Nell'ambito dell'implementazione del proprio sistema di gestione della sicurezza delle informazioni, conforme alla norma **UNI CEI ISO/IEC 27001** ed in considerazione dell'importanza strategica che lo stesso riveste per il business dell'Azienda, come Direzione di RIMSA, abbiamo adottato una politica di sicurezza adeguata.

Siamo consapevoli che la gestione della sicurezza delle informazioni è un processo culturale complesso che coinvolge le risorse umane assegnate a tutte le unità organizzative all'interno del perimetro di certificazione.

Crediamo che la sicurezza delle informazioni, sia la risultante di un insieme di elementi scientifici, tecnologici, organizzativi, procedurali, relazionali e di comunicazione, in cui un ruolo determinante è svolto dalle variabili umane che interagiscono fortemente nei processi produttivi e che si traduce in un impegno costante verso la centralità dell'utenza e il miglioramento dei propri servizi.

I principi sui quali basiamo il nostro sistema di Sicurezza delle Informazioni sono:

- **INFORMATION SECURITY BY DESIGN**
  Intesa come modo di operare di default all'interno della nostra Organizzazione. I principi Information Security by Design sono applicati a tutti i tipi di informazioni, e si riassumono in:
  - Proattività non reattività (prevenire non correggere): anticipare e prevenire gli eventi che possano provocare un danno alle informazioni prima che essi accadano.
  - Information Security incorporata nella progettazione: componente essenziale per la realizzazione del nucleo funzionale del nostro sistema di trattamento e protezione dei dati.
  - Massima funzionalità: conciliare tutti gli interessi legittimi e gli obiettivi comuni con modalità di valore positivo "vantaggioso per tutti".
  - Sicurezza: estensione del sistema per l'intero ciclo vitale delle informazioni per assicurare che le stesse siano conservate con cura e poi distrutte in modo sicuro alla fine del processo.
  - Visibilità e trasparenza: informazioni ed obiettivi stabiliti, soggetti a verifica indipendente.
  - Rispetto per le informazioni dei clienti: considerare prioritari gli interessi dei clienti offrendo efficaci interventi di default della information security, informazioni appropriate, riservate, integre e disponibili.
  - Utilizzare, se necessario, servizi Cloud certificati che garantiscano alla nostra organizzazione e ai nostri clienti/committenti non solo la sicurezza delle informazioni, ma anche la protezione dei dati ivi contenuti.

- **INFORMATION SECURITY BY DEFAULT**
  Information Security come impostazione di default: realizzare il massimo livello di protezione delle informazioni assicurando che siano automaticamente garantiti, in un qualunque sistema la Riservatezza, l'Integrità e la Disponibilità.
  RIMSA, mette in pratica meccanismi per garantire che:
  - non siano rese accessibili informazioni a un numero indefinito di persone, ad esclusione delle informazioni di carattere pubblico.
  - siano mappati i supporti (software, hardware, digitali e non) che contengo informazioni, ivi inclusi gli eventuali servizi Cloud.
  - siano attuate politiche di ridondanza delle informazioni atte a garantirne sempre la disponibilità.
  - siano identificate le risorse che possono accedere alle informazioni, come da disposizioni in materia di protezione dei dati personali in accordo con la legislazione vigente.
  - Geograficamente i dati saranno conservati nel rispetto del GDPR, sul territorio italiano o nell'ambito comunitario.

- **INFORMATION SECURITY**
  Inteso come protezione delle informazioni da:
  - forze "distruttive",
  - azioni indesiderate di utenti non autorizzati,
  - modifiche accidentali o fraudolente.

Ed è proprio attraverso la costante applicazione di questi principi che vogliamo perseguire i nostri obiettivi e quindi è per noi imprescindibile:

- Garantire la soddisfazione e la tranquillità dei nostri soci e clienti poiché hanno la consapevolezza che per noi il rispetto e la sicurezza delle loro informazioni e dei loro dati è un elemento indispensabile a prescindere dalle logiche di mercato;
- Garantire una protezione dell'informazione adeguata in termini di confidenzialità, integrità e disponibilità;
- Proteggere l'interesse dei clienti, dei dipendenti e delle terze parti;
- Assicurare la conformità alle leggi e ai regolamenti applicabili in materia di trattamento e protezione dell'informazione e dei dati personali in accordo alla legislazione vigente;
- Garantire al personale ed ai collaboratori una adeguata conoscenza e grado di consapevolezza dei problemi connessi con la sicurezza dell'informazione, al fine di acquisire sufficiente coscienza delle loro responsabilità in merito al suo trattamento;
- Accertare che tutti i fornitori esterni abbiano consapevolezza dei problemi di sicurezza delle informazioni e rispettino la politica di sicurezza adottata, ivi inclusi i fornitori di servizi cloud che devono garantire sicurezza, integrità e disponibilità delle informazioni e dei dati personali archiviati sui loro server;
- Stabilire regole precise per l'applicazione di standard, procedure e sistemi per realizzare L'Information Security Management System (ISMS) ed essere quindi pronti a rispondere alle costanti nuove sfide e minacce che il mondo cibernetico ci propone;
- adottare lo standard ISO 27002 – "Information Technology -- Security Techniques -- Code of Practice for Information Security Controls", come standard per l'implementazione del sistema di gestione della sicurezza dell'informazione e perseguire la conformità;
- garantire che tutto il personale abbia consapevolezza delle regole tecniche ed organizzative nell'utilizzo dei sistemi informativi aziendali descritte nelle procedure del sistema di gestione;
- garantire che tutto il personale sia informato della responsabilità nella gestione delle informazioni;
- Utilizzare risorse e tecnologie adeguate, che garantiscano il risultato delle prestazioni;
- Garantire le condizioni di sicurezza in ogni tipologia di attività o fase di trattamento dei dati personali e sensibili:
  - **Riservatezza:** le informazioni devono essere accessibili solo a coloro che sono autorizzati ad accedervi.
  - **Integrità:** le informazioni devono essere accurate e complete, e le modifiche alle informazioni devono essere autorizzate e tracciabili.
  - **Disponibilità:** le informazioni devono essere disponibili agli utenti autorizzati quando necessario.

Per realizzare tali obiettivi ed intenti, **RIMSA** si impegna:

- a sviluppare, mantenere, controllare e migliorare in modo costante l'Information Security Management System (nel seguito indicato come ISMS), in conformità alla norma ISO/IEC 27001 in grado di soddisfare i requisiti dichiarati e migliorare in continuo l'efficacia, l'affidabilità e la disponibilità dei servizi IT erogati e dei processi primari e accessori.
- alla redazione, aggiornamento e controllo di piani di sviluppo affinché le infrastrutture ed i servizi IT siano di supporto alle attività di business, adottando opportune politiche di sicurezza.

- alla conservazione sicura delle informazioni gestite, ivi comprese le informazioni dei nostri clienti / committenti.
- all'adeguata definizione del contenuto tecnico dei servizi forniti (specifiche di servizio) che trova riscontro in una serie di riferimenti normativi specialistici fra i quali protocolli informatici e documentazione tecnico-scientifica.
- alla qualificazione e competenza del personale addetto.
- alla corretta esecuzione delle attività di indagine, analisi (anche sperimentale) progettazione e assistenza, presupposti essenziali per la validità dei servizi erogati, assicurata dalla competenza e affidabilità del personale, secondo protocolli validati e riconosciuti e, in subordine, alla conformità del sistema alla norma ISO/IEC 27001.
- a fornire un quadro strutturale per stabilire e riesaminare gli obiettivi per la sicurezza delle informazioni.
- a diffondere i principi ed i valori dichiarati nella politica aziendale dall'organizzazione e a rendere attiva ed efficace la comunicazione da e verso le diverse parti interessate affinché sia compresa e partecipata.
- all'osservanza di norme e leggi che regolamentano i servizi ed il trattamento dei relativi dati e mantenere sotto controllo la sicurezza del complesso delle registrazioni e delle informazioni gestite.
- a riesaminare periodicamente la propria politica ed obiettivi ogni qual volta ve ne sia l'esigenza, a seguito dell'attuazione di modifiche che la influenzano, per accertarne la continua idoneità e rendere effettivo il proprio impegno al miglioramento continuo.
- a diffondere i principi ed i valori dichiarati nella politica aziendale dall'organizzazione e a rendere attiva ed efficace la comunicazione da e verso le diverse parti interessate affinché sia compresa e partecipata.
- ad effettuare formazione in ambito della sicurezza delle informazioni e privacy per tutto il personale.

La Direzione
RIMSA P. LONGONI SRL