Politica per la sicurezza delle informazioni ISO/IEC 27001:2022

Primeur Group

Versione 2.0

Approvato dal Managing Director di Primeur Suisse SA

• 2a Edizione Dicembre 2024

Le società del Gruppo Primeur (soggette alla direzione ed al coordinamento di Topicus.com Cooperatief U.A.-NL., di seguito anche solo "PRIMEUR") offrono piattaforme e soluzioni di *data integration* ai propri clienti e, pertanto, l'obiettivo della sicurezza delle informazioni risulta primario. Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni che l'azienda ha fatto propri al fine di realizzare e mantenere un efficiente Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

La sicurezza delle informazioni ha come obiettivo primario la promozione di una cultura aziendale che tuteli la protezione dei dati (digitali e analogici), dei processi aziendali, delle procedure e delle *policies* e, in generale, di tutte le relative componenti dell'organizzazione.

In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere i seguenti obiettivi:

- **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;

La mancanza di adeguati livelli di sicurezza può comportare, nell'ambito di una qualsiasi attività aziendale, conseguenze sia in termini di responsabilità del personale (violazione delle normative aziendali), sia dal punto di vista aziendale (rischio di danni di natura economico/finanziaria, di mancata soddisfazione del cliente, di danneggiamento dell'immagine aziendale nonché di incorrere in rilevanti sanzioni legate alla violazione delle normative vigenti).

L'adozione di adeguati livelli di sicurezza delle informazioni è, quindi, un requisito fondamentale per garantire l'affidabilità delle informazioni trattate, nonché l'efficacia ed efficienza dei servizi erogati da PRIMEUR; di conseguenza, è essenziale identificare le esigenze di sicurezza attraverso le seguenti attività:

- analisi e trattamento dei rischi, che consentono all'azienda di acquisire la consapevolezza e la visibilità sul livello di esposizione al rischio della propria organizzazione;
- applicazione di relative *policies* e procedure interne;
- applicazione della normativa cogente, volontaria e delle clausole contrattuali in tema di sicurezza delle informazioni.

PERIMETRO ORGANIZZATIVO

La presente Politica, approvata dal Managing Director di Primeur Suisse SA, holding di Gruppo Primeur (soggetta alla direzione ed al coordinamento di Topicus.com Cooperatief U.A.-NL.), si rivolge a tutto il personale dipendente ed ai collaboratori di PRIMEUR, nonché a tutte le parti interessate esterne coinvolte nella gestione delle informazioni trattate dalle società del Gruppo.

IDENTIFICAZIONE, CLASSIFICAZIONE E GESTIONE DEGLI ASSET

Al fine di garantire la piena conoscenza delle informazioni gestite in PRIMEUR e la valutazione della loro criticità e al fine di agevolare l'implementazione di adeguati livelli di protezione, PRIMEUR si impegna a:

- censire ed aggiornare periodicamente un elenco di tutti i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
- associare ad un ben preciso responsabile ogni risorsa (bene materiale/immateriale);
- classificare le informazioni in base al loro livello di criticità, in modo da gestirle con livelli di riservatezza ed integrità coerenti ed appropriati. La criticità delle informazioni deve essere valutata in maniera quanto più oggettiva possibile, attraverso l'utilizzo di adeguate metodologie di lavoro;
- definire modalità di gestione e sistemi di protezione per le informazioni e gli *asset* su cui risiedono, coerenti con il livello di criticità identificato.

GESTIONE SICURA DEGLI ACCESSI

In ossequio al "principio dei privilegi minimi" *(o "Least privilege"* o, ancora *"Zero trust security model":* a un'entità dovrebbero essere concessi solo i privilegi di cui ha bisogno per portare a termine il suo lavoro*),* al fine di garantire maggiore resilienza in ambito di sicurezza e accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti, occorre agire conformemente ai seguenti punti:

- L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti. La comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.
- L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato all'autorizzazione e successivamente al superamento di una procedura di identificazione ed autenticazione degli stessi.
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione e gestite attraverso credenziali univoche;
- I sistemi e servizi utilizzati da PRIMEUR devono essere opportunamente protetti, segregati e periodicamente verificati, in modo da minimizzare la possibilità di accessi non autorizzati.

NORME COMPORTAMENTALI PER LA GESTIONE SICURA DELLE RISORSE AZIENDALI

Al fine di garantire che i dipendenti e collaboratori di PRIMEUR adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni:

- gli ambienti di lavoro e le risorse aziendali devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate;
- vengono definite opportune procedure per la gestione ed utilizzo delle informazioni, sia su supporto digitale che su supporto cartaceo;
- i sistemi ed i servizi utilizzati devono essere impiegati da dipendenti e dai collaboratori secondo procedure condivise e approvate.

PERSONALE E SICUREZZA

Al fine di garantire che il personale che opera per conto di PRIMEUR (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni:

- durante la permanenza in PRIMEUR il personale deve ricevere un'adeguata e periodica formazione inerente le tematiche di sicurezza dei dati;
- il *management* deve garantire e verificare che il personale abbia le conoscenze pertinenti in materia di sicurezza delle informazioni e dei sistemi che sviluppano o mantengono. Il personale coinvolto nel ciclo di vita dello sviluppo dei sistemi informativi deve essere consapevole delle proprie responsabilità in materia di sicurezza dei sistemi e delle informazioni.
- nelle fasi di selezione ed inserimento del personale in PRIMEUR devono essere valutati quali siano i livelli di conoscenza delle problematiche di sicurezza aziendale in funzione delle attività che dovranno essere svolte;
- in apposita procedura devono essere previste le misure di sicurezza attinenti telelavoro/lavoro agile/da remoto e utilizzo di dispositivi portatili e quelle relative all'ottimizzazione dell'area di lavoro;
- le modalità di chiusura del rapporto di lavoro con PRIMEUR dovranno essere coerenti con gli obiettivi di sicurezza aziendale.

GESTIONE DEGLI EVENTI ANOMALI E DEGLI INCIDENTI

Al fine di garantire che le anomalie e gli incidenti che potrebbero avere ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business, occorre che:

- tutti i dipendenti e i collaboratori siano tenuti a rilevare e notificare, secondo le procedure, eventuali problematiche legate alla sicurezza delle informazioni;
- gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure, coinvolgendo anche i fornitori esterni e terze parti.

GESTIONE DELLA SICUREZZA FISICA

Al fine di prevenire l'accesso non autorizzato alle sedi ed ai singoli locali aziendali e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni:

- deve essere garantita la gestione della sicurezza delle aree e dei locali tramite la definizione dei livelli adeguati di protezione.
- deve essere garantita la sicurezza delle apparecchiature tramite:
    - la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;
    - la messa a disposizione delle risorse necessarie al loro funzionamento;
    - la predisposizione di un adeguato livello di manutenzione.

ASPETTI CONTRATTUALI CONNESSI ALLA SICUREZZA DELLE INFORMAZIONI

Al fine di assicurare la conformità dei contratti con le terze parti ai requisiti legali ed ai principi legati alla sicurezza delle informazioni, in accordo con le caratteristiche specifiche della relazione che PRIMEUR deve instaurare con le terze parti stesse:

- gli accordi con le terze parti (clienti e fornitori) che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza che sono stati valutati come appropriati;
- gli accordi con terze parti, ove necessario, devono garantire il rispetto dei requisiti di legge in generale e, specificatamente, in materia di protezione dei dati personali.

GESTIONE DELLA BUSINESS CONTINUITY

Al fine di garantire la continuità dell'attività di PRIMEUR e l'eventuale ripristino tempestivo dei servizi erogati che possano essere colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto aziendale:

- devono essere attentamente identificati e valutati, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business;

- devono essere definite le tempistiche delle attività di ripristino ed i relativi costi e le modalità più idonee a permettere all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto, in modo tale da consentire la riduzione delle conseguenze negative sull'azienda.

MONITORAGGIO, TRACCIAMENTO E VERIFICHE TECNICHE

Al fine di garantire la rilevazione tempestiva di eventi anomali, incidenti e vulnerabilità dei sistemi informativi, in modo da poter assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni:

- i sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, *hardware* e *software*, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato;
- a fronte dei risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative;
- devono essere pianificate attività periodiche di *audit* del sistema di gestione della sicurezza delle informazioni.

CICLO DI VITA DEI SISTEMI E DEI SERVIZI

Al fine di assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi dell'organizzazione:

- i requisiti di garanzia e di sicurezza devono essere rispettati all'inizio di ogni progetto di sviluppo, per garantire che siano efficaci e che non vi siano ripercussioni negative sul progetto o sul prodotto;
- i requisiti di sicurezza non sono in nessun caso considerati separatamente dai requisiti funzionali dei sistemi. Per considerare in modo efficace la sicurezza, occorre pianificarla fin dall'inizio del processo di sviluppo e/o manutenzione per garantire che sia inserita nel contesto del sistema.
- nella fase di progettazione e sviluppo devono essere gestite le seguenti tematiche:

- inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e sistemi;
- adozione di *best practices* e *standards* riconosciuti per lo sviluppo e la manutenzione del *software*;
- gestione controllata della documentazione;
- separazione degli ambienti di sviluppo e test.

- nella fase di erogazione del servizio devono essere gestite le seguenti tematiche:
  - *capacity management* dell'infrastruttura tecnologica;
  - miglioramento della sicurezza dei sistemi e dei dati (*configuration management*, installazione di sistemi *anti-malware*);
  - gestione dei cambiamenti;
  - adozione di procedure di *backup* e *restore*;
  - adozione di procedure di dismissione controllata dei sistemi;
  - monitoraggio dei sistemi e servizi;
  - gestione utenze;
  - *performance monitoring*.

RISPETTO DELLA NORMATIVA APPLICABILE

Al fine di garantire il rispetto della normativa vigente degli obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali:

- tutti i requisiti normativi e contrattuali in materia di sicurezza dell'organizzazione e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi;
- i responsabili delle diverse aree devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati, rispettati e verificati;
- il mancato rispetto di quanto indicato in questo documento, e in tutti gli altri che da esso discendono, sarà gestito in ottemperanza a quanto previsto nel CCNL oppure, nel caso di inadempienze di terze parti, secondo i rapporti contrattuali in essere.

TEAM RESPONSABILE DELLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il Team responsabile del Sistema di Gestione della Sicurezza delle Informazioni, supportato dal *management*, dovrà farsi promotore, al fine di rendere la presente Politica generale di sicurezza coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo e legislativo in materia di sicurezza delle informazioni;
- risultati di analisi sui costi, impatti, efficacia ed efficienza del Sistema di Gestione per la Sicurezza delle Informazioni.

Mendrisio, 23 Dicembre 2024