raggiunta, attraverso azioni preventive e correttive.
  - Il Sistema di Gestione della Sicurezza delle informazioni è verificato periodicamente ed eventualmente migliorato sulla base delle risultanze e/o impatti esterni o interni rilevanti.
- Un'attività di analisi del rischio informatico è eseguita con cadenza periodica o a fronte di cambiamenti significativi; in funzione del livello di rischio evidenziato sono definite adeguate misure di sicurezza. L'attività di analisi del rischio è condotta anche a fronte di nuove iniziative o progetti che presentano impatti sul sistema informativo della Società.
- Le valutazioni dei rischi operativi e di sicurezza relativi ai servizi di pagamento sono condotte periodicamente con una frequenza almeno annuale per i sistemi ICT critici e almeno ogni tre anni per i sistemi non critici.
- Sono previsti controlli periodici, secondo i ruoli e le responsabilità definiti, volti ad accertare la robustezza e l'efficacia delle contromisure realizzate, nonché per garantire la congruenza con il processo di valutazione dei rischi ICT e di sicurezza.
- Per ciascun nuovo progetto aziendale o iniziativa riguardante il patrimonio informativo, la sicurezza delle informazioni deve essere sempre considerata e valutata, prestando particolare attenzione ai dati relativi alle informazioni personali secondo quanto definito dalla normativa di riferimento.
- Sono ripartire in modo opportuno le responsabilità sulla base del principio di segregazione dei compiti (rif. "segregati on of duties") al fine di limitare eventi quali modifiche non autorizzate o abuso delle risorse aziendali.

- Gli utenti hanno accesso alle informazioni aziendali necessarie allo svolgimento delle rispettive mansioni ed in base al ruolo aziendale assegnato, secondo il principio del “Privilegio minimo” e “Bisogno di sapere” (rif. “need-to-know”).
- Sono stabiliti e mantenuti contatti con gruppi di interesse specialistici e associazioni professionali in materia di sicurezza delle informazioni, al fine di promuovere l’aggiornamento continuo, migliorare la conoscenza delle best practice, scambiare informazioni in merito a minacce, vulnerabilità, nuovi servizi, prodotti e tecnologie.
- Le verifiche di sicurezza sono condotte in seguito al verificarsi di un incidente nonché in caso di cambiamenti significativi all’infrastruttura, ai processi o alle procedure o a causa di un rilascio di applicazioni critiche connesse ad internet (nuove o modificate).
- È prevista l’esecuzione di verifiche volte a identificare l’esistenza di potenziali scenari di rischio non noti o rilevanti, a fronte del rilevamento di minacce o modifiche occorse.
- Ogni trasferimento di informazioni deve essere preventivamente autorizzato nel rispetto degli standard/istruzioni operative in vigore (si rimanda anche al documento interno Norme comportamentali per la gestione dei beni aziendali).

## 5.1. Sicurezza nell'ambito della gestione del personale

La tutela delle informazioni è in gran parte affidata al personale che opera in azienda ed è pertanto necessario che l'intera organizzazione sia responsabilizzata sulle tematiche afferenti alla sicurezza delle informazioni, soprattutto per le mansioni che richiedono di gestire informazioni con livelli di classificazione elevati o relativi a dati personali. Il personale viene quindi adeguatamente formato in merito alle politiche, linee guida, misure di sicurezza comportamentali al fine di diffondere la cultura della protezione del patrimonio informativo aziendale e limitare i rischi inerenti il” fattore umano”.

Al fine di garantire una corretta conoscenza delle tematiche di sicurezza, in corrispondenza di ogni nuovo ingresso, il neo-assunto è chiamato a prendere visione della Policy di Sicurezza delle Informazioni e delle Norme Comportamentali per la gestione dei beni aziendali, definite da ASSOTHERM SRL, e di fornirne con apposita firma scritta o elettronica l’attestazione di avvenuta lettura e comprensione.

ASSOTHERM SRL si impegna a garantire la sicurezza delle informazioni durante tutto il ciclo di vita del rapporto di lavoro e, in particolare, nei seguenti momenti:

- Assunzione – i ruoli e le responsabilità di dipendenti, collaboratori, professionisti e terzi parti in materia di sicurezza delle informazioni vengono chiaramente identificati, sia all’atto della ricerca della nuova risorsa, sia all’atto dell’assunzione vera e propria.
- Durante il rapporto di lavoro – ASSOTHERM SRL richiede ai dipendenti, collaboratori, professionisti e alle terze parti che hanno autorizzazione ad accedere alle informazioni aziendali di applicare le opportune misure di sicurezza e le procedure a protezione del trasferimento delle informazioni attraverso tutte le tipologie di strutture di comunicazione, nel rispetto degli standard/istruzioni operative in vigore. Lo sviluppo delle competenze in materia di sicurezza delle informazioni viene garantito attraverso la previsione di un piano di formazione e mediante l’erogazione di sessioni formative (generali o specifiche) e di awareness, anche a seconda del ruolo edella mansione svolta, con cadenza annuale per il personale e trimestrale per il Top Management. La formazione viene erogata anche al personale esterno per specifiche esigenze (ad esempio, se il consulente offre un servizio continuativo).
- Cessazione del rapporto di lavoro – i dipendenti, i collaboratori, i professionisti e le terzi parti restituiscono tutti i beni di ASSOTHERM SRL in loro possesso al termine del rapporto di lavoro. Il diritto degli stessi di accedere alle e/o utilizzare le informazioni e gli strumenti adibiti al trattamento delle informazioni, è revocato alla cessazione del rapporto.

## 5.1. Gestione delle informazioni e degli asset

Le attività legate alla gestione delle informazioni e degli asset hanno come obiettivo l'applicazione delle regole e delle misure atte a garantire adeguati livelli di sicurezza sui dati e sulle strutture di elaborazione delle informazioni e prevenire i relativi rischi nell'ordinaria operatività aziendale:

- ASSOTHERM SRL definisce ed applica opportuni livelli di classificazione al fine di proteggere in modo efficace i sistemi aziendali e le informazioni stesse attraverso tutto il loro ciclo di vita. La classificazione delle informazioni prevede l'organizzazione dei documenti, in formato elettronico e cartaceo, secondo uno schema accettato e condiviso dall'organizzazione. Sulla base del livello di classificazione assegnato sono definite le misure di sicurezza da applicare. Il livello di classificazione assegnato alle informazioni viene monitorato periodicamente ed eventualmente rivisto in seguito a cambiamenti.
- Coerentemente con i livelli di classificazione delle informazioni definiti, viene applicata l'assegnazione di una specifica "etichetta" alle informazioni, in modo che tutti coloro che abbiano esigenza di gestire l'informazione siano consapevoli dello specifico livello di riservatezza ad essa assegnata.
- Il personale interno ed esterno è istruito affinché vengano applicati i seguenti principi chiave della sicurezza:
    - Clean Desk Policy;
    - Utilizzo dei dispositivi di sicurezza fisica per la protezione delle dotazioni informatiche relative alla postazione di lavoro, così come da dotazione aziendale (es. lucchetti per pc).
- Al fine di garantire e mantenere un livello adeguato di sicurezza, ASSOTHERM SRL censisce, monitora e controlla gli asset e le informazioni ad essi connesse, con l'obiettivo di applicarvi idonee misure Gestione delle informazioni e degli asset
- Le attività legate alla gestione delle informazioni e degli asset hanno come obiettivo l'applicazione delle regole e delle misure atte a garantire adeguati livelli di sicurezza sui dati e sulle strutture di elaborazione delle informazioni e prevenire i relativi rischi nell'ordinaria operatività aziendale:
- ASSOTHERM SRL definisce ed applica opportuni livelli di classificazione al fine di proteggere in modo efficace i sistemi aziendali e le informazioni stesse attraverso tutto il loro ciclo di vita. La classificazione delle informazioni prevede l'organizzazione dei documenti, in formato elettronico e cartaceo, secondo uno schema accettato e condiviso dall'organizzazione. Sulla base del livello di classificazione assegnato sono definite le misure di sicurezza da applicare. Il livello di classificazione assegnato alle informazioni viene monitorato periodicamente ed eventualmente rivisto in seguito a cambiamenti.
- Coerentemente con i livelli di classificazione delle informazioni definiti, viene applicata l'assegnazione di una specifica "etichetta" alle informazioni, in modo che tutti coloro che abbiano esigenza di gestire l'informazione siano consapevoli dello specifico livello di riservatezza ad essa assegnata.
- Il personale interno ed esterno è istruito affinché vengano applicati i seguenti principi chiave della sicurezza: o Clean Desk Policy;
    - Utilizzo dei dispositivi di sicurezza fisica per la protezione delle dotazioni informatiche relative alla postazione di lavoro, così come da dotazione aziendale (es. lucchetti per pc).
- Al fine di garantire e mantenere un livello adeguato di sicurezza, ASSOTHERM SRL censisce, monitora e controlla gli asset e le informazioni ad essi connesse, con l'obiettivo di applicarvi idonee misure.

### 5.1. Controllo degli accessi logici

L'organizzazione si impegna a identificare e attuare presidi di natura tecnica ed organizzativa per la gestione degli accessi logici ai sistemi aziendali con l'obiettivo di minimizzare il rischio di accesso illegittimo, modifica indesiderata o perdita dei dati:

- Il controllo degli accessi alle reti e ai sistemi avviene nel rispetto di un processo formale di autenticazione, opportunamente mantenuti aggiornati rispetto alla situazione organizzativa dell'azienda, in rispetto del principio di "Privilegio minimo" (rif. "least privilege") e di "Necessità di conoscere (rif. "Need to know") secondo il quale le informazioni sono condivise solamente con chi ha una legittima necessità di accedervi ed è esplicitamente autorizzato al loro accesso ed elaborazione.
- Tutti i sistemi, le apparecchiature e le applicazioni aziendali che consentono l'elaborazione delle informazioni o l'esecuzione di operazioni di business devono prevedere meccanismi per l'identificazione dell'utente.
- Esiste un processo formale per l'assegnazione dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi. Nel caso in cui l'utente venga assegnato a nuovi incarichi o termini il rapporto di collaborazione, il profilo utente ad esso assegnato e i relativi diritti sono immediatamente modificati o revocati secondo un processo formale. Vengono inoltre eseguite verifiche periodiche sugli utenti inattivi in modo da garantirne l'effettivo aggiornamento e/o rimozione.
- Sono definite formalmente le tipologie di account di sistema consentite e le condizioni di appartenenza a gruppi e ruoli.
- Sono documentate e implementate procedure che prevedono appropriati meccanismi di autenticazione e di controllo di accesso degli utenti alle reti aziendali (ivi compresi protocolli di "Multi Factor Authentication").
- Sono formalmente nominati e adeguatamente monitorate le utenze privilegiate (super-user) che accedono ai sistemi.
- Sia richiesto ai collaboratori in telelavoro di ri-autenticarsi periodicamente durante lunghe sessioni di lavoro (anche da remoto) nonché dopo alcuni minuti di inattività ("Away from keybord").
- ASSOTHERM SRL esegue costanti controlli affinché i privilegi associati ad un utente riflettano il minimo necessario per permettergli di operare nell'ambito dei relativi incarichi. I profili sono mantenuti aggiornati nel tempo e periodicamente riesaminati al fine di verificare la sussistenza delle condizioni iniziali di assegnazione. Ogni modifica che si renda necessaria deve essere formalmente autorizzata.
- Sono definite regole e controlli affinché le password e i fattori di autenticazione consentano di ridurre al minimo le possibilità di compromissione.

### 5.1. Sicurezza fisica

Al fine di contrastare il manifestarsi di accessi fisici non autorizzati, che potrebbero condurre a potenziali minacce alla salvaguardia degli asset e delle informazioni o comportare interferenze con l'operatività aziendale, ASSOTHERM SRL adotta misure per garantire l'accesso controllato del personale e dei visitatori e il blocco degli accessi non autorizzati, oltre alle misure volte a proteggere gli uffici, i Data Center esternalizzati, le aree sensibili e le attrezzature da possibili incidenti fisici o calamità naturali:

- ASSOTHERM SRL progetta e realizza apposite misure di controllo perimetrale, verificando che non vi siano varchi non adeguatamente protetti che possano permettere un accesso incontrollato al perimetro dell'azienda, ai locali e alle aree sicure. Sono predisposti e gestiti opportuni strumenti che

consentano la puntuale e tempestiva individuazione di accessi non autorizzati, laddove dovessero fallire le misure di controllo degli accessi stessi.

Sono identificate le aree sicure e le altre aree che per criticità operativa devono essere subordinate a controlli maggiormente restrittivi e sono applicate ulteriori misure per la registrazione e il controllo degli accessi, consentendo l'ingresso al solo personale autorizzato. L'accesso fisico alle risorse ICT è formalmente autorizzato in base ai compiti e alle responsabilità individuali e limitata alle persone adeguatamente formate e monitorate. Inoltre, le autorizzazioni sono periodicamente revisionate per garantire che i diritti di accesso non più necessari siano revocati tempestivamente quando non richiesti.

- Sono predisposte opportune misure affinché la collocazione delle apparecchiature di elaborazione delle informazioni sia tale da offrire un adeguato livello di protezione da minacce intenzionali, incidentali e ambientali, anche per quanto concerne la disposizione dei cablaggi e dei collegamenti a reti di telecomunicazione o alimentazione delle stesse.
- Per le apparecchiature elettroniche a supporto delle attività operative, o adibite all'elaborazione delle informazioni, sono assicurate costantemente condizioni ambientali idonee (in termini di temperatura, umidità e assenza di fattori di disturbo) volte ad assicurarne la piena operatività e salvaguardia. Le misure di sicurezza a protezione dai rischi ambientali sono inoltre commisurate all'importanza degli edifici e alla criticità delle operazioni o dei sistemi ICT situati al loro interno.
- Sono adottate adeguate misure per la gestione della manutenzione di tutte le apparecchiature di trattamento delle informazioni, al fine di assicurarne la continua disponibilità e integrità.

## 5.1. Gestione del sistema informativo

L'attività di gestione dei sistemi informativi aziendali è costituita da un insieme eterogeneo di attività, processi e strumenti che mirano a raggiungere un adeguato livello di sicurezza delle informazioni e che interessano nello specifico le reti, l'infrastruttura di supporto e i sistemi applicativi di ASSOTHERM SRL:

- Sono previsti procedure e controlli al fine di prevenire e individuare la presenza di malware nei sistemi informativi e reagire in caso di infezione. Le soluzioni anti-malware sono mantenute costantemente aggiornate in modo da seguire l'evoluzione della minaccia.
- ASSOTHERM SRL definisce e predispone un modello per il salvataggio periodico delle informazioni, al fine di assicurare che possano essere ripristinate secondo i requisiti temporali e i metodi definiti. Vengono inoltre effettuate e documentate prove periodiche di ripristino dei backup, in modo da garantirne la perdurante efficacia.
- Le soluzioni di backup sono collocate a una distanza ragionevole dai sistemi principali, al fine di eludere qualsiasi danno eventualmente causato da compromissioni al sistema principale.
- Al fine di intercettare tempestivamente le potenziali vulnerabilità tecniche sui sistemi aziendali, ASSOTHERM SRL definisce un processo di gestione delle vulnerabilità con l'obiettivo di mitigare proattivamente eventuali minacce che possono influenzare la protezione del patrimonio informativo in termini di riservatezza, integrità e disponibilità. Sono periodicamente condotte attività di test e verifica (VA-PT, social engineering, secure code review, ecc.) volte alla rilevazione delle vulnerabilità dei sistemi aziendali (tra le quali possono essere eventualmente previste attività di "Red Team") e la conseguente identificazione di eventuali azioni correttive.
- ASSOTHERM SRL provvede ad autorizzare, controllare e registrare tutte le modifiche della configurazione apportate a sistemi, apparecchiature ed applicazioni. Il processo di gestione delle modifiche prevede che esse siano organizzate tenendo conto delle misure di sicurezza necessarie, delle modalità di verifica e accettazione e dei tempi di rilascio per il passaggio dai sistemi di test ai sistemi di produzione.

- 
- apportate a sistemi, apparecchiature ed applicazioni. Il processo di gestione delle modifiche prevede che esse siano organizzate tenendo conto delle misure di sicurezza necessarie, delle modalità di verifica e accettazione e dei tempi di rilascio per il passaggio dai sistemi di test ai sistemi di produzione.
- ASSOTHERM SRL provvede affinché l'installazione delle patch di sicurezza, messe a disposizione periodicamente dai fornitori, avvenga con tempistiche tali da garantire un'esposizione minima per i sistemi, le apparecchiature e le applicazioni, al fine di contrastare possibili disservizi e minacce esterne.
- • ASSOTHERM SRL definisce attività e metodi affinché tutte le operazioni effettuate sugli apparati e che potrebbero avere conseguenze sulla sicurezza delle informazioni, siano tracciabili e ricostruibili.
- • L'organizzazione adotta inoltre, ove tecnicamente possibile, soluzioni adeguate affinché gli apparati producano registrazioni di tutti gli eventi significativi per la sicurezza delle informazioni, funzionali alla pronta individuazione o alla ricostruzione successiva di incidenti. Dove possibile, sono predisposti allarmi per segnalare la necessità di attenzione o d'intervento al personale interessato. Queste informazioni sono altresì conservate e protette dalla modifica non autorizzata e dalla perdita accidentale, anche secondo le specifiche richieste della normativa vigente.
- • ASSOTHERM SRL mantiene la continua e precisa sincronizzazione di data e ora dei sistemi, alfine di garantire l'usabilità congiunta di registrazioni diverse, e quindi la correlazione dei singoli eventi.
- • ASSOTHERM SRL prevede l'impiego delle tecniche di crittografia al fine di migliorare il livello di protezione del patrimonio informativo e stabilisce i criteri e le modalità di adozione rispetto a tuttigli ambiti applicabili (reti, apparecchiature e sistemi informativi). Vengono pertanto identificate, documentate e applicate tecniche crittografiche ove tecnicamente possibile e ove richiesto dalla normativa vigente, anche tenendo in considerazione il modello di classificazione delle informazioni.
- 

### 5.1. Gestione delle reti di telecomunicazione

Allo scopo di assicurare la protezione dei flussi informativi, ASSOTHERM SRL definisce e documenta i presidi tecnico-organizzativi per la gestione della sicurezza delle reti, dei dispositivi e delle strutture per l'elaborazione delle informazioni, in particolare salvaguardando i seguenti aspetti:

- Gestione delle comunicazioni e dell'operatività – le reti vengono adeguatamente gestite, testate e monitorate, al fine di essere protette dalle minacce e mantenerne la sicurezza dei sistemi e delle applicazioni connesse.
- Segregazione delle reti – sono identificati gruppi di servizi, utenti e sistemi informativi secondo la tipologia di informazioni trattate e in base al loro rischio intrinseco, allo scopo di progettare e implementare una corretta segregazione delle reti.
- Accesso da remoto alla rete aziendale – sono predisposti procedure operative e strumenti tecnologici affinché la connessione da remoto alla rete aziendale avvenga in rispetto dei requisiti di sicurezza definiti, solo per un periodo di tempo limitato a quanto necessario e previa specifica autorizzazione (per linee guida di dettaglio si rimanda al paragrafo 5.13).

### 5.1. Acquisizione, sviluppo e manutenzione dei sistemi informativi

ASSOTHERM SRL salvaguarda la sicurezza delle informazioni nell'intero ciclo di vita dei sistemi aziendali, considerandola sin dalla fase di progettazione al fine di minimizzare le vulnerabilità legate allo sviluppo dei sistemi.

- Le attività di acquisizione, sviluppo e manutenzione dei sistemi devono pertanto essere condotte garantendo l'identificazione, la documentazione e la successiva applicazione dei requisiti di sicurezza a protezione delle informazioni trattate e in ottemperanza dei requisiti normativi e delle best practices applicabili.
- ASSOTHERM SRL definisce ruoli, responsabilità e regole nell'ambito del processo di sviluppo del software, dotandosi di un processo di SSDLC (Secure Software Development Life Cycle) oltre che organizzando un più ampio processo di Security by Design finalizzato alla definizione e implementazione di adeguate misure di sicurezza all'avvio di iniziative progettuali o a fronte di modifiche sostanziali.

## 5.1. Sicurezza nella gestione delle terze parti

Le attività di trattamento delegate a terze parti, outsourcer o fornitori aventi o meno accesso fisico alla struttura dell'azienda, costituiscono rilevanti fattori di rischio per la sicurezza delle informazioni. ASSOTHERM SRL garantisce pertanto l'applicazione dei presidi di sicurezza del patrimonio informativo nell'ambito del rapporto con terze parti, nel rispetto delle normative applicabili:

- I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso dei fornitori alle risorse di ASSOTHERM SRL devono essere concordati con la terza parte e opportunamente documentati. Gli accordi con i fornitori includono requisiti per affrontare i rischi e gli incidenti relativi alla sicurezza delle informazioni.
- ASSOTHERM SRL adotta quindi opportune misure organizzative e tecniche per amministrare l'accesso dei fornitori alle risorse di elaborazione delle informazioni, attraverso l'uso di controlli che devono essere identificati e applicati.
- ASSOTHERM SRL controlla, esamina e verifica regolarmente il servizio del fornitore, anche mediante la conduzione di audit periodici sui servizi erogati. Le modifiche ai servizi offerti dai fornitori devono essere gestiti tenendo in considerazione le criticità delle informazioni aziendali, dei sistemi e dei processi coinvolti, se opportuno rivalutandone i rischi.

## 5.1. Gestione degli incidenti di sicurezza

La tempestiva rilevazione e gestione di eventuali incidenti di sicurezza è di fondamentale importanza per la protezione del patrimonio informativo di ASSOTHERM SRL, al fine di raggiungere l'obiettivo di ripristinare un livello di sicurezza tollerabile durante una situazione avversa e agevolare il conseguente avvio del processo di rimedio:

- L'azienda stabilisce una procedura e attribuisce specifici ruoli e responsabilità nell'ambito del processo di gestione degli incidenti di sicurezza, al fine di mitigare gli impatti derivanti dalla perdita di riservatezza, integrità e disponibilità delle informazioni.
- Il personale è istruito e messo nella condizione di poter riferire tempestivamente i casi o i sospetti di criticità relativi alla sicurezza degli asset e delle informazioni, anche mediante appositi canali. A valle della segnalazione, gli eventi relativi alla sicurezza delle informazioni vengono valutati al fine di stabilire se debbano essere classificati come incidenti e che impatto possano aver prodotto.
- Sono stabiliti e mantenuti i contatti con le autorità rilevanti in materia di sicurezza delle informazioni (ad esempio Autorità Governative, Forze dell'Ordine, centri specialistici, ecc.), al fine di poter prevenire e reagire tempestivamente agli incidenti rilevanti.

## 5.1. Aspetti di sicurezza nella gestione della continuità operativa

ASSOTHERM SRL individua, analizza, definisce e mantiene periodicamente un modello di gestione della continuità operativa con l'obiettivo di aumentare la resilienza organizzativa e la capacità di rispostaa un incidente o un evento critico a prescindere dalla causa generante. Tale modello si esplica sia nella gestione ordinaria in normale operatività che nella gestione straordinaria in emergenze o crisi:

- ASSOTHERM SRL si impegna a definire, implementare, gestire e mantenere attività e iniziative volte a garantire la continuità operativa ordinaria dei servizi e dei processi critici per l'organizzazione. In particolar modo:
    - identifica e valuta i processi critici tramite l'esecuzione delle attività di Business Impact Analysis (BIA) e Risk Assessment;
    - definisce la strategia di Business Continuity e identificazione delle risorse a supporto del sistema di gestione della continuità operativa;
    - implementa i controlli e le misure necessarie per assicurare la continuità dei processi critici e dei relativi asset;
    - garantisce che le strutture per l'elaborazione delle informazioni siano realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità;
    - gestisce le terze parti al fine di assicurare che le stesse garantiscano il rispetto dei requisiti di continuità operativa;
    - pianifica ed eroga sessioni di formazione e awareness volte a sensibilizzare e istruire la popolazione aziendale su tematiche di business continuity;
    - pianifica ed esegue attività di test periodiche del sistema di gestione della continuità operativa a garanzia delle effettive capacità di gestione delle situazioni anomale;
    - migliora in modo continuativo il sistema di continuità operativa tramite l'ausilio di KPI volti a monitorare il sistema e l'esecuzione di attività di follow-up a seguito di eventuali incidenti occorsi.
- Il processo di gestione delle emergenze e della crisi ha l'obiettivo di supportare le funzioni organizzative di ASSOTHERM SRL coinvolte in una situazione di crisi, con impatti sui processi critici, nella conduzione delle attività di gestione della crisi stessa.

## 5.1. Conformità

ASSOTHERM SRL si adopera per garantire l'osservanza delle disposizioni normative rilevanti ai fini del presente documento, attraverso il controllo e monitoraggio continuo dei livelli di adeguamento ai requisiti di legge e alla normativa interna all'organizzazione:

- Le misure relative alla sicurezza delle informazioni sono pertanto progettate in conformità con i requisiti legali, normativi e alle politiche, le procedure, i regolamenti vigenti e inerenti alle attività dell'organizzazione.
- La gestione della sicurezza delle informazioni viene svolta in modo conforme, oltre che ai requisiti legali, anche agli adempimenti di natura contrattuale.

## 5.1. Misure di sicurezza per lo Smartworking e per l'utilizzo di dispositivi non aziendali (BYOD)

Al fine di garantire la sicurezza informatica in relazione alla modalità di lavoro in Smart Working e l'eventuale utilizzo di dispositivi personali dei dipendenti, è necessario che:

- sia effettuato un Risk Assessment mirato sulla selezione delle metodologie di accesso remoto (es. tunneling, application portals, remote desktop access, direct application access) e condotta una valutazione del rischio, inclusa la probabilità e l'entità di eventuali danni in relazione a:
    - accesso, uso, divulgazione, interruzione, modifica o distruzione non autorizzati del sistema, delle informazioni che elabora, memorizza o trasmette e di qualsiasi informazione correlata;

    - problemi relativi alla Privacy per i soggetti interessati derivanti dal trattamento intenzionale di informazioni.
- sia presente documentazione relativa ai requisiti di accesso remoto.
- sia fornita l'autorizzazione dell'accesso remoto prima di consentire le connessioni.
- sia utilizzato un protocollo di "Mutual authentication", ove possibile, per verificare la legittimità di un Server di accesso remoto prima di fornire le credenziali di autenticazione dell'utente.
- siano previste misure di crittografia all'avanguardia per le connessioni di accesso remoto.
- siano definiti adeguatamente i requisiti di accesso ai dispositivi mobili e le autorizzazioni per connettere i dispositivi mobili ai sistemi dell'organizzazione.
- sia proibito l'utilizzo di sistemi informativi esterni, come dispositivi client personali (BYOD) e dispositivi client controllati da terze parti, che possono elaborare, archiviare o trasmettere dati controllati dall'organizzazione, ivi comprese misure sanzionatorie ad hoc in caso di mancato rispetto delle linee guida da parte dei dipendenti.
- sia implementata una segmentazione/segregazione della rete (ad es. l'utilizzo di sottoreti) per mantenere i componenti accessibili pubblicamente e/o da remoto fuori dalle reti interne che ospitano i sistemi critici.
- siano implementati adeguati presidi per il monitoraggio e il controllo delle comunicazioni nei punti chiave del perimetro.
- siano implementate adeguate misure di sicurezza logica (PIN, password, antivirus, firewall, cifratura) dei dispositivi mobili aziendali a protezione dei dati (laptop, smartphone, tablet, altro).

## 6. Responsabile della Policy e suo aggiornamento

Il Responsabile della Policy e del suo aggiornamento, con i relativi compiti di coordinamento con le funzioni coinvolte, è la Funzione Information Security & IT Compliance.

## 7. Rispetto della Policy

È responsabilità di tutto il personale (dipendenti, collaboratori, interinali, stagisti) assicurare il rispetto delle linee guida e politiche di cui al presente documento in ogni attività.