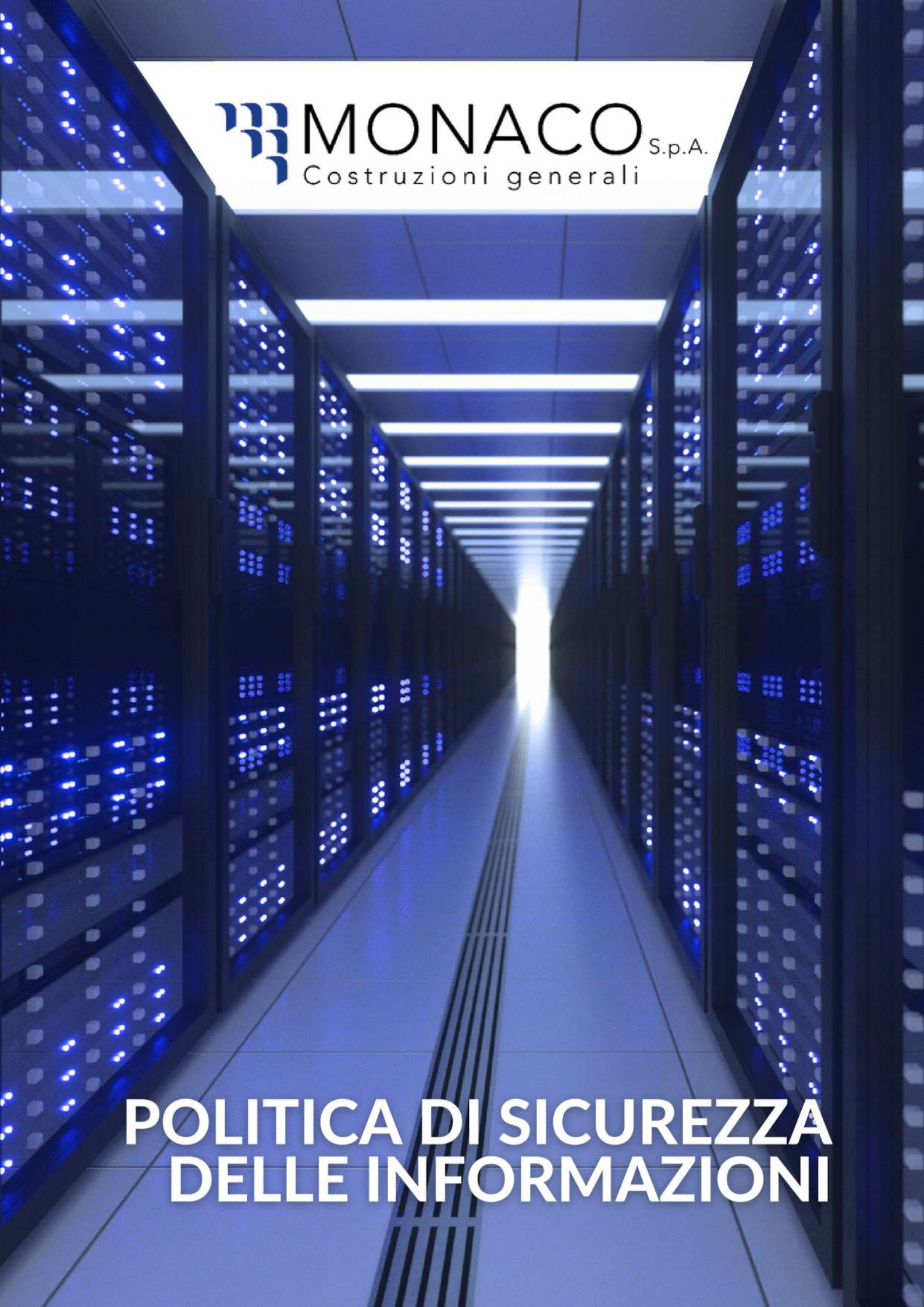

POLITICA DI SICUREZZA DELLE INFORMAZIONI

SCOPO

La presente Politica per la, Sicurezza delle Informazioni e Anticorruzione, documentata, affissa nei locali dell'organizzazione, divulgata al personale e alle parti terze, costituisce la guida per i processi decisionali di <<MONACO>>. fornendo, con indirizzi ben identificati e specificati, l'ambito entro il quale devono essere definiti gli Obiettivi per la Sicurezza delle Informazioni e che tutte le funzioni debbono perseguire ognuna in base alle proprie attribuzioni.

PRINCIPI

La presente Politica per la, Sicurezza delle Informazioni e Anticorruzione, documentata, affissa nei locali dell'organizzazione, divulgata al personale e alle parti terze, costituisce la guida per i processi decisionali di <<MONACO>>. fornendo, con indirizzi ben identificati e specificati, l'ambito entro il quale devono essere definiti gli Obiettivi per la Sicurezza delle Informazioni e che tutte le funzioni debbono perseguire ognuna in base alle proprie attribuzioni.

I principi permanenti che stanno alla base della Politica <<MONACO>>. si basano sulla condivisione, sul coinvolgimento e sulla partecipazione di tutto il personale dell'organizzazione per l'efficace attuazione del Sistema di Gestione per la Sicurezza delle Informazioni secondo i requisiti presenti nelle norme di riferimento, e sono:

- l'integrazione nei processi decisionali del Risk Based Thinking;
- il rispetto del Codice Etico dell'organizzazione, attraverso l'applicazione delle Procedure del Sistema di Gestione Integrato che costituisce naturale completamento operativo dei Protocolli del Modello Organizzativo adottato ai sensi del D.Lgs. 231/2001;
- Il rispetto del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (...) e del DECRETO LEGISLATIVO 10 agosto 2018, n. 101 recante le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679
- la soddisfazione delle parti interessate, dove per parti interessate si intendono i Clienti, l'Organizzazione, il Personale, i Fornitori ed in senso lato il contesto ambientale e sociale in cui opera la <<MONACO>>.;
- il rispetto dei requisiti contrattuali al pari di quelli delle Direttive, Norme, Regolamenti e Leggi applicabili;
- il miglioramento continuo;
- la competenza e la consapevolezza delle risorse coinvolte;
- l'efficacia e l'efficienza nella realizzazione del prodotto e del servizio.
- Il rispetto delle prassi e delle politiche a protezione delle informazioni.

FUNZIONE E STRUTTURA DELLA POLITICA

Sulla base dei suddetti principi, l'Alta Direzione elabora gli Obiettivi da perseguire assegnandoli alle funzioni responsabili e registrandoli. A.D. tiene sotto controllo l'andamento e ne verifica il raggiungimento in occasione delle periodiche riunioni di Riesame. La presente Politica è aggiornata e riesaminata periodicamente.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

<<MONACO>>., nell'ambito dei propri scopi garantisce un servizio attento e rispondente alle esigenze dei propri Clienti, tutelandone al meglio i diritti, nella maniera più soddisfacente possibile per entrambe le parti.
In particolare, data l'importanza e la criticità della prestazione che in alcuni casi può essere chiamata a svolgere, <<MONACO>>. intende offrire servizi che garantiscano il Cliente anche dal punto di vista della riservatezza e tutela delle informazioni.
L'Alta Direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

L'obiettivo principale del Sistema di Sicurezza delle Informazioni è il rispetto delle richieste contrattuali del Cliente che si concretizza nell'assicurare per tutte le informazioni e i dati inerenti all'oggetto:

- riservatezza – assicurando che le informazioni siano accessibili solo alle persone autorizzate
- integrità – tutelando l'esattezza e la completezza delle informazioni e dei metodi con cui sono elaborate
- disponibilità – assicurando che gli utenti autorizzati possano accedere alle informazioni ed ai beni associati, quando richiesto.

A tale scopo <<MONACO>>.:

- rispetta leggi, norme e regolamenti vigenti al fine di raggiungere anche la soddisfazione del Cliente;
- garantisce lo standard di sicurezza delle informazioni mediante controlli costanti;
- garantisce un'efficace assistenza in termini di tempestività e costanza nella comunicazione delle informazioni relative ai procedimenti e di rispetto degli obblighi di riservatezza, integrità e disponibilità;
- garantisce la sicurezza di tutte le informazioni inerenti l'oggetto delle forniture per assicurare la protezione delle informazioni dalla perdita di riservatezza, integrità e disponibilità.

La Politica di sicurezza delle informazioni si realizza, inoltre, attraverso l'attuazione delle misure previste ai seguenti punti:

- sistema per la continuità operativa (business continuity) in caso di perdita o danneggiamento delle informazioni;
- Politica di backup per le macchine critiche e di salvataggio ed archiviazione dei dati;
- controllo dei dati in transito per la sicurezza della rete su cui poggia il sistema informatico dell'organizzazione;
- sistema di credenziali per l'autenticazione degli accessi logici;
- verifica periodica idoneità dei luoghi dove sono contenute le macchine critiche e controllo degli accessi fisici;
- gestione dei log per le attività ritenute critiche;
- formazione degli amministratori di sistema e degli utenti;
- registro asset hardware/software costantemente aggiornato;
- gestione centralizzata antivirus;
- verifica continua del sistema informatico con registrazione esiti;
- test e audit interni sul sistema;
- applicazione delle politiche di sicurezza delle informazioni implementate all'interno del proprio perimetro di sicurezza.

L'osservanza e l'attuazione delle policy sono responsabilità di:

a. Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione. Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
b. Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda. Devono garantire il rispetto dei requisiti contenuti nella presente policy.

Il Responsabile del Sistema di Gestione che, nell'ambito del Sistema di Gestione Integrato e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni.
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione Integrato.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

L'Alta Direzione verificherà periodicamente e regolarmente e in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione Integrato, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.
Il Responsabile del Sistema di Gestione Integrato ha la responsabilità del riesame della politica.
Tale riesame periodico rendiconta lo stato delle azioni preventive e correttive e l'aderenza alla politica e tiene conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.
Il risultato del riesame include tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

INDIRIZZO
ALTA DIREZIONE

MONACO S.p.A.