Politica di Sicurezza delle Informazioni – P-ISMS-001.00

REVISIONE	DATA	OGGETTO	EMISSIONE	VERIFICA	APPROVAZIONE
0	03/06/25	Prima emissione	D. Oliveri	L. Tilli	G. Tumini

TMC srl riconosce che la protezione delle informazioni è essenziale per il successo aziendale e per mantenere la fiducia dei propri clienti, dipendenti e altre parti interessate.

La sicurezza delle informazioni è un aspetto fondamentale per proteggere i dati sensibili, assicurare la continuità operativa e rispettare gli obblighi legali.

Questa politica definisce gli obiettivi, i principi guida e le misure per la gestione della sicurezza delle informazioni in linea con lo Standard ISO 27001, in compliance con i controlli della normativa TISAX (AL2), ed in linea con gli obiettivi aziendali nel rispetto di:

- GDPR
- IATF 16949
- UNI EN ISO 9001
- UNI EN ISO 14001
- UNI EN ISO 3834
- UNI EN 1090

L'ambito di applicazione dell'ISMS / SGSI (Sistema di Gestione della Sicurezza delle Informazioni) comprende tutte le sedi operative dell'azienda dove vengono sviluppati e realizzati i prodotti secondo i più elevati standard qualitativi del Made in Italy

Sede: Zona Industriale Punta penna (snc) 66054 - Vasto

Le misure possono riferirsi a:

- Dati OEM: File tecnici (CAD, specifiche) forniti dai partner.
- Infrastrutture IT: Server locali e cloud utilizzati per l'archiviazione.
- Sito web aziendale: Strumento informativo.

L'obiettivo delle Politiche Aziendali di TMC srl è quello di mitigare i rischi legati alla compromissione della sicurezza adibita per la tutela delle informazioni.

Le politiche di sicurezza a cui si fa riferimento sono state adattate alle esigenze aziendali.

Qualunque aggiornamento relativo alle politiche di sicurezza per la tutela delle informazioni deve essere approvata da TMC srl e deve essere pubblicata e/o comunicata dalla stessa tramite i canali di comunicazione di seguito riportati:

- Email di comunicazione
- Pubblicazione nell'intranet
- Pubblicazione sul sito tmcvasto.com
- Affissione nella bacheca aziendale.
- Documento firmato dalla direzione o da un suo rappresentante

Nel presente documento, per semplificare la lettura e garantire chiarezza espositiva, i termini "noi", "ci", "nostro" e simili faranno riferimento a TMC srl.

Documenti Allegati

La Politica qui di seguito definisce metodi e requisiti che sono approfonditi nelle relative politiche in uso:

- POLITICA INTEGRATA-Qualita-Ambiente-Sicurezza- TMC S.r.l. rev1 31.07.2023
- TMC srl_Piano di monitoraggio e Audit
- Risk Management TMC srl
- (BCP) - TMC srl Piano di Continuità Operativa
- TMC srl Analisi del contesto
- TMC srl- Handle an Incident
- TMC srl_Disaster Recovery (DR)
- TMC srl_Piano di Formazione e Consapevolezza del rischio
- TMC srl- Modulo Autorizzazione per Riprese Fotografiche o Video
- TMC srl- Modulo di Registrazione Visitatori
- TMC srl- Modulo Richiesta Accesso Aree Riservate
- TMC srl- Procedura per la Valutazione dei Rischi
- TMC srl- Registro Accessi alle Aree Protette
- TMC srl(NDA) Accordi di riservatezza
- TMC srl_Dispositivi e lavoro da remoto
- TMC srl_Relazione con partner e fornitori
- TMC srl - Piano di Implementazione e Monitoraggio dei Controlli di Sicurezza
- TMC srl Request for Change (RFC)
- TMC srl_Segnalazione incidente
- TMCsrl-Incident Response Policy and Procedures
- Password Policy TMC srl
- Ruoli e Responsabilità TMC srl
- Dichiarazione di Applicabilità (SoA - Statement of Applicability)

Questi documenti nel suo insieme costituiscono l’ISMS / SGSI (Sistema di gestione della sicurezza delle informazioni) di TMC srl

Scopo e Ambito

Ci impegniamo a garantire che tutte le informazioni aziendali siano trattate con il massimo livello di protezione attraverso obiettivi chiari e misurabili.

Gli obiettivi di sicurezza delle informazioni sono fondamentali per preservare la confidenzialità, l'integrità e la disponibilità delle informazioni.

Questa politica si applica a tutte le informazioni gestite da TMC srl, indipendentemente dal formato, dalla natura o dal supporto utilizzato.

Le informazioni coperte includono, ma non si limitano a:

- Dati elettronici: tutti i dati digitali trattati e archiviati nei sistemi informatici aziendali, inclusi file, database, e-mail, e comunicazioni elettroniche.
- Documenti cartacei: qualsiasi documento fisico che contenga informazioni aziendali, come contratti, rapporti, manuali e altri materiali riservati.
- Comunicazioni verbali: conversazioni, briefing e riunioni aziendali, inclusi gli scambi informali tra dipendenti, partner, fornitori e clienti.
- Informazioni digitali: comprendono documenti elettronici, immagini, audio e video archiviati o trasmessi tramite dispositivi digitali, applicazioni aziendali, piattaforme cloud e altre tecnologie.

Nota:

- Leggi NDA

L'ambito di applicazione di questa politica include:

- Sedi aziendali: tutti gli uffici e le strutture operative di TMC srl sede di Vasto.
- Dipendenti: ogni persona che lavora per TMC srl a qualsiasi titolo (a tempo pieno, part-time, stagisti, consulenti, etc.), che deve attenersi alle politiche e alle procedure aziendali relative alla sicurezza delle informazioni.
- Partner e fornitori: tutte le organizzazioni o individui che forniscono servizi o prodotti a TMC srl e che trattano informazioni sensibili aziendali, i quali devono rispettare i requisiti di sicurezza stabiliti nel contratto e nell'accordo di collaborazione.
- Terze parti: entità che, pur non essendo direttamente controllate da TMC srl, accedono alle informazioni aziendali sensibili per motivi specifici

L’obiettivo principale di questa politica è garantire i seguenti principi fondamentali in tutte le operazioni aziendali:

- Confidenzialità: Assicurare che le informazioni siano accessibili solo a persone autorizzate e che vengano protette da accessi non autorizzati.
- Integrità: Proteggere le informazioni da modifiche non autorizzate o dannose, garantendo che i dati siano accurati, completi e affidabili.
- Disponibilità: Garantire che le informazioni siano accessibili quando necessario e che i sistemi e le risorse aziendali siano operativi in modo continuo, senza interruzioni.

L'applicazione di questa politica si estende a tutte le operazioni aziendali di TMC srl, dalle attività quotidiane interne alla gestione delle relazioni con clienti e fornitori.

Il rispetto delle normative e degli standard internazionali, come lo standard ISO/IEC 27001, è essenziale per tutelare le informazioni e le risorse aziendali, nonché per mantenere la fiducia di tutti gli stakeholder.

Revisione e adattamento continuo: Le politiche saranno riviste periodicamente, con l'intento di adattarsi ai cambiamenti normativi, tecnologici e organizzativi, al fine di continuare a garantire un alto livello di sicurezza delle informazioni in tutta l'organizzazione.

Garantire la Confidenzialità delle Informazioni:

Impedire l'accesso non autorizzato alle informazioni aziendali è una priorità.

TMC srl adotta misure di protezione per garantire che solo gli utenti legittimi possano accedere e utilizzare i dati sensibili, evitando che vengano divulgati a persone non autorizzate

- I dati devono essere utilizzati esclusivamente per scopi aziendali legittimi, e ogni trattamento di dati sensibili deve avvenire nel rispetto delle normative in vigore
- Le procedure di autenticazione e di gestione dei privilegi sono implementate per controllare l'accesso alle informazioni e impedire l'abuso dei diritti di accesso, e documentate all’interno della Password Policy di TMC srl

Salvaguardare l'Integrità delle Informazioni:

Ci impegniamo a prevenire qualsiasi alterazione non autorizzata delle informazioni aziendali. Tutti i dati devono rimanere accurati, completi e consistenti.

Per garantire l'integrità delle informazioni i dati altamente sensibili e classificati da TMC come Segreto Industriale vengono crittografati.

Inoltre il monitoraggio delle azioni sulla rete deve essere attivo tramite l’utilizzo delle tecnologie di tracciamento dei dati log al fine di identificare eventuali modifiche non autorizzate.

Viene effettuato il monitoraggio della sicurezza dei sistemi aziendali tramite test di vulnerabilità ad attacchi informatici (Vulnerability Assessment) pianificati

Assicurare la Disponibilità delle Informazioni e dei Sistemi Critici:

- TMC srl assicura che le informazioni e i sistemi critici siano sempre disponibili, anche in situazioni di emergenza o in caso di disastri.
- Viene mantenuto un piano di disaster recovery (DR) e un sistema di continuità operativa (BCP) per garantire che, in caso di guasti o attacchi, i sistemi aziendali possano essere rapidamente ripristinati, minimizzando i tempi di inattività.
- I backup regolari e la ridondanza delle infrastrutture sono fondamentali per assicurare che i dati possano essere recuperati in caso di malfunzionamenti, guasti hardware o incidenti imprevisti.

Migliorare Continuamente il Sistema di Gestione della Sicurezza delle Informazioni (ISMS):

- TMC srl si impegna a migliorare continuamente il proprio Sistema di Gestione della Sicurezza delle Informazioni (ISMS) per rispondere ai cambiamenti tecnologici, alle nuove minacce informatiche e alle evoluzioni normative.
- Le politiche di sicurezza vengono periodicamente riviste e aggiornate per adattarsi alle nuove tecnologie e alle potenziali vulnerabilità emergenti. Inoltre, vengono effettuati audit (Vedi La politica sui piani di Audit e Monitoraggio di TMC srl), e valutazioni dei rischi (Vedi Risk Management ed Incident Response) per garantire che le misure di sicurezza siano sempre efficaci e adeguate.
- Il personale viene regolarmente formato e sensibilizzato sui rischi emergenti e sulle migliori pratiche di sicurezza per garantire che l'intera organizzazione sia preparata a difendersi da attacchi informatici e da altre minacce (Riferimento a Piano di Formazione e Consapevolezza del rischio).

Confidenzialità

Al fine di garantire che tutte le informazioni riservate siano trattate in modo sicuro e che il rischio di accessi non autorizzati venga ridotto al minimo, TMC srl adotta le seguenti misure:

1. Crittografia dei Dati:
    - I dati sensibili, sia durante il trasferimento che quando sono archiviati (a riposo), vengono crittografati
2. Controllo dell’Accesso e Gestione dei Privilegi:
    - L'accesso alle informazioni aziendali è limitato solo alle persone autorizzate e per scopi legittimi.
3. Gli utenti devono essere autenticati tramite:
    - Password complesse
        i. Chiave di cifratura su asset sensibili o account con diritti da amministratore
    - La gestione dei privilegi è centralizzata per assicurare che ogni dipendente abbia accesso solo alle informazioni necessarie per il suo ruolo. L’approccio di "accesso minimo" deve essere applicato rigorosamente.

Nota:

Le procedure e le politiche in questione sono presenti all’interno del Password Policy aziendale.

4. Sensibilizzazione dei Dipendenti:
    - TMC srl si impegna a sensibilizzare costantemente i dipendenti riguardo ai rischi associati alla divulgazione non autorizzata delle informazioni e alle

possibili minacce come phishing, ingegneria sociale, e altri tipi di attacchi informatici.
- Sono organizzati corsi di formazione regolari e sessioni di aggiornamento su temi legati alla sicurezza delle informazioni, che includono buone pratiche, comportamenti da evitare e procedure di risposta in caso di violazione della sicurezza.
- Ogni dipendente è tenuto a seguire le politiche aziendali relative alla gestione delle informazioni riservate e deve essere consapevole delle conseguenze derivanti dalla violazione della confidenzialità.
- Leggi:

    i. Piano di Formazione e Audit

5. Gestione dei Dispositivi Aziendali:
    - Tutti gli asset aziendali compresi i dispositivi, i computer, gli smartphone, i tablet e altri dispositivi elettronici, devono essere trattati in conformità con le politiche di sicurezza stabilite da TMC srl
    - I dispositivi devono essere protetti da password robuste, software di sicurezza aggiornato (antivirus, firewall, ecc.), e devono essere configurati per attivare automaticamente la crittografia dei dati sensibili.

    - Le politiche di sicurezza per i dispositivi aziendali sono contenute nell'allegato "Dispositivi aziendali e lavoro remoto", che fornisce linee guida dettagliate per l'adozione delle tecnologie di difesa e protezione più appropriate. L'allegato include anche le procedure per il monitoraggio dei dispositivi aziendali e per l'intervento tempestivo in caso di vulnerabilità o incidente di sicurezza.
    - Leggi:

        i. Dispositivi e lavoro da remoto

6. Monitoraggio e Audit:
    - Saranno effettuati audit regolari e verifiche di conformità per garantire che le misure di protezione siano efficaci e che le politiche di sicurezza vengano rispettate.

Il personale e le altre parti interessate devono restituire tutti i beni dell'organizzazione in loro possesso al cambiamento o alla cessazione del loro impiego

Integrità

L'integrità delle informazioni è fondamentale per noi, in quanto garantisce che i dati siano accurati, completi e non siano stati alterati in modo non autorizzato.

TMC srl adotta una serie di misure tecniche e organizzative per garantire che le informazioni siano protette da manipolazioni indesiderate e siano sempre verificabili.

Le principali misure adottate includono:

Verifica dell'Integrità dei Dati:

1. I log di accesso e le attività di modifica dei dati vengono tracciati e auditati regolarmente per identificare modifiche sospette o inusuali che potrebbero compromettere l'integrità delle informazioni. Ogni modifica ai dati sensibili o alle configurazioni dei sistemi viene registrata per garantire la trasparenza e la responsabilità.
2. Per prevenire la perdita o la corruzione dei dati, TMC srl adotta sistemi di backup sicuri che consentono il ripristino accurato delle informazioni. I backup vengono eseguiti regolarmente su server interni, supporti esterni sicuri ed in cloud, e vengono archiviati in ambienti protetti da crittografia avanzata per evitare accessi non autorizzati.

Disponibilità

La disponibilità delle informazioni è un principio fondamentale per il buon funzionamento di TMC srl, poiché le informazioni devono essere accessibili in modo continuo e tempestivo per supportare l'efficienza operativa e garantire che i processi aziendali non subiscano interruzioni. TMC srl implementa una serie di soluzioni tecnologiche e processi operativi per garantire che le informazioni siano sempre disponibili, anche in situazioni critiche o di emergenza. Le misure adottate includono:

1. Soluzioni di Disaster Recovery e Continuità Operativa:
    - TMC srl ha messo in atto soluzioni di disaster recovery (DR) per garantire la rapida ripresa delle attività aziendali in caso di guasti gravi o disastri naturali. Questi sistemi di recovery permettono di ripristinare rapidamente i dati e i servizi critici, riducendo al minimo i tempi di inattività e l'impatto sulle operazioni aziendali.
    - Le soluzioni di continuità operativa (BCP) sono progettate per mantenere le operazioni aziendali attive anche in caso di eventi catastrofici, come interruzioni della fornitura di energia, attacchi informatici su larga scala o disastri naturali. Questi piani di contingenza includono la gestione di risorse di backup, e l'uso di infrastrutture in cloud che possono essere rapidamente attivate.
2. Utilizzo di VPN e Tecnologie di Accesso Sicuro:
    - TMC srl adotta Virtual Private Network (VPN) e altre tecnologie di accesso sicuro per garantire che le informazioni aziendali possano essere consultate e utilizzate in modo protetto anche da luoghi remoti, e per proteggere le comunicazioni e il trasferimento dei dati, in particolare quando si operano in contesti di smart working o in situazioni di emergenza (Vedi la policy aziendale: Protezione dei dispositivi e lavoro da remoto).
    - L'utilizzo di VPN sicure assicura che il traffico di dati sensibili venga cifrato, impedendo che vengano intercettati o manipolati durante il loro transito su reti

non sicure, come Internet pubblici o reti aziendali vulnerabili. Inoltre, le VPN forniscono un canale protetto per l'accesso alle risorse aziendali interne, riducendo il rischio di accessi non autorizzati.
    - Tecnologie di autenticazione a più fattori (MFA) vengono impiegate per rafforzare la sicurezza dell'accesso, in particolare per i dipendenti e i partner che necessitano di entrare in contatto con sistemi ed informazioni aziendali sensibili. Questo garantisce che solo gli utenti autorizzati possano accedere alle risorse aziendali, anche in situazioni critiche.
3. Backup Regolari e Testati:
    - TMC srl implementa un sistema di backup regolari e sicuri per garantire che tutti i dati critici siano sempre protetti e possano essere recuperati tempestivamente in caso di guasto o attacco informatico. I backup vengono effettuati su base giornaliera.
    - I backup vengono conservati in posizioni sicure, sia locali che off-site (come cloud o data center remoti), per garantire che i dati possano essere ripristinati rapidamente anche in caso di incidenti che compromettano le infrastrutture aziendali primarie.

Impegno della Leadership

La Direzione di TMC srl si impegna a supportare attivamente e a garantire che la sicurezza delle informazioni sia una priorità a livello aziendale.

L’impegno della leadership è fondamentale per il successo del Sistema di Gestione della Sicurezza delle Informazioni e per la creazione di una cultura aziendale che promuova la protezione delle informazioni

Le azioni concrete intraprese dalla Direzione includono:

Fornitura di Risorse Adeguate:

- Risorse adeguate sono destinate non solo per l'acquisto di strumenti tecnologici necessari per proteggere le informazioni aziendali, ma anche per investire in formazione continua per il personale, aggiornamenti delle infrastrutture e analisi dei rischi.
- La leadership assicura che ci sia una gestione efficace delle risorse per fronteggiare le sfide emergenti legate alla sicurezza delle informazioni e per garantire che l'organizzazione rimanga conforme agli standard e alle normative internazionali di sicurezza.
- Viene garantita una supervisione costante e un monitoraggio continuo delle politiche di sicurezza, affinché siano sempre allineate con le esigenze aziendali e con l’evoluzione del panorama delle minacce.

Promozione di una Cultura di Consapevolezza della Sicurezza:

- La Direzione si impegna a promuovere una cultura della sicurezza in tutta l'organizzazione. Ciò include la creazione di una mentalità orientata alla protezione delle informazioni, in modo che ogni dipendente, a tutti i livelli, comprenda l'importanza della sicurezza informatica e delle politiche aziendali.
- La leadership promuove la formazione regolare dei dipendenti, offrendo corsi di aggiornamento e sensibilizzazione sui rischi legati alla sicurezza delle informazioni, alle minacce emergenti e alle migliori pratiche da adottare per proteggere i dati aziendali.
- Vengono messi a disposizione strumenti e risorse per consentire ai dipendenti di applicare concretamente quanto appreso, come sistemi di autenticazione sicura, linee guida per la protezione dei dispositivi aziendali, e procedure per la gestione sicura dei dati.

Adozione e Approvazione

La politica di sicurezza delle informazioni di TMC srl si applica a tutti i livelli dell'organizzazione, inclusi dipendenti, fornitori e partner.

1. Impegno da parte della Direzione:
   - La Direzione di TMC srl ha formalmente approvato questa politica e si impegna a garantire la sua corretta implementazione il monitoraggio e l'evoluzione della stessa.
   - La Direzione è anche responsabile di fornire risorse adeguate per l'implementazione e il miglioramento continuo delle misure di sicurezza, nonché per la promozione di una cultura della sicurezza all'interno dell'organizzazione.
2. Obblighi per i dipendenti:
   - Tutti i dipendenti di TMC srl sono tenuti a prendere visione della politica di sicurezza delle informazioni e a seguire le direttive contenute al suo interno.
   - Ogni dipendente è responsabile di adottare comportamenti sicuri nel trattamento delle informazioni aziendali e nel rispetto delle normative applicabili.
   - Eventuali violazioni della politica da parte dei dipendenti saranno trattate in conformità con le politiche disciplinari aziendali ed in base al principio di proporzionalità verso la gravità dell'infrazione.
     Le azioni disciplinari che è possibile adottre in caso di violazioni delle politiche inerenti la sicurezza delle informazioni sono:
     i. Richiamo scritto
     ii. Sospensione dal lavoro
     iii. Licenziamento con preavviso
     iv. Licenziamento senza preavviso

     In caso di gravi violazioni dolose che compromettano la sicurezza delle informazioni o volte ad acquisire profitto dalle informazioni classificate

aziendali e configurino un profilo di reato verranno denunciate all'autorità di competenza.
Ogni provvedimento disciplinare intrapreso prevede la possibilità di giustificazione scritta e l'assistenza di rappresentanze sindacali o legali da parte dell'interessato.

3. Responsabilità di fornitori e partner:
    - I fornitori e partner di TMC srl che trattano informazioni per conto dell'azienda sono tenuti a rispettare gli obblighi contrattuali in materia di sicurezza delle informazioni.
      In caso di violazioni della politiche da parte di fornitori e partner TMC SRL intraprenderà tutte le azioni che riterrà opportune per tutelare i propri interessi
4. Formazione e sensibilizzazione:
    - TMC srl garantirà che tutti i dipendenti ricevano formazione regolare sulla politica di sicurezza delle informazioni, sui rischi associati alla gestione delle informazioni e sulle best practice da seguire.

Gestione della Configurazione

L'azienda adotta una rigorosa Gestione della Configurazione per garantire che tutte le risorse informatiche, tra cui hardware, software, sistemi di rete e applicazioni, siano configurate in modo sicuro.

La gestione delle configurazioni include:

1. Inventario delle risorse: È mantenuto un inventario accurato e aggiornato di tutte le risorse IT aziendali sensibili.
2. Controllo delle modifiche: Le modifiche alle configurazioni, sia hardware che software, sono soggette a un processo di approvazione formale, che prevede la documentazione dettagliata, la valutazione dei rischi per evitare l'introduzione di vulnerabilità.
3. Monitoraggio: Sono implementati strumenti di monitoraggio continuo per rilevare e segnalare qualsiasi modifica non autorizzata alle configurazioni.
4. Formazione e consapevolezza: I dipendenti che gestiscono e modificano le configurazioni sono regolarmente formati sui rischi legati alla configurazione errata e sulle migliori pratiche di sicurezza. La formazione è obbligatoria per tutti i responsabili IT, le figure ISOS ed i Team Leader.

L'azienda considera la Gestione della Configurazione come una componente cruciale per mantenere un ambiente IT sicuro, prevenire attacchi informatici e proteggere le informazioni aziendali e dei clienti.

In caso di non conformità alle politiche di TMC srl da parte della direzione, si potrebbe incorrere a sanzioni.

In caso di non conformità alle politiche da parte dei dipendenti di TMC srl, la stessa si ritiene in possibilità di applicare sanzioni o azioni disciplinari nei confronti dei dipendenti responsabili delle violazioni.

Linee Guida Generali

Le linee guida generali di TMC srl Per la sicurezza delle informazioni stabiliscono le pratiche e i comportamenti da adottare per proteggere i dati aziendali e garantire la sicurezza dei sistemi.

Queste linee guida sono fondamentali per mantenere un ambiente sicuro e conforme alle normative.

Le principali linee guida includono:

1. Classificazione delle informazioni:
    - Le informazioni aziendali devono essere classificate in base alla loro sensibilità. Ogni categoria di informazioni, come quelle riservate, confidenziali, interne o pubbliche, avrà un livello di protezione adeguato alla sua natura
        i. Vedi Matrice di classificazione dei dati.
    - La protezione delle informazioni deve essere proporzionata al loro livello di sensibilità.
2. Accesso alle informazioni:
    - L'accesso alle informazioni aziendali è concesso solo a persone autorizzate. Questo principio si basa sul minimo privilegio, che implica che ogni individuo debba avere accesso solo alle informazioni necessarie per svolgere il proprio lavoro.
    - L'accesso a informazioni sensibili sarà monitorato e limitato tramite l'uso di tecnologie di tracciamento dei dati di log e tramite la gestione dei privilegi utente.
3. Protezione dei dispositivi aziendali:
    - Tutti i dispositivi aziendali, inclusi computer, smartphone, tablet e altri dispositivi mobili, devono essere protetti con password robuste. Le password devono essere complesse, e aggiornate regolarmente come descritto all’interno della Password Policy.
    - È necessario mantenere i dispositivi aziendali protetti tramite l'uso di software di sicurezza aggiornati, come antivirus e firewall, per prevenire vulnerabilità da attacchi informatici.
4. Gestione degli incidenti di sicurezza:
    - Gli incidenti di sicurezza devono essere segnalati immediatamente al Responsabile della sicurezza delle informazioni e gestiti tempestivamente secondo le procedure aziendali stabilite.

- Il Responsabile in sicurezza delle informazioni coordinerà la risposta agli incidenti, che include l'analisi dell'incidente, la mitigazione del danno, e la comunicazione con i soggetti interessati (dipendenti, fornitori, clienti, autorità competenti, se necessario).
- Ogni incidente di sicurezza deve essere registrato in modo dettagliato, con informazioni sui fatti, le azioni intraprese e le lezioni apprese. Questo aiuta a migliorare le politiche e i processi di sicurezza per prevenire futuri incidenti.(vedi incident Response)

Gestione delle modifiche

Ambito:

Questo processo definisce le modalità di gestione, approvazione e implementazione delle modifiche ai sistemi informativi, infrastrutture IT e processi aziendali, al fine di garantire che siano effettuate in modo controllato e sicuro, minimizzando l'impatto sui servizi e riducendo i rischi per la sicurezza delle informazioni.

Obiettivo:

Garantire che tutte le modifiche siano valutate, approvate e implementate nel rispetto dei requisiti di sicurezza, continuità operativa e conformità normativa.

Processo:

1. Richiesta di modifica:
   - Ogni modifica deve essere formalizzata tramite una Richiesta di Modifica (RFC - Request for Change) contenente:
     - Descrizione della modifica.
     - Motivo e obiettivo.
     - Impatto previsto (tecnico, organizzativo, di sicurezza).
     - Analisi dei rischi associati.
     - Pianificazione delle attività necessarie.
2. Valutazione e approvazione:
   - Le richieste di modifica sono valutate
   - La valutazione considera:
     - Impatti su sicurezza, continuità e conformità.
     - Risorse necessarie.
     - Eventuali dipendenze con altri sistemi o processi.
   - Solo le modifiche approvate possono essere implementate.
3. Pianificazione e test:

    - Prima dell'implementazione, le modifiche sono testate in ambienti controllati per verificare:
        - Funzionalità.
        - Assenza di impatti negativi sui sistemi esistenti.
        - Conformità ai requisiti di sicurezza.

È predisposto un piano di rollback per ripristinare lo stato precedente in caso di problemi.

4. Implementazione:
    - Le modifiche sono implementate seguendo il piano approvato.
5. Verifica post-implementazione:
    - Dopo l'applicazione, si effettuano verifiche per garantire che:
        - La modifica funzioni come previsto.
        - Non vi siano problemi di sicurezza o funzionalità.
    - I risultati sono documentati.
6. Documentazione:
    - Ogni modifica implementata è documentata nel registro delle modifiche, includendo:
        - Data e orario dell'implementazione.
        - Responsabili coinvolti.
        - Risultati delle verifiche.
        - Eventuali problemi riscontrati e risolti.

Ridondanza delle strutture di elaborazione

Per garantire la sicurezza e la continuità operativa, TMC srl ha implementato una strategia di ridondanza e backup strutturata come segue:

- Utilizzo di un dispositivo di backup esterno dedicato, che effettua copie regolari dei dati aziendali critici.
- Backup in cloud dei dati presenti sui server, assicurando che le informazioni siano protette anche in caso di eventi che coinvolgano le infrastrutture fisiche.

Questa configurazione consente a TMC srl di mantenere la disponibilità dei dati, ridurre il rischio di perdita di informazioni e assicurare la resilienza contro guasti o eventi imprevisti.

Gestione delle Vulnerabilità Tecniche

1. L'azienda utilizza strumenti automatizzati di scansione delle vulnerabilità per eseguire analisi periodiche dei sistemi e delle reti aziendali.
2. Ogni vulnerabilità identificata viene valutata in base alla sua gravità e al potenziale impatto sulla sicurezza dei sistemi aziendali.
3. Le vulnerabilità critiche vengono trattate come priorità assoluta.

Protezione contro Malware

Le seguenti misure devono essere adottate per prevenire, rilevare e contrastare le minacce informatiche:

1. Utilizzo di Software Anti Malware
    - Tutti i dispositivi aziendali devono essere dotati di software anti malware
2. Aggiornamenti Regolari
    - I sistemi operativi, i software e le applicazioni devono essere mantenuti sempre aggiornati con le ultime patch di sicurezza, salvo casi eccezionali di impossibilità.
3. Uso di Firewall
    - Deve essere attivo un firewall su tutte le macchine aziendali connesse alla rete.
4. Controllo degli Accessi
    - I privilegi di accesso devono essere limitati ai soli utenti che necessitano di accedere a determinate risorse, applicando il principio del minimo privilegio. Le credenziali di accesso devono essere protette e non devono essere condivise.
5. Backup Regolari
    - I dati aziendali devono essere sottoposti a backup regolari, sia in cloud che su dispositivi fisici separati dalla rete aziendale. I backup devono essere criptati per proteggere i dati da possibili attacchi di ransomware.
6. Formazione degli Utenti
    - Gli utenti aziendali devono essere formati periodicamente sui rischi legati al malware, in particolare per riconoscere e evitare email di phishing, allegati sospetti e link dannosi. La formazione deve includere anche la gestione delle password e l'uso di metodi di autenticazione sicura come descritto nella politica di Formazione del Personale Aziendale.
7. Crittografia dei Dati
    - I dati sensibili devono essere cifrati, sia a riposo che in transito, per garantire la protezione in caso di violazioni di sicurezza. Le chiavi di crittografia devono essere gestite in modo sicuro.

TMC srl Vieta il download, l’installazione e l’utilizzo di software non autorizzato dalla stessa. I software possono essere installati solo dal Team IT in seguito alla richiesta della Direzione di TMC srl.

Uso Accettabile delle Informazioni e degli Asset Associati

TMC srl ha definito e implementato regole precise per l'uso accettabile delle informazioni e degli asset aziendali, al fine di garantire che tutte le risorse vengano utilizzate in modo conforme agli obiettivi aziendali e alle normative in vigore. Le politiche stabiliscono che tutti i

dispositivi aziendali, le informazioni sensibili e le risorse tecnologiche devono essere utilizzati esclusivamente per scopi professionali e in conformità con le necessità operative.

Le regole di utilizzo includono, ma non si limitano a:

- L'uso esclusivo di dispositivi aziendali per attività professionali, vietando l'installazione di software non autorizzato e l'uso di dispositivi per scopi personali.
- L'accesso alle informazioni sensibili è limitato a coloro che ne hanno necessità per motivi di lavoro e deve avvenire in conformità con i livelli di autorizzazione previsti.
- Le informazioni aziendali devono essere trattate con la massima riservatezza, conservate in modo sicuro e protette da misure di sicurezza adeguate, come la crittografia.
- L'accesso alla rete aziendale deve avvenire tramite canali sicuri, come VPN, e in conformità con le procedure di sicurezza interne.

Monitoraggio e Miglioramento

TMC srl si impegna a garantire che la politica di sicurezza delle informazioni rimanga efficace e aggiornata, rispondendo ai cambiamenti tecnologici, organizzativi e normativi. Per mantenere e migliorare continuamente il livello di sicurezza, vengono adottate le seguenti misure:

1. Revisione annuale della politica:
    - La politica verrà rivista annualmente o quando necessario per garantire che rispecchi le modifiche nell'organizzazione, le nuove normative applicabili e l'evoluzione delle minacce informatiche.
    - La revisione include l'aggiornamento delle misure di sicurezza, delle pratiche operative e dei controlli per allinearsi con i nuovi standard o le best practice emergenti.
2. Audit interni e revisioni periodiche:
    - Verranno effettuati audit interni regolari per esaminare la conformità alle politiche di sicurezza e identificare eventuali debolezze nei processi o nelle misure implementate.
    - Le revisioni periodiche dei processi di sicurezza permetteranno di eseguire un controllo approfondito delle pratiche aziendali in relazione alla protezione delle informazioni, facendo emergere aree di possibile miglioramento.
3. Analisi dei rischi:
    - TMC srl condurrà analisi dei rischi per valutare le vulnerabilità potenziali e l'impatto di eventuali minacce sulla sicurezza delle informazioni aziendali.
    - L'azienda eseguirà regolarmente valutazioni delle performance del sistema di gestione della sicurezza (ISMS) per monitorare l'efficacia delle misure di protezione e per apportare modifiche a quelle che non soddisfano gli obiettivi prefissati.
4. Gestione degli incidenti di sicurezza:

- In caso di incidenti di sicurezza, TMC srl adotta un processo strutturato per la gestione e l'analisi degli eventi, al fine di identificare le cause e le lacune nei controlli di sicurezza.
- Ogni incidente sarà un'opportunità per identificare aree di miglioramento nelle pratiche aziendali e adottare nuove soluzioni preventive per evitare il ripetersi di situazioni simili in futuro.

Questa politica è vincolante e ha l'obiettivo di assicurare che tutte le parti coinvolte nella gestione delle informazioni aziendali siano allineate e agiscano in modo sicuro ed efficace, proteggendo la riservatezza, l'integrità e la disponibilità delle informazioni trattate.

Approvato da:

La Direzione - TMC srl

Data

03 / 06 / 2025

Firma