ITALMOBILIARE
INVESTMENT HOLDING

LINEE GUIDA

Sicurezza delle Informazioni
Cyber Security

2026

Italmobiliare S.p.A.
SEDE LEGALE:
Via Borgonuovo 20, Milano
www.italmobiliare.it

Sommario

SICUREZZA DELLE INFORMAZIONI 3

Scopo 3
Obiettivi 3
I principi e i requisiti di sicurezza 4

CYBER SECURITY 5

Procedure e regolamenti interni di sicurezza delle informazioni 5
Organizzazione della sicurezza 5
Sicurezza dei progetti 5
Remote Working 5
Risorse Umane 5
Gestione degli Asset e Classificazione delle Informazioni 6
Controllo Accessi 8
Crittografia 8
Sicurezza fisica e ambientale 8
Sicurezza delle Operazioni 9
Sicurezza delle Comunicazioni 9
Acquisizione, sviluppo e manutenzione dei sistemi 9
Relazioni con i Fornitori ICT 9
Gestione degli Incidenti di Sicurezza delle Informazioni 10
Sicurezza nella Continuità Operativa 10
Compliance e Audit 10

AMBITO DI APPLICAZIONE 11

REVISIONI 11

Sicurezza delle Informazioni

SCOPO

Le presenti linee guida individuano gli obiettivi e i principi generali cui si ispira Italmobiliare S.p.A. per il trattamento e la protezione delle informazioni nell'ambito della propria organizzazione, con l'obiettivo di supportare le esigenze del business, favorire il rispetto delle disposizioni legali e regolamentari applicabili e orientare le scelte aziendali in materia di gestione dei rischi secondo criteri coerenti con le best practice di settore.

Un livello non adeguato di sicurezza delle informazioni può infatti determinare impatti reputazionali, economici e competitivi, connessi anche al fermo delle attività, all'eventuale applicazione di penali o sanzioni e, più in generale, al mancato presidio delle normative vigenti.

I requisiti di sicurezza delle informazioni sono pertanto finalizzati a ricondurre entro livelli accettabili i rischi legati alla gestione delle informazioni.

Il presente documento si propone quale riferimento di indirizzo generale per la gestione della Sicurezza delle Informazioni di Italmobiliare S.p.A. Le società del Gruppo possono considerare i principi e le best practice ivi richiamati nell'ambito della propria autonomia organizzativa e decisionale; la definizione, l'approvazione e l'attuazione delle relative misure restano di esclusiva competenza degli organi di ciascuna società.

OBIETTIVI

Le presenti linee guida intendono fornire un riferimento di indirizzo per l'adozione di strumenti, misure e comportamenti orientati a:

- Supportare la strategia aziendale, valorizzando la sicurezza delle informazioni quale fattore abilitante per il business;
- Salvaguardare il patrimonio di Italmobiliare S.p.A., anche sotto il profilo finanziario, fisico, reputazionale e della proprietà intellettuale;
- Assicurare disponibilità, riservatezza e integrità delle informazioni trattate;
- Garantire il rispetto della normativa vigente e degli impegni assunti verso terze parti;
- Favorire la continuità dei servizi mediante l'applicazione di procedure di sicurezza adeguate;
- Promuovere la consapevolezza di dipendenti, collaboratori e terze parti rispetto alle rispettive responsabilità;
- Agevolare la corretta classificazione e protezione delle informazioni gestite;
- Assicurare accessi sicuri a informazioni, sedi e locali aziendali;
- Prevenire, classificare, gestire e comunicare tempestivamente anomalie, vulnerabilità e incidenti che possano incidere sui sistemi informativi o sui livelli di sicurezza aziendale.

PRINCIPI E REQUISITI DI SICUREZZA

Al fine di tutelare il patrimonio aziendale, le linee guida richiamano i seguenti **Requisiti di Sicurezza** come riferimenti di indirizzo:

- **Riservatezza**: è opportuno che le informazioni siano accessibili ai soli soggetti autorizzati.
- **Integrità**: è buona prassi salvaguardare completezza, accuratezza e conformità delle informazioni lungo il loro intero ciclo di vita.
- **Disponibilità**: è opportuno favorire, per i soggetti autorizzati e quando necessario, l'accesso alle informazioni e agli strumenti tecnologici necessari per gestirle, consultarne il contenuto e garantirne la continuità di utilizzo.

Le linee guida richiamano inoltre i seguenti **Principi** come riferimenti utili per orientare le scelte organizzative e tecniche:

- **Need to Know**: l'accesso dovrebbe essere limitato alle sole informazioni necessarie allo svolgimento della mansione assegnata.
- **Segregation of Duties**: è opportuno suddividere le attività all'interno dei processi aziendali in modo da contribuire alla prevenzione di frodi o errori.
- **Least Privilege Access**: è raccomandabile concedere il minimo insieme di privilegi necessario, in termini di accesso a sistemi e informazioni, per l'esecuzione delle attività dell'utente.
- **Security by Design**: è buona prassi considerare le potenziali vulnerabilità e le relative misure di mitigazione sin dalla progettazione di soluzioni e processi, nonché nelle successive fasi di definizione e implementazione.
- **Security by Default**: è opportuno adottare, come impostazione predefinita, misure di sicurezza e configurazioni adeguate al livello di rischio e coerenti con le opzioni più sicure disponibili.

Italmobiliare S.p.A., nell'ambito della propria organizzazione si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutte le risorse informative fisiche ed elettroniche di propria competenza.

Cyber Security

A seguire vengono riportati gli elementi di buona prassi in ogni ambito rilevante ai fini della sicurezza informatica cui ogni società del Gruppo può ispirarsi, quale riferimento non vincolante, nella definizione delle proprie strategie di cyber security secondo best practices di settore e garantendo il pieno presidio delle obbligazioni previste dalla normativa vigente di riferimento.

PROCEDURE E REGOLAMENTI INTERNI DI SICUREZZA DELLE INFORMAZIONI

Definire e mantenere processi, ruoli e responsabilità chiari in materia di sicurezza delle informazioni, supportati da documentazione aggiornata, preferibilmente approvata dagli organi competenti e oggetto di monitoraggio periodico.

ORGANIZZAZIONE DELLA SICUREZZA

Promuovere la definizione di ruoli e responsabilità chiari, favorendo la separazione delle attività potenzialmente in conflitto, quali richiesta, approvazione, esecuzione e controllo. Ove necessario, inoltre, individuare referenti per i rapporti con autorità competenti e gruppi di interesse, nonché mantenere un presidio continuativo sulle minacce rilevanti, attraverso attività di intelligence di livello strategico, tattico e operativo.

SICUREZZA DEI PROGETTI

Considerare la sicurezza delle informazioni fin dalle fasi iniziali di progettazione di soluzioni, processi e iniziative, anche attraverso l'identificazione preventiva dei rischi e la definizione dei requisiti di sicurezza applicabili. Tale approccio può costituire un utile riferimento anche per i progetti che prevedono il coinvolgimento di fornitori esterni, prevedendo, ove opportuno, specifiche clausole contrattuali in materia di sicurezza. Qualora emergano rischi significativi, valutare la predisposizione di un piano di protezione dedicato, volto a definire le misure di mitigazione, le responsabilità e le modalità di monitoraggio nel corso del progetto.

REMOTE WORKING

Individuare misure di sicurezza specifiche per il lavoro a distanza, volte a fornire indirizzi su obblighi e divieti applicabili, modalità sicure di gestione degli accessi, utilizzo dei dispositivi aziendali, impiego di reti affidabili e protezione delle informazioni da accessi non autorizzati. Tali misure possono includere, ove applicabile, l'utilizzo di soluzioni quali VPN, cifratura e autenticazione a più fattori, nonché adeguati presidi per il backup, la revoca tempestiva dei diritti di accesso e la restituzione degli asset aziendali al termine del rapporto o quando non più necessari.

RISORSE UMANE

Promuovere processi strutturati per la selezione e lo screening dei nuovi assunti, nonché iniziative di formazione, accettazione delle policy aziendali e sottoscrizione degli accordi di riservatezza applicabili. La Funzione HR può svolgere un ruolo di indirizzo nel favorire la formazione e la consapevolezza del personale rispetto alle buone pratiche di sicurezza delle informazioni, prevedendo anche canali idonei per la segnalazione di eventuali violazioni. Le responsabilità in materia di riservatezza e tutela delle informazioni possono permanere anche successivamente alla cessazione del rapporto di lavoro, secondo quanto previsto dagli accordi e dalle disposizioni applicabili.

GESTIONE DEGLI ASSET E CLASSIFICAZIONE DELLE INFORMAZIONI

Promuovere il censimento degli asset e delle informazioni a essi associate, individuando per ciascuno requisiti, restrizioni e diritti di accesso coerenti con la relativa criticità e con il livello di classificazione applicabile. Per ogni fase del ciclo di vita dell'informazione, dalla generazione alla classificazione, condivisione, custodia, archiviazione e distruzione, individuare misure di sicurezza adeguate, quali protezione tramite password, custodia sicura, crittografia e cancellazione sicura, al fine di favorire un presidio coerente e continuativo delle informazioni trattate.

Di seguito sono richiamate alcune buone prassi per la definizione dei principali presidi tecnici.

Classificazione delle Informazioni

Adottare una tassonomia di classificazione articolata su più livelli, definiti in funzione della sensibilità delle informazioni e del potenziale impatto derivante da accessi, utilizzi o divulgazioni non autorizzati. Le informazioni pubbliche sono destinate alla divulgazione e non richiedono particolari restrizioni. Per le informazioni interne è opportuno prevedere misure di base, quali l'accesso limitato al personale interno, l'utilizzo di strumenti aziendali e la protezione delle credenziali. Per le informazioni riservate, in ragione della loro criticità, è raccomandabile adottare misure più stringenti, tra cui accessi autorizzati, utilizzo di liste di distribuzione controllate, conservazione sicura, stampa protetta, limitazione dell'archiviazione su dispositivi non approvati e cifratura. Le informazioni strettamente riservate, aventi rilevanza strategica o privilegiata, possono essere gestite con presidi rafforzati, quali condivisione limitata a specifiche liste di utenti, utilizzo di sistemi aziendali sicuri, tracciamento degli accessi, clausole di riservatezza e interventi di manutenzione autorizzati.

Utilizzo degli Asset Aziendali

Definire regole di comportamento e indicazioni specifiche per l'utilizzo degli asset aziendali e delle informazioni, al fine di favorirne un impiego corretto, sicuro e coerente con le finalità lavorative. In particolare, prevedere la limitazione della divulgazione non autorizzata di informazioni, dell'invio o della gestione di documenti illeciti, della disattivazione dei presidi antivirus, dell'installazione di software non autorizzato, nonché dell'utilizzo non consentito dei social media e di servizi di file sharing non approvati.

Credenziali e Password

Definire regole per l'assegnazione, l'utilizzo, la scelta e il rinnovo delle password, prevedendo criteri di complessità adeguati e modalità di gestione coerenti con il livello di rischio associato agli account e ai sistemi interessati. Inoltre, prevedere la modifica tempestiva delle password in caso di sospetta compromissione, nonché l'utilizzo di meccanismi di autenticazione forte per l'accesso ad applicazioni, sistemi o servizi di particolare rilevanza strategica.

Strumenti di Collaborazione e di Comunicazione

Privilegiare l'utilizzo di strumenti aziendali approvati per le attività di collaborazione e comunicazione, al fine di favorire adeguati livelli di sicurezza, controllo e protezione delle informazioni condivise. Promuovere attività di formazione e sensibilizzazione sull'uso sicuro della posta elettronica e dei servizi di collaborazione elettronica, anche con riferimento ai rischi connessi a phishing, condivisione non autorizzata di informazioni e utilizzo improprio degli strumenti disponibili. Ove opportuno, adottare soluzioni di Data Loss Prevention, volte a prevenire la divulgazione non autorizzata o accidentale di dati e informazioni aziendali.

Protezione da Malware

Adottare misure di protezione contro i malware, comprendenti soluzioni antivirus, filtri antispam, firewall e attività di formazione e sensibilizzazione volte a rafforzare la capacità degli utenti di riconoscere minacce, messaggi sospetti e siti potenzialmente malevoli. Definire indicazioni per la gestione di comunicazioni, allegati o collegamenti non attendibili, prevedendo, tra l'altro, la raccomandazione di non aprire o interagire con tali contenuti, al fine di ridurre il rischio di infezioni, compromissioni dei sistemi o accessi non autorizzati alle informazioni aziendali.

Software Consentiti

Prevedere l'utilizzo esclusivo di software autorizzato, attraverso processi controllati di installazione, configurazione e aggiornamento. Inoltre, limitare l'installazione non autorizzata di software di qualsiasi tipo, al fine di ridurre il rischio di introduzione di applicazioni non approvate, vulnerabilità tecniche o componenti potenzialmente dannose per la sicurezza dei sistemi e delle informazioni aziendali.

Accesso a Internet e Navigazione Sicura

Valutare l'implementazione di sistemi di web filtering e altre misure di controllo della navigazione, al fine di ridurre l'esposizione a contenuti malevoli, siti non affidabili o utilizzi non coerenti con le finalità aziendali. Si suggeriscono inoltre attività di sensibilizzazione rivolte agli utenti, finalizzate a rafforzare la consapevolezza sui rischi connessi all'accesso a Internet, inclusi possibili danni ai sistemi e alle informazioni aziendali, nonché eventuali responsabilità personali derivanti da comportamenti non conformi.

Accesso da remoto

Adottare misure di sicurezza specifiche per l'accesso da remoto, finalizzate a proteggere le informazioni aziendali durante la connessione a sistemi, applicazioni e servizi al di fuori della rete aziendale. Tali misure possono includere, ove applicabile, l'utilizzo di canali cifrati, soluzioni VPN e meccanismi di autenticazione forte, nonché indicazioni sull'uso sicuro delle reti pubbliche o non controllate, al fine di ridurre il rischio di accessi non autorizzati, intercettazioni o compromissioni delle informazioni trattate.

Gestione dispositivi mobili

Definire regole per la configurazione, l'inventario e la gestione dei dispositivi mobili, includendo, ove applicabile, funzionalità di gestione remota, backup, cifratura dei dispositivi portatili e misure di protezione dei dati aziendali. Inoltre, disciplinare le condizioni e le modalità di eventuale utilizzo di dispositivi personali secondo modelli BYOD, favorendo adeguati livelli di sicurezza, controllo e separazione tra informazioni aziendali e personali.

Social Network e Intelligenza Artificiale

Definire regole per l'utilizzo responsabile dei social network aziendali e degli strumenti di intelligenza artificiale, al fine di prevenire la divulgazione non autorizzata di informazioni riservate e favorire un impiego coerente con i principi di sicurezza, correttezza e responsabilità. In particolare, evitare l'inserimento di dati aziendali sensibili o riservati in soluzioni di intelligenza artificiale non approvate, prevedendo al contempo un utilizzo etico e consapevole di tali strumenti e forme adeguate di supervisione umana sui contenuti generati o elaborati.

Gestione Data Breach, Furto, Smarrimento

Definire procedure per la gestione di data breach, furti e smarrimenti, al fine di favorire una tempestiva segnalazione degli eventi, una risposta coordinata e una corretta valutazione degli impatti. Tali procedure possono disciplinare le modalità di denuncia, l'eventuale attivazione degli adempimenti previsti dal GDPR e dai regolamenti interni, nonché il coinvolgimento delle funzioni competenti per la gestione delle attività di analisi, comunicazione e mitigazione del rischio.

- **Controlli e Azioni Disciplinari**

Prevedere sistemi di monitoraggio della sicurezza, nel rispetto dei principi di trasparenza, proporzionalità e minimizzazione, al fine di rilevare eventuali comportamenti anomali, violazioni o utilizzi non conformi delle risorse aziendali. In caso di violazioni gravi o reiterate delle regole di sicurezza, può essere valutata l'introduzione di opportune azioni disciplinari, secondo quanto previsto dalla normativa applicabile, dai contratti di lavoro e dai regolamenti interni.

- **Trattamento dati utenti e Record Retention**

Conservare i dati relativi agli utenti per un periodo limitato e proporzionato rispetto alle finalità del trattamento, nel rispetto dei criteri di data retention definiti e della normativa applicabile in materia di protezione dei dati personali. Inoltre, prevedere modalità di gestione, archiviazione e cancellazione coerenti con i principi di minimizzazione, limitazione della conservazione e sicurezza delle informazioni trattate.

- **Consapevolezza della Sicurezza Informatica**

Prevedere attività periodiche di formazione, aggiornamento e sensibilizzazione rivolte ai dipendenti sui principali temi di sicurezza informatica, al fine di rafforzare la consapevolezza dei rischi e promuovere comportamenti coerenti con le policy aziendali. Tali attività possono includere campagne di phishing simulato, comunicazioni informative, materiali di approfondimento e iniziative mirate a favorire il riconoscimento delle minacce e la corretta gestione delle informazioni aziendali.

CONTROLLO ACCESSI

Definire processi strutturati per la gestione degli accessi logici e fisici, favorendo il corretto governo delle identità digitali, l'assegnazione e la verifica periodica dei diritti di accesso, nonché il presidio delle utenze privilegiate. Inoltre, prevedere, ove applicabile, meccanismi di autenticazione forte e sistemi di tracciamento delle azioni rilevanti, al fine di contribuire alla protezione delle informazioni, dei sistemi e degli ambienti aziendali da accessi non autorizzati.

CRITTOGRAFIA

Definire regole per la cifratura dei dispositivi, delle informazioni e dei canali di comunicazione, in misura proporzionata al livello di classificazione e criticità delle informazioni trattate. Inoltre, gestire le chiavi crittografiche secondo criteri riconosciuti, assicurandone protezione, disponibilità e controllo lungo l'intero ciclo di vita. Ove necessario, si raccomanda infine l'utilizzo di firme digitali o altri meccanismi equivalenti per favorire autenticità, integrità e non ripudio delle informazioni e delle transazioni rilevanti.

SICUREZZA FISICA E AMBIENTALE

Adottare misure di sicurezza fisica e ambientale volte a proteggere gli asset informatici e gli spazi in cui essi sono collocati, attraverso controlli di accesso fisico, monitoraggio delle aree sensibili, regole di Clean Desk e Clear Screen e presidi contro minacce ambientali, eventi accidentali e disastri. Tali misure possono inoltre disciplinare, ove applicabile, la protezione degli asset utilizzati fuori sede e lo smaltimento sicuro delle apparecchiature, al fine di contribuire alla prevenzione di accessi non autorizzati, danneggiamenti, perdite di disponibilità o indebita esposizione delle informazioni.

SICUREZZA DELLE OPERAZIONI

Presidiare la sicurezza delle operazioni mediante misure organizzative e tecniche volte a favorire il corretto funzionamento, la protezione e la continuità delle risorse informatiche. In particolare, prevedere procedure operative formalizzate e aggiornate per l'utilizzo sicuro delle risorse aziendali, processi strutturati di gestione dei cambiamenti e delle configurazioni, attività continuative di monitoraggio della capacità, presidi per la protezione da malware e aggiornamento dei sistemi, nonché procedure di backup, logging e monitoraggio degli eventi rilevanti. Inoltre, regolamentare l'installazione del software, la gestione delle vulnerabilità tecniche, il patch management, la cancellazione sicura delle informazioni e l'eventuale utilizzo di tecniche di data masking negli ambienti non produttivi, valutando infine l'adozione di misure idonee a prevenire la fuga di dati attraverso strumenti di classificazione, DLP, firewall, antivirus e sistemi di rilevazione delle intrusioni.

SICUREZZA DELLE COMUNICAZIONI

Presidiare la sicurezza delle comunicazioni mediante misure tecniche e organizzative volte a proteggere le reti aziendali, i servizi di comunicazione e le informazioni trasferite o condivise. Tali misure possono favorire adeguati livelli di controllo, riservatezza e tracciabilità, includendo, ove applicabile, la gestione e il monitoraggio delle reti aziendali, la segregazione logica, l'utilizzo di firewall e soluzioni di network access control, nonché presidi per la gestione sicura dei servizi di rete. Inoltre, adottare strumenti di web filtering, iniziative di sensibilizzazione sull'uso responsabile di Internet, indicazioni per il trasferimento sicuro delle informazioni in formato digitale, fisico o verbale e specifici accordi di riservatezza per la protezione delle informazioni classificate.

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI

Gestire l'acquisizione, lo sviluppo e la manutenzione dei sistemi integrando i requisiti di sicurezza lungo l'intero ciclo di vita delle applicazioni e delle infrastrutture, dalla fase di analisi e definizione dei requisiti fino alle attività di sviluppo, test, rilascio, manutenzione ed evoluzione. In tale ambito, individuare i requisiti di sicurezza sulla base di una valutazione del rischio, applicare i principi di Security by Design fin dalle fasi iniziali e favorire la separazione degli ambienti di sviluppo, test e produzione. Inoltre, disciplinare lo sviluppo sicuro attraverso procedure definite, anche quando affidato a fornitori esterni, prevedendo, ove opportuno, test di sicurezza, utilizzo di repository sicuri e misure di protezione dei dati negli ambienti di test, quali tecniche di data masking.

RELAZIONI CON I FORNITORI ICT

Gestire i rapporti con i fornitori ICT attraverso processi strutturati di selezione, contrattualizzazione, monitoraggio e revisione, favorendo una chiara definizione di ruoli e responsabilità, l'accettazione di requisiti di sicurezza estesi all'intera filiera ICT e il controllo periodico del rispetto degli stessi, anche con riferimento ai servizi cloud. La valutazione dei fornitori può tenere conto di competenze, certificazioni, capacità di garantire la continuità operativa, diritto di audit, nonché requisiti etici e di sostenibilità. Inoltre, disciplinare nei contratti la prevenzione e gestione degli incidenti di sicurezza, il trattamento e la protezione dei dati, gli obblighi di riservatezza, la gestione delle sub-forniture, l'eventuale applicazione di penali e le modalità di dismissione del rapporto, incluse restituzione dei dati e cancellazione sicura.

GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI

Supportare la gestione degli incidenti di sicurezza delle informazioni con un processo strutturato, volto a favorire l'individuazione tempestiva degli eventi, la corretta valutazione della loro gravità e il coordinamento delle attività di risposta, ripristino e chiusura. A tal fine, individuare chiaramente il referente per la gestione degli incidenti e, ove necessario, un gruppo di risposta dedicato, nonché definire ruoli, responsabilità e modalità di segnalazione rapida degli eventi. Gli incidenti possono essere valutati e classificati in base a priorità e impatto, gestiti secondo fasi predefinite, tracciati mediante appositi registri e trattati con adeguati livelli di riservatezza, anche attraverso l'utilizzo di canali sicuri e specifiche responsabilità per il personale coinvolto. Le evidenze raccolte e le lezioni apprese possono infine costituire un riferimento utile per aggiornare policy, procedure e knowledge base, contribuendo al miglioramento continuo dei presidi di sicurezza.

SICUREZZA NELLA CONTINUITÀ OPERATIVA

Definire requisiti di sicurezza e continuità operativa volti a favorire la resilienza dei servizi e dei sistemi ICT, sulla base delle esigenze del business e degli esiti di eventuali Business Impact Analysis. A tal fine, sviluppare, mantenere e testare periodicamente piani di Business Continuity e Disaster Recovery, prevedendo misure di ridondanza e resilienza dei sistemi IT, quali contratti alternativi, data center separati e duplicazione dei componenti critici. La pianificazione della risposta ICT può inoltre includere la determinazione di obiettivi di ripristino coerenti, quali RTO e RPO, nonché la verifica periodica dell'efficacia delle misure adottate.

COMPLIANCE E AUDIT

Gestire le attività di compliance e audit attraverso un insieme coordinato di misure volte a favorire il rispetto dei requisiti legali, regolamentari, statutari e contrattuali applicabili, nonché la corretta protezione delle evidenze e delle registrazioni rilevanti. In tale ambito, presidiare i processi relativi alla protezione dei dati personali, alla privacy e alla proprietà intellettuale, assicurando che le modalità operative siano adeguatamente definite, comunicate e comprese dai soggetti interessati. Inoltre, prevedere audit indipendenti, controlli interni e verifiche periodiche di conformità, anche attraverso attività di vulnerability assessment e, ove opportuno, penetration test.

Ambito di applicazione

Il presente documento è adottato da Italmobiliare S.p.A. con esclusivo riferimento alla propria organizzazione e si applica unicamente al personale, ai processi, alle informazioni, agli asset, ai sistemi informativi e di rete, nonché ai fornitori di propria competenza. Nei confronti delle società controllate e partecipate esso non ha natura vincolante e costituisce unicamente uno strumento di condivisione di principi generali e di best practice di settore. Ciascuna società del Gruppo definisce, approva e attua in piena autonomia, per il tramite dei propri organi di amministrazione e delle proprie strutture, le politiche, le misure e gli investimenti in materia di sicurezza delle informazioni, e valuta autonomamente l'applicabilità nei propri confronti della normativa in materia di cybersicurezza (ivi incluso il D.lgs. 138/2024, di recepimento della Direttiva (UE) 2022/2555 – NIS 2), adempiendo in via autonoma ai relativi obblighi.

In particolare, Italmobiliare S.p.A. non adotta decisioni, né esercita influenza sulle decisioni, relative alle misure di gestione dei rischi per la sicurezza informatica delle società del Gruppo; non detiene né gestisce sistemi informativi e di rete delle società del Gruppo; non effettua per loro conto operazioni di sicurezza informatica, né fornisce loro servizi TIC o servizi di sicurezza; non esercita attività di supervisione o verifica delle misure di sicurezza informatica delle società controllate o partecipate e non impartisce piani di adeguamento o azioni correttive. Eventuali flussi informativi da e verso Italmobiliare S.p.A. per finalità societarie, finanziarie o di valutazione dell'investimento non comportano poteri di utilizzo, controllo o intervento in materia di sicurezza informatica e non incidono sull'autonomia delle società interessate.

Al fine di mantenerne nel tempo l'efficacia e l'allineamento alle evoluzioni organizzative, tecnologiche e normative, il presente documento può essere oggetto di revisione o aggiornamento periodico. Le revisioni e gli aggiornamenti del presente documento producono effetti esclusivamente all'interno dell'organizzazione di Italmobiliare S.p.A.

Revisioni

Data emissione	Redatto	Verificato	Approvato	Emesso
30/07/2026	Sistemi Informativi ITM	Sistemi Informativi ITM	Risorse Umane ITM	Risorse Umane ITM

Rev.	Data Rev.	Descrizione della revisione