POLITICA DI SECURITY

RINA considera la sicurezza delle persone e dei beni aziendali una priorità.

Secondo quanto enunciato nel Codice Etico ed in linea con il principio internazionalmente riconosciuto del dovere di protezione, il Gruppo RINA si impegna a dare alle persone una prospettiva di stabilità e sicurezza. Le attività di security sono finalizzate a garantire la protezione delle persone presenti in siti aziendali e dei beni dell'azienda da minacce derivanti da comportamenti avversi di terzi che potrebbero provocare danni, diretti o indiretti, alle persone, ai beni ed alla reputazione di RINA.

RINA adotta un modello di security atto a garantire la riduzione del rischio e un'efficiente gestione delle crisi. Ciò attraverso le soluzioni ritenute idonee a minimizzare l'impatto e la probabilità che si verifichino eventi negativi.

In linea con i suddetti principi, l'obiettivo di proteggere il personale, i beni, le informazioni e la reputazione del Gruppo da potenziali minacce di security, si realizza attraverso le seguenti attività:

i. La valutazione dei rischi di security associati agli asset, ai progetti ed alle attività aziendali, sulla base di metodologie di valutazione del rischio riconosciute, al fine di adottare idonee misure di mitigazione;

ii. La gestione della sicurezza delle persone e dei beni aziendali, nel rispetto delle norme internazionali e nazionali applicabili e dei più alti standard di riferimento, tra cui la Dichiarazione sui Diritti Umani ed i "Principi Volontari sulla Sicurezza ed i Diritti Umani";

iii. L'adozione di un programma di gestione del rischio di viaggio, che includa la valutazione dei rischi di security delle trasferte ed i criteri per l'adozione di protocolli di security atti a minimizzarli;

iv. La gestione delle crisi, in modo da assicurare una costante e coerente risposta nel caso di eventuali emergenze o situazioni di crisi di security, e garantire la continuità operativa;

i. La sicurezza delle informazioni, per evitare l'uso improprio di informazioni, sia fisiche sia digitali, relative al personale, a terze parti ed alle attività aziendali, come specificato nell'Addendum sulla Sicurezza delle Informazioni;

ii. Business Intelligence, per effettuare - in ottemperanza al Codice Etico e nei soli casi previsti dalle norme interne di RINA – verifiche informative su persone fisiche e giuridiche al fine di valutarne l'affidabilità.

La presente Politica è sottoposta a revisione annuale, al fine di assicurare che la gestione dei rischi di security sia efficacemente applicata nell'ambito dell'organizzazione del RINA.

Genova, 9 Settembre 2019

Presidente e Amministratore Delegato

(Ugo Salerno)

POLITICA DI SECURITY

Addendum sulla Sicurezza delle Informazioni

Le informazioni rappresentano un asset di fondamentale importanza per RINA ed i propri stakeholders, in considerazione delle attività di business svolte nei servizi TIC (testing, inspection e certificazione) e di consulenza ingegneristica. Violazioni della riservatezza, dell'integrità o della disponibilità delle informazioni del RINA, dovuti ad azioni di agenti endogeni o esogeni, hanno il potenziale di arrecare un danno rilevante all'azienda ed ai suoi stakeholders, incluse perdite finanziarie e di reputazione.

RINA è impegnata ad assicurare che le proprie parti interessate gestiscano le informazioni aziendali sensibili e confidenziali in modo da evitare utilizzi impropri ed al fine di garantire un appropriato livello di riservatezza, integrità e disponibilità dei dati.

Ai fini della presente Politica, per informazioni aziendali si intendono tutte le informazioni riferite direttamente e/o indirettamente alla natura ed alle attività dell'azienda e generalmente di proprietà di questa. L'informazione è qualsiasi insieme di dati, elaborati, comunicati utilizzato nello svolgimento dell'attività lavorativa (es. documenti, filmati, ecc.). L'informazione può risiedere in qualsiasi supporto idoneo a contenere e a registrare insiemi di dati, quali carta e memorie informatiche.

Al fine di implementare quanto sopra, RINA adotta un sistema di gestione della sicurezza delle informazioni in linea con i migliori standard internazionali e con la norma ISO 27001, comprensivo di un insieme di misure organizzative, procedurali e di sicurezza.

RINA ha adottato una struttura organizzativa per gestire i rischi per la sicurezza delle informazioni, adottare le necessarie procedure e implementare i presidi di controllo. I Manager delle Unità operative di RINA sono responsabili di controllare che la sicurezza delle informazioni sia implementata nell'ambito della propria area di responsabilità. Tutto il personale di RINA deve ottemperare ai regolamenti ed alle procedure interne ed assicurare che, per quanto di propria competenza, le informazioni aziendali siano gestite conformemente alle procedure richiamate.

RINA si impegna ad assicurare che tutto il personale riceva adeguata formazione in tema di sicurezza in relazione alle attività ed allo scopo delle informazioni gestite, e che sia mantenuto un adeguato livello di consapevolezza interna sui rischi per la sicurezza delle informazioni nonché sulle politiche e procedure interne in tema.

RINA riesamina periodicamente gli indicatori del Sistema di Gestione per la Sicurezza delle Informazioni ed è impegnato a conseguire il miglioramento continuo. L'obiettivo è di assicurare che l'esposizione al rischio sia allineata con le strategie e gli obiettivi aziendali, e che le azioni correttive siano implementate ove necessarie.

Tutte le attività inerenti alla sicurezza delle informazioni sono condotte in piena ottemperanza delle normative applicabili nonché dei best standard internazionali.

Il presente Addendum è sottoposto a revisione periodica, al fine di assicurarne l'allineamento con la strategia e l'organizzazione del RINA.

Genova, 9 Settembre 2019