Politica per la sicurezza delle informazioni

Il presente documento rappresenta la Politica per la sicurezza delle informazioni per Officine Meccaniche Rezzatesi Srl e per tutte le aziende del gruppo OMR, inclusa OMR Holding (di seguito indicate come "OMR" o Organizzazione).

OMR opera nel settore automotive nel campo della fabbricazione e assemblaggio di strutture di telai in alluminio, produzione di fusione in lega di alluminio e lavorazione di pezzi singoli e assemblati.

OMR considera la sicurezza delle informazioni di business e dei dati personali un elemento fondamentale per la continuità, l'affidabilità e la competitività aziendale. Per questo motivo l'Organizzazione ha adottato un Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) volto a governare in modo strutturato rischi, controlli e responsabilità.
I requisiti di legge, regolamentari, contrattuali e di settore applicabili alla sicurezza delle informazioni e alla protezione dei dati trattati da OMR sono identificati e mantenuti aggiornati nel **OMR-RegistroRequisitiApplicabili**, che costituisce il riferimento unico per il recepimento nel SGSI degli obblighi esterni e delle richieste dei clienti. L'ISMS di OMR si ispira alle migliori pratiche e agli standard internazionali di riferimento in materia di gestione della sicurezza delle informazioni.
La presente Politica si inserisce nel Sistema di Gestione per la Sicurezza delle Informazioni di OMR e trova attuazione attra verso la documentazione del SGSI, tra cui in particolare il **OMR-Manuale-CompliancePrivacy-ISMS**, il **OMR-SoA-SicurezzaInformazioni**, il **OMR-RegistroRequisitiApplicabili**, il **OMR-RegolamentoComitatoSicurezza** e le **OMR-SchedeRuolo-SicurezzaPrivacy**.
L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di OMR è di garantire un adeguato livello di sicurezza delle informazioni nell'ambito delle attività di gestione ed elaborazione dei dati, attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i processi che sottintendono i servizi erogati sono soggetti.

Inoltre, il Sistema di Gestione per la Sicurezza per le Informazioni di OMR definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza delle informazioni e dei dati personali di base:

- ***Riservatezza**, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;*
- ***Integrità**, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;*
- ***Disponibilità**, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.*

OMR verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire di:

- *Definire il Sistema di Gestione per la Sicurezza delle Informazioni per la verifica dell'adeguatezza del sistema informativo aziendale, garantendo che la sicurezza sia parte integrante del processo di erogazione dei servizi aziendali.*
- *adottare criteri e metodologie per l'analisi e la gestione del rischio;*
- *istituire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della continuità del servizio, attraverso l'attuazione e il mantenimento del piano di continuità del business;*
- *istituire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela degli interessati, i cui dati personali sono trattati dall'organizzazione;*
- *pianificare un percorso formativo, specifico e periodico in materia di sicurezza delle informazioni e dei dati personali per il personale di OMR;*
  *OMR garantisce che le attività di formazione e sensibilizzazione in materia di sicurezza delle informazioni siano svolte in modo **continuativo e periodico**, affinché tutto il personale mantenga un livello di consapevolezza adeguato ai rischi e ai propri compiti operativi.*
  Il programma formativo prevede momenti di aggiornamento annuale, attività di onboarding per il nuovo personale e

This specification is copyright and the property of OMR It must not be copied (in whole or in part), used for manufacture or otherwise disclosed without prior written consent of the company. Any copies of this specification made by any method must also include a copy of this legend.

campagne di sensibilizzazione costante.
L'efficacia della formazione è verificata attraverso ***test di apprendimento e simulazioni pratiche****, quali ad esempio campagne di phishing o esercitazioni comportamentali, i cui risultati vengono registrati nel* ***Registro Formazione ISMS*** *e riesaminati periodicamente dal Responsabile ISMS e dalla Direzione.*

- *controllare periodicamente l'esposizione dei servizi aziendali e dei trattamenti di dati personali alle principali minacce;*
- *verificare gli incidenti di sicurezza e i data breach e adottare le opportune contromisure;*
- *promuovere la cultura riguardante la sicurezza delle informazioni e la tutela dei dati personali;*
- *garantire la congruità dei singoli budget destinati alla sicurezza, coerentemente alle politiche e alle linee strategiche aziendali definite;*
- *definire gli obiettivi e le responsabilità delle figure organizzative di sicurezza e privacy.*

Le linee guida, le procedure e le istruzioni operative di sicurezza sono dettagliate in uno specifico impianto documentale, e rese disponibili al personale in funzione degli incarichi ricoperti.

A prescindere dal ruolo ricoperto, è compito di tutto il personale OMR:

- *Conoscere i contenuti del presente documento e contribuire nell'attuazione delle direttive e degli obiettivi di sicurezza in esso indicati;*
- *applicare le linee guida, le procedure e le istruzioni operative di sicurezza di propria competenza ;*
- *trattare correttamente le informazioni di business e i dati personali;*
- *segnalare la presenza di eventuali incidenti di sicurezza, di data breach, di anomalie o di possibili minacce.*

OMR consente la comunicazione e la diffusione delle informazioni e dei dati personali verso l'esterno, solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti, in relazione agli specifici flussi formalizzati definiti, per garantire il pieno ed efficiente governo del processo comunicativo.
Il presente documento è approvato dalla Direzione di OMR. Il **Responsabile ISMS** ne assicura il mantenimento e il riesame in occasione di modifiche rilevanti del contesto interno ed esterno, dei processi aziendali, dell'organizzazione o dei requisiti applicabili, nonché nell'ambito del riesame periodico del Sistema di Gestione per la Sicurezza delle Informazioni.

This specification is copyright and the property of OMR It must not be copied (in whole or in part), used for manufacture or otherwise disclosed without prior written consent of the company. Any copies of this specification made by any method must also include a copy of this legend.