ITALMOBILIARE
INVESTMENT HOLDING

# Framework di Cyber Security del Gruppo Italmobiliare

## Documento di sintesi

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

## Sommario

# Il Framework di Cyber Security

Il Gruppo Italmobiliare si è dotato di un Framework di Security Governance composto da una raccolta di documenti volti a indirizzare i principali macro-domini della sicurezza delle informazioni e della cyber security. Tale Framework mira a definire regole, misure e principi applicabili da tutte le società del gruppo, personalizzandole secondo specificità locali e di business, ma sempre coerentemente con principi e obiettivi centrali.

Il Framework dettaglia in modo strutturato e capillare tutte le policy, i processi, le regole tecniche, organizzative e comportamentali necessarie per la gestione centralizzata e diffusa della sicurezza delle informazioni e della cyber security all'interno del Gruppo Italmobiliare, secondo le migliori best practice e in conformità agli standard internazionali e alle normative vigenti.

Il programma prevede revisioni periodiche per garantire efficacia, adattabilità e attualità. È stato sviluppato per proteggere le informazioni e gli asset del gruppo, minimizzando rischi di natura economica, reputazionale e legale, oltre che assicurare conformità normativa.

Il Framework si compone attualmente dei seguenti documenti:

- Politica sulla Sicurezza delle Informazioni;
- Glossario;
- Regolamento sulla sicurezza delle informazioni;
- Regolamento sulla Classificazione delle informazioni e gestione degli Asset
- Regolamento per la Gestione dei Fornitori ICT
- Regolamento per la Gestione degli Incidenti di sicurezza delle informazioni

# Politica sulla Sicurezza delle Informazioni

Il primo documento del Framework è la "Politica sulla sicurezza delle informazioni".

La politica, oltre ad introdurre il Framework, ne definisce, lo scopo, i principali principi ispiratori, gli obiettivi e l'ambito di applicazione.

La "Politica sulla sicurezza delle informazioni" è riportata, nella sua interezza, nella seconda parte del presente documento.

# Glossario

Una ricca sezione di definizioni chiarisce tutti i termini chiave: da asset e amministratore di sistema a data breach, malware, endpoint, funzione ICT, GDPR, incidenti di sicurezza, KPI/KSI, least privilege access, legal entity, minaccia, misura di sicurezza, multi-factor authentication, penetration test, phishing, privacy, remote working, titolare del trattamento, utente, vulnerabilità, ecc.

# Regolamento sulla sicurezza delle informazioni

Il regolamento sottolinea il ruolo delle informazioni come asset cruciale e la gestione della sicurezza come fattore abilitante per il business. Inoltre, chiarisce che la compromissione della riservatezza, integrità e disponibilità (RID) può avere impatti critici.

Il regolamento stabilisce regole minime di sicurezza, adattabili da ogni società del gruppo secondo le proprie specificità, e si ispira agli standard internazionali (ISO/IEC 27001/27002, NIST, Framework nazionale Cybersecurity).

Ambiti della sicurezza delle informazioni trattati:

- Procedure e regolamenti interni
- Organizzazione della sicurezza
- Risorse umane
- Gestione degli asset
- Controllo accessi
- Crittografia
- Sicurezza fisica e ambientale
- Sicurezza delle operazioni
- Sicurezza delle comunicazioni
- Acquisizione, sviluppo e manutenzione dei sistemi
- Relazioni con i fornitori
- Gestione incidenti
- Continuità operativa
- Compliance

Per praticità di fruizione, al fine di approfondire alcune delle tematiche sopraelencate il regolamento si avvale dei tre documenti di approfondimento seguito elencati:

- Regolamento sulla Classificazione delle informazioni e gestione degli Asset
- Regolamento per la Gestione dei Fornitori ICT
- Regolamento per la Gestione degli Incidenti di sicurezza delle informazioni

Il regolamento è vincolante per tutte le società controllate del gruppo e può essere adottato volontariamente dalle partecipate.

A seguire vengono riportate le principali misure riportate nel regolamento e nei documenti ad esso collegati.

## Procedure e regolamenti interni di sicurezza delle informazioni

Ogni società deve implementare processi, ruoli e responsabilità chiari, documentazione aggiornata, approvata dalla direzione e monitorata periodicamente. L'analisi di efficacia delle misure di sicurezza adottate va tracciata e condivisa periodicamente con la capogruppo.

## Organizzazione della sicurezza

Devono essere identificati ruoli e responsabilità, segregate attività in conflitto (richiesta, approvazione, esecuzione, controllo), definiti contatti con autorità e gruppi di interesse, e mantenuta un'intelligence costante sulle minacce, sia strategica, sia tattica che operativa.

## Sicurezza dei progetti

La sicurezza delle informazioni deve essere considerata fin dalla progettazione, identificando rischi e requisiti, anche in collaborazione con fornitori esterni, con inclusione di specifiche clausole contrattuali di sicurezza. Se emergono rischi, va predisposto un piano di protezione specifico.

## Remote Working

Sono descritte in dettaglio le misure di sicurezza per lavoro a distanza, inclusi obblighi, divieti, gestione degli accessi e dispositivi, restrizioni di utilizzo reti non sicure, protezione delle informazioni da accessi non autorizzati, backup, revoca dei diritti di accesso, e restituzione degli asset. Vengono elencate misure tecniche come VPN, autenticazione multifattore, antivirus, cifratura, ecc.

## Risorse Umane

Definisce processi di selezione e screening dei nuovi assunti, obblighi di formazione e accettazione delle policy, accordi di riservatezza. La funzione HR deve assicurare che tutto il personale sia formato e consapevole delle buone pratiche di sicurezza, con canali per la segnalazione di violazioni. Le responsabilità possono continuare anche dopo la cessazione del rapporto di lavoro (es. accordi di riservatezza post-rapporto, trasferimento informazioni).

# Gestione degli Asset e Classificazione delle Informazioni

Ogni società deve censire asset e informazioni associate, definendo requisiti, restrizioni e diritti di accesso. Il regolamento approfondisce la gestione del ciclo di vita dell'informazione (generazione, classificazione, condivisione, custodia, archiviazione, distruzione), indicando misure per ogni fase (protezione tramite password, custodia sicura, crittografia, cancellazione sicura).

## Classificazione delle Informazioni

Viene proposta una tassonomia a quattro livelli:

- Pubbliche: Destinate alla divulgazione, nessuna restrizione.
- Interne: Necessarie alla normale operatività, la cui divulgazione non autorizzata comporta danno lieve. Misure: accesso solo agli interni, strumenti aziendali, protezione credenziali, ecc.
- Riservate: Critiche, la cui divulgazione può causare danni rilevanti. Misure più stringenti: accesso autorizzato, lista di distribuzione, conservazione sicura, stampa protetta, divieto archiviazione su dispositivi non approvati, crittografia.
- Strettamente Riservate: Di rilevanza strategica/privilegiata, la cui fuga può causare danni gravi. Misure: condivisione solo con lista utenti, sistemi aziendali sicuri, tracking, clausole di riservatezza, manutenzione autorizzata.

## Utilizzo degli Asset Aziendali

Definisce regole di comportamento e divieti per l'uso di asset e informazioni, tra cui: divieto di divulgazione non autorizzata, invio di documenti illeciti, disattivazione antivirus, installazione software non autorizzato, uso non consentito di social media e servizi di file sharing non approvati.

## Credenziali e Password

Regole rigorose per l'assegnazione, uso, scelta e rinnovo delle password, obbligo di cambio password in caso di sospetta compromissione, difesa con autenticazione forte per applicazioni strategiche.

## Strumenti di Comunicazione e DLP

Obbligo di utilizzare solo strumenti aziendali approvati, raccomandazione di soluzioni DLP, formazione sull'uso sicuro della posta elettronica e dei servizi di collaborazione elettronica.

## Protezione da Malware

Utilizzo obbligatorio di antivirus, filtri antispam, firewall, formazione sul riconoscimento di minacce, divieto di apertura di mail/siti sospetti.

## Software Consentiti/Installazione

Solo software autorizzato e processi rigorosi di installazione e aggiornamento, divieto di installazione non autorizzata di software di qualsiasi tipo.

## Accesso a Internet e Navigazione Sicura

Implementazione di sistemi di web filtering, sensibilizzazione sul rischio di danni e responsabilità personali.

## Accesso da remoto

Richiesta di protezione delle informazioni attraverso crittografia, autenticazione forte, VPN, attenzione all'utilizzo di reti pubbliche.

## Gestione dispositivi mobili, BYOD

Regole per configurazione, inventario, gestione remota, backup, crittografia dispositivi portatili, divieto di uso BYOD salvo esplicita autorizzazione.

## Social Network e Intelligenza Artificiale

Norme per uso responsabile di social network aziendali, vietando divulgazione di informazioni riservate. Suggerimenti sull'uso etico e responsabile di AI, divieto assoluto di inserimento di dati aziendali sensibili in soluzioni AI non approvate, obbligo di supervisione umana.

## Gestione Data Breach, Furto, Smarrimento

Procedure dettagliate per la segnalazione, risposta, valutazione, denuncia ed eventuale avvio delle procedure previste da GDPR e regolamenti interni.

## Controlli e Azioni Disciplinari

Previsione di sistemi di monitoraggio della sicurezza, rispetto dei principi di trasparenza e proporzionalità, possibili azioni disciplinari in caso di violazione reiterata o grave.

## Trattamento dati utenti e Record Retention

Conservazione limitata nel tempo dei dati trattati, rispetto dei criteri di data retention e delle normative privacy.

### Consapevolezza della Sicurezza Informatica

Formazione e aggiornamento dei dipendenti su temi di sicurezza, campagne di phishing simulato, materiale informativo.

## Controllo Accessi

Definizione di processi per regolamentare accessi logici e fisici, gestione delle identità, periodica verifica dei diritti di accesso, gestione delle utenze privilegiate, obbligo di autenticazione forte e logging delle azioni chiave.

## Crittografia

Adozione di regole per cifratura dei dispositivi e canali di comunicazione proporzionate al livello di classificazione delle informazioni, gestione chiavi secondo best practice e utilizzo di firme digitali per autenticità, integrità e non ripudio.

## Sicurezza fisica e ambientale

Protezione dello spazio fisico degli asset informatici, controlli di accesso fisico, monitoraggio aree sensibili, protezione contro minacce ambientali e disastri, gestione della sicurezza degli asset fuori sede e smaltimento sicuro delle apparecchiature.

### Regole di Clean Desk e Clear Screen

Politiche per mantenere libere le scrivanie e protetti i dispositivi, archiviazione sicura di documenti e supporti rimovibili, stampa protetta, cancellazione dati da lavagne e altri strumenti di visualizzazione.

## Sicurezza delle Operazioni

- Procedure documentate per uso sicuro e corretto delle risorse informatiche.
- Gestione del cambiamento e delle configurazioni.
- Gestione della capacità delle risorse.
- Protezione contro i malware e aggiornamento costante dei sistemi.
- Procedure di backup, test e conservazione sicura delle copie.
- Logging e monitoraggio degli eventi rilevanti, sincronizzazione degli orologi di sistema.
- Installazione software solo da personale autorizzato.
- Gestione delle vulnerabilità tecniche tramite assessment e patch management.
- Cancellazione sicura delle informazioni e data masking per test/ambienti non produttivi.
- Prevenzione della fuga di dati tramite soluzioni come classificazione, DLP, firewall, antivirus e IDS.

## Sicurezza delle Comunicazioni

- Gestione e controllo delle reti aziendali, segregazione tramite VLAN, uso di firewall e network access control.
- Gestione sicura dei servizi di rete, logging delle attività di fruizione dei servizi.
- Web filtering e sensibilizzazione sull'uso responsabile di Internet.
- Regole per il trasferimento di informazioni (digitale, fisica, verbale).
- Accordi di riservatezza per la protezione delle informazioni classificate.

## Acquisizione, sviluppo e manutenzione dei sistemi

- Definizione dei requisiti di sicurezza delle applicazioni e dei sistemi, determinati tramite valutazione del rischio.
- Applicazione dei principi di Security by Design e separazione degli ambienti di sviluppo/test/produzione.
- Gestione dello sviluppo sicuro, anche in outsourcing, test di sicurezza, uso di repository sicuri, valutazione di data masking per ambienti di test.

## Relazioni con i Fornitori ICT

Il regolamento disciplina la selezione, la contrattualizzazione, il monitoraggio e la revisione dei fornitori ICT, includendo:

- Definizione di ruoli e responsabilità (referente, asset owner, coordinatore privacy, ecc).
- Requisiti di sicurezza da accettare da parte dei fornitori, estesi all'intera filiera ICT.
- Monitoraggio delle variazioni nei rapporti, rispetto dei requisiti di sicurezza anche per servizi cloud.
- Valutazione dei fornitori in base a competenze, certificazioni (ISO 27001, 27017, 27018, 27701, CSA STAR, ecc.), capacità di gestione della continuità operativa, diritto di audit, requisiti etici e di sostenibilità.
- Negoziazione e formalizzazione dei contratti includendo regole per la prevenzione degli incidenti di sicurezza, gestione dei dati, standard di riservatezza, gestione delle sub-forniture, diritto di audit, penali, e regole di dismissione (restituzione dati, cancellazione sicura, ecc).

## Gestione degli Incidenti di Sicurezza delle Informazioni

- Identificazione di un referente e di eventuale gruppo di risposta agli incidenti (con competenze ICT e di sicurezza).
- Definizione di regole interne, ruoli e responsabilità, e metodi per la segnalazione rapida degli eventi di sicurezza.
- Metodo di valutazione e classificazione degli incidenti per priorità e impatto (Grave, Alto, Medio, Basso), con descrizione di impatto e urgenza.

- Dettaglio delle fasi di gestione degli incidenti: identificazione, analisi, classificazione, escalation, risposta e ripristino, chiusura e lesson learned.
- Tracciamento incidenti tramite Track Record che include dettagli come data, descrizione, azioni intraprese, escalation, chiusura, root cause analysis.
- Gestione riservata delle informazioni sugli incidenti, uso di canali sicuri, responsabilità del personale coinvolto, possibili accordi di riservatezza specifici.
- Lezioni apprese dagli incidenti e aggiornamento delle policy e della knowledge base.

## Sicurezza nella Continuità Operativa

Definizione dei requisiti per la continuità operativa, sviluppo e test di piani di Business Continuity, Disaster Recovery, ridondanza dei sistemi IT (contratti multipli, data center separati, duplicazione componenti hardware, ecc). Pianificazione della risposta ICT e determinazione di RTO/RPO in base a Business Impact Analysis.

## Compliance e Audit

- Identificazione, aggiornamento e rispetto dei requisiti legali, regolamentari, statutari e contrattuali, inclusi privacy e proprietà intellettuale.
- Protezione delle evidenze e delle registrazioni, inclusa la gestione della catena di custodia e la categorizzazione delle registrazioni.
- Processi per la protezione dei dati personali (GDPR) e comunicazione efficace dei processi a tutti gli interessati.
- Audit indipendenti e interni sulla sicurezza delle informazioni. Obbligo di test periodici di conformità (vulnerability management e penetration test).
- Protezione dei sistemi informativi durante attività di test e audit tramite strumenti adeguati, logging e conformità contrattuale.

ITALMOBILIARE
INVESTMENT HOLDING

# POLITICA SULLA SICUREZZA DELLE INFORMAZIONI

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

# POLITICA SULLA SICUREZZA DELLE INFORMAZIONI

## INDICE

# Introduzione

Italmobiliare S.p.A. (di seguito "Italmobiliare" o "la Holding") ha definito un programma di interventi finalizzati a formalizzare un *Framework di Security Governance*, con valenza sia per Italmobiliare che per le società controllate e partecipate (di seguito complessivamente "il Gruppo Italmobiliare o Gruppo), che abbia lo scopo di proteggere in maniera adeguata le informazioni e gli asset aziendali. Gli obiettivi sono quelli di indirizzare le regole e le misure di base, nell'ambito dei macro-domini di information e cyber security, da osservare in tutte le iniziative condotte dalle Legal Entity (di seguito "LE")[1] del Gruppo.

In tale contesto la Holding, nel rispetto del suo ruolo di Governance, definisce l'indirizzo strategico mentre le singole LE del Gruppo analizzano e contestualizzano a livello locale, in maniera potenzialmente differente a seconda delle relazioni che intercorrono con la Holding (ad es. in funzione che si tratti di una società controllata oppure di una partecipata) e delle specificità di business, le regole definite, fornendo periodicamente monitoraggio sullo stato del Sistema di Sicurezza delle Informazioni.

Il **Framework di Security Governance** è un insieme di documenti che hanno l'obiettivo di indirizzare i macro-domini di sicurezza / cyber security (es. obiettivi di sicurezza, gestione degli asset, classificazione delle informazioni, governo delle utenze, sviluppo sicuro, governo dei fornitori ICT, gestione degli incidenti, continuità operativa, etc.). Ogni LE deve adottare le indicazioni in essi contenute declinandole secondo il proprio contesto ma nel rispetto dei principi e degli obiettivi presenti nel documento.

Per garantire la sua efficacia il framework può essere soggetto a revisione o aggiornamento periodico.

## GLI IMPEGNI

La funzione che gestisce i Servizi informatici (Funzione ICT) nelle diverse società del Gruppo si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutte le risorse informative fisiche ed elettroniche. La mancanza di un adeguato livello di sicurezza delle informazioni può comportare danni reputazionali, danni di natura economica legati al fermo delle attività o al pagamento di penali, svantaggio competitivo, nonché eventuali sanzioni rispetto alle normative vigenti.

I requisiti di sicurezza delle informazioni intendono essere un meccanismo per ridurre a livelli accettabili i rischi legati alla gestione delle informazioni.

[1] Legal Entity, intese come le Società controllate dalla Holding e le Società nelle quali Italmobiliare possiede delle partecipazioni.

# Scopo

La presente policy ha lo scopo di descrivere gli obiettivi e i principi generali che il Gruppo deve adottare nel trattamento delle informazioni al fine di supportare le esigenze del business e di garantire il rispetto di prescrizioni legali o regolamentari e delle scelte in materia di gestione dei rischi. Il documento costituisce normativa d'indirizzo per il supporto alla Gestione della Sicurezza delle Informazioni all'interno del Gruppo.

## I PRINCIPI E I REQUISITI DI SICUREZZA

Al fine di tutelare il patrimonio aziendale la policy prevede l'adozione dei **Requisiti di Sicurezza** enunciati qui di seguito:

1 **Riservatezza**: l'informazione deve essere disponibile solo a coloro che ne sono autorizzati.

2 **Integrità**: occorre salvaguardare la completezza, l'accuratezza e la conformità dell'informazione durante l'intero ciclo di vita della stessa.

3 **Disponibilità**: è necessario assicurare l'accesso alle informazioni ed agli elementi architetturali associati a coloro che sono autorizzati e quando ne fanno richiesta.

Inoltre, prevede l'adozione dei seguenti **Principi**:

4 **Need to Know**, occorre limitare l'accesso alle sole informazioni alle quali l'utente ha necessità di accedere per l'espletamento della mansione a cui è assegnato.

5 **Segregation of Duties**, è opportuno suddividere le attività all'interno di un processo aziendale per evitare frodi o errori.

6 **Least Priviledge Access**, occorre concedere il minimo insieme di privilegi possibile (accessi a sistemi ed informazioni) per l'esecuzione dell'attività dell'utente.

7 **Security by Design**, sin dalla fase di progettazione di una soluzione, così come nelle successive fasi di definizione e di implementazione, occorre prendere in considerazione le potenziali vulnerabilità e le misure di sicurezza atte a mitigarle.

8 **Security by Default**, occorre determinare e scegliere, "per impostazione predefinita", le misure di sicurezza e le impostazioni di configurazione più sicure possibili.

# Obiettivi

La presente Policy di Sicurezza delle Informazioni si pone l'obiettivo, per mezzo dei principi definiti nel Framework di Security Governance, di indirizzare e fornire gli strumenti per:

a. Supportare la strategia aziendale rendendo la sicurezza delle informazioni uno dei fattori chiave per il successo del business;
b. Salvaguardare il patrimonio del Gruppo nei suoi aspetti finanziari, fisici, di proprietà intellettuale e di reputazione e garantire la disponibilità, la riservatezza e la correttezza delle informazioni trattate;
c. Rispettare la conformità con le normative vigenti e con gli impegni di sicurezza stabiliti nei contratti con le terze parti;
d. Garantire la continuità dei servizi attraverso l'applicazione di procedure di sicurezza stabilite;
e. Assicurare che i dipendenti, i collaboratori e le terze parti siano ben informati sulle pratiche di sicurezza delle informazioni e che siano consapevoli delle loro responsabilità in tale ambito;
f. Consentire il raggiungimento della piena conoscenza delle informazioni gestite e valutarne la criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
g. Garantire l'accesso sicuro alle informazioni, alle sedi ed ai singoli locali aziendali in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari;
h. Prevenire, classificare, gestire e comunicare correttamente eventuali anomalie, vulnerabilità e incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale.

## AMBITO DI APPLICAZIONE

La presente Politica si applica a tutti i processi e a tutte le risorse, umane e asset strumentali (anche esterne), coinvolti nella gestione delle informazioni trattate dal Gruppo Italmobiliare.

In particolare, i destinatari del documento sono:

1. I livelli direttivi delle Società del Gruppo, che adottano la Policy e assicurano un adeguato commitment e le risorse necessarie per consentire l'effettiva attuazione dei principi ivi definiti;
2. I dipendenti del Gruppo che hanno il compito di attuare quanto definito nella presente Politica, ciascuno per gli ambiti di propria competenza:
   - I dipendenti delle società controllate da Italmobiliare Investment Holding, in maniera vincolate;
   - I dipendenti delle società partecipate, sotto forma di indirizzo strategico / linee guida;
3. Le terze parti che, nell'ambito di rapporti con le Società del Gruppo, hanno la possibilità di accedere al patrimonio informativo aziendale.

# Revisioni

| Data emissione | Redatto | Verificato | Approvato | Emesso |
|---|---|---|---|---|
| 01/12/2023 | Sistemi Informativi ITM | Sistemi Informativi ITM | Risorse Umane ITM | Risorse Umane ITM |

| Rev. | Data Rev. | Descrizione della revisione |
|---|---|---|
| | | |
| | | |
| | | |