Policy

Cyber Security

INDICE

1. SCOPO 3
2. AMBITO DI APPLICAZIONE 3
3. RIFERIMENTI 3
4. IMPEGNO E PRINCIPI GENERALI 4
5. OBIETTIVI DI SICUREZZA 5
6. ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA 5
6.1. MODELLO ORGANIZZATIVO DI CYBER SECURITY 6
7. RESPONSABILITÀ E AGGIORNAMENTO 8

1. SCOPO

Il Gruppo Fincantieri (di seguito anche "Fincantieri" o il "Gruppo") considera la sicurezza informatica un elemento strategico per la creazione e la protezione del valore aziendale. Essa contribuisce alla tutela del patrimonio informativo, alla resilienza e continuità delle operazioni, alla protezione degli interessi del business e alla salvaguardia della reputazione del Gruppo. La disciplina rappresenta inoltre un presupposto fondamentale per il rispetto degli obblighi normativi che regolano a livello internazionale e nazionale la protezione dei diritti e delle libertà fondamentali delle persone, assicurando la riservatezza, l'integrità e la disponibilità delle informazioni, dei dati e dei servizi del Gruppo.

In un contesto caratterizzato dalla progressiva convergenza tra tecnologie digitali, sistemi produttivi e catene del valore, nonché da un panorama di minacce informatiche in continua evoluzione, la corretta gestione del rischio cyber assume una rilevanza crescente per il perseguimento degli obiettivi strategici e operativi del Gruppo. In tale scenario, il Gruppo adotta un approccio strutturato, sistemico, esteso all'intero ecosistema digitale e alla filiera tecnologica, in coerenza con gli standard e le migliori pratiche riconosciute a livello internazionale.

La presente Policy stabilisce quindi i principi fondamentali e gli obiettivi di governance della sicurezza informatica del Gruppo, delineando il modello di controllo interno e di gestione dei rischi e le misure organizzative, procedurali e tecnologiche adottate per prevenire, rilevare, contrastare e gestire le minacce informatiche e i relativi rischi.

2. AMBITO DI APPLICAZIONE

La presente Policy si applica a Fincantieri S.p.A. (di seguito "Fincantieri") e alle Società del Gruppo, controllate direttamente o indirettamente, con sede in Italia e all'estero.

La presente Policy è resa disponibile a tutto il personale dipendente attraverso la pubblicazione nella Intranet aziendale ed è altresì consultabile da tutti gli stakeholder tramite il sito Internet istituzionale del Gruppo Fincantieri.

3. RIFERIMENTI

La presente Policy è stata definita sulla base delle indicazioni contenute nella MG-001 "Sistema Normativo", quale riferimento normativo interno, nonché nelle seguenti fonti esterne:

- NIST Cybersecurity Framework (CSF) 2.0 (2024)
- ISO/IEC 27001:2022 – *Information Technology – Security techniques – Information security management systems – Requirements*
- ISO/IEC 27005:2022 – *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*
- Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (*General Data Protection Regulation*)
- Regolamento (UE) 2024/2847 relativo ai requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (*Cyber Resilience Act*)
- Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS2) e rispettivi decreti di recepimento a livello nazionale

- Linee guida tecniche dell'ENISA relative al regolamento di esecuzione (UE) 2024/2690 della Commissione che stabilisce le norme di applicazione della direttiva NIS2 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di sicurezza informatica (2025)
- Legge sulla sicurezza digitale (*Digital Security Act 2025*), che recepisce in Norvegia la Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS1)
- Framework Nazionale per la Cybersecurity e la Data Protection (2025)
- Legge 18 novembre 2019, n. 133 – Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e relativi decreti attuativi.

4. IMPEGNO E PRINCIPI GENERALI

Fincantieri riconosce la sicurezza informatica quale elemento essenziale per la tutela degli asset aziendali e per la continuità operativa del business e ne assicura l'integrazione nei processi core, nelle scelte strategiche del Gruppo e nelle linee di trasformazione digitale dei prodotti di riferimento.

In considerazione della propria presenza internazionale e della natura eterogenea dei contesti geografici, normativi, industriali e tecnologici in cui opera, il Gruppo promuove un approccio unitario alla sicurezza informatica, volto a garantire livelli di protezione coerenti, proporzionati al rischio e allineati agli obiettivi di business.

A tal fine, Fincantieri si impegna a:

- Assicurare che le strategie e le iniziative di sicurezza informatica supportino il perseguimento degli obiettivi di business del Gruppo, contribuendo alla difesa della propria competitività industriale e proprietà intellettuale, allo sviluppo dei prodotti, alla resilienza della filiera e alla salvaguardia della reputazione;
- Assicurare la piena conformità normativa, anche attraverso il monitoraggio costante delle evoluzioni della stessa, nel garantire la cyber resilienza del business, operando per la tutela della continuità operativa, la salvaguardia del know-how industriale e la protezione dei servizi essenziali che il Gruppo garantisce allo Stato italiano e al mercato, in qualità di system integrator in segmenti ad alto valore aggiunto della cantieristica navale, sia militare sia civile;
- Proteggere le informazioni, i dati e gli asset critici, prevenendo gli utilizzi illeciti delle tecnologie digitali e contrastando le minacce informatiche che possano compromettere la continuità operativa, il patrimonio informativo e la sicurezza dei servizi digitali, incluse le forme di abuso, manipolazione cognitiva, estorsione o coercizione digitale;
- Cooperare con le istituzioni che compongono l'architettura nazionale ed internazionale preposta a garantire la cyber resilienza nelle geografie di interesse strategico del Gruppo, favorendo uno scambio trasparente pubblico/privato finalizzato al contrasto delle forme più sofisticate di minaccia organizzata;
- Assicurare trasparenza nella gestione della cyber security, garantendo la tempestiva e completa comunicazione dei rischi, degli incidenti e delle vulnerabilità rilevanti verso gli stakeholder competenti, attraverso flussi informativi chiari, accurati, tracciati e verificabili;
- Integrare la sicurezza informatica lungo l'intero ciclo di vita dei processi, dei prodotti e dei servizi del Gruppo, promuovendo un approccio basato sulla gestione del rischio che contribuisca alla protezione del processo industriale, alla salvaguardia del valore generato per tutti gli stakeholder e al rafforzamento della resilienza e della sicurezza della filiera tecnologica e produttiva.

5. OBIETTIVI DI SICUREZZA INFORMATICA

Fincantieri persegue i seguenti obiettivi di sicurezza informatica:

- Assicurare l'esistenza di processi di identificazione, analisi, valutazione, e trattamento dei rischi cyber che possano impattare il business, gli asset critici, il know-how industriale, la reputazione e gli interessi strategici del Gruppo, incluse le minacce dirette a compromettere l'affidabilità delle informazioni, la fiducia nei processi digitali e la capacità decisionale dell'organizzazione;
- Assicurare l'adozione di misure tecniche, organizzative e procedurali proporzionali al rischio in grado preservare la riservatezza, l'integrità, la disponibilità e l'utilizzo affidabile delle informazioni, degli asset critici, dei sistemi e dei servizi essenziali per il business;
- Preservare la capacità del Gruppo di mantenere la continuità operativa delle attività aziendali e del processo industriale, prevenendo, rilevando, contenendo e gestendo efficacemente i tentativi di incursione e sabotaggio cyber;
- Promuovere l'adozione di adeguati livelli di sicurezza e resilienza per le principali piattaforme navali sviluppate dal Gruppo, anche lungo la catena di approvvigionamento, attraverso processi di qualificazione, valutazione, monitoraggio e collaborazione con fornitori, partner e terze parti, proporzionati alla criticità delle forniture;
- Favorire la tempestiva identificazione, escalation, comunicazione delle informazioni relative a rischi, vulnerabilità e incidenti di sicurezza, garantendo adeguati livelli di trasparenza, consapevolezza, coordinamento e supporto decisionale verso i soggetti competenti interni ed esterni;
- Stabilire principi, standard e controlli comuni che consentano di garantire livelli di protezione coerenti, proporzionati al rischio e progressivamente armonizzati nelle diverse Società e geografie in cui il Gruppo opera, assicurandone il periodico aggiornamento e miglioramento in funzione dell'evoluzione delle minacce, delle tecnologie e del contesto normativo.

Al fine di garantire il conseguimento degli obiettivi sopra richiamati, il Gruppo definisce e adotta, nell'ambito del proprio Sistema Normativo[1], un corpus organico di principi, policy, standard e procedure in materia di cyber security, volto a disciplinare in maniera coerente e integrata i processi, i controlli e le responsabilità connessi alla gestione della sicurezza informatica.

Le iniziative di investimento e sviluppo delle capacità di cyber security, incluse quelle relative a processi, risorse umane e soluzioni tecnologiche, assicurano la concreta attuazione di tale impianto e contribuiscono al continuo rafforzamento della capacità del Gruppo di prevenire, rilevare, contrastare e gestire le minacce informatiche più sofisticate.

6. ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA

Fincantieri definisce e adotta un modello organizzativo di cyber security volto a garantire un'efficace governance delle politiche e dei processi di sicurezza informatica, coerentemente con il contesto normativo di riferimento e con le caratteristiche organizzative del Gruppo, assicurando l'integrazione tra le esigenze operative locali e la strategia aziendale a livello globale.

Tale modello è orientato a favorire il coordinamento tra il livello centrale e le realtà locali, garantendo un presidio efficace per la sicurezza informatica e la coerenza nell'attuazione degli indirizzi strategici definiti a livello di Gruppo.

[1] Per la descrizione del Sistema Normativo di Fincantieri si rinvia al documento MG-001 – Management Guideline "Sistema Normativo".

In tale ottica, l'organizzazione per la sicurezza informatica prevede una chiara definizione e allocazione di ruoli, responsabilità e funzioni che sia adeguata, proporzionata e coerente rispetto al livello di rilevanza delle Società del Gruppo in riferimento alle tematiche di cyber security. In tale contesto, l'assetto organizzativo di dettaglio viene delineato in funzione di diversi fattori, quali il volume delle attività svolte da ciascuna Società, lo svolgimento di attività di sviluppo prodotti e soluzioni tecnologiche critiche, l'esposizione a vincoli normativi in ambito cyber security, nonché le specifiche caratteristiche organizzative e il grado di integrazione con i sistemi e le infrastrutture di Gruppo.

Il modello organizzativo complessivo in ambito cyber security è approvato e promosso dal Consiglio di Amministrazione di Fincantieri, che ne assicura e supervisiona la diffusione, la coerenza con i driver strategici aziendali, il sostegno e l'efficace attuazione nell'ambito dell'organizzazione, quale elemento fondamentale per la gestione dei rischi di cyber security a livello di Gruppo.

6.1. MODELLO ORGANIZZATIVO DI CYBER SECURITY

Il modello organizzativo di cyber security del Gruppo si fonda sulla chiara attribuzione di ruoli e responsabilità, assicurando un presidio efficace e coordinato dei rischi cyber a tutti i livelli dell'organizzazione. Tale modello si articola lungo una catena di governo che, a partire dagli organi di indirizzo strategico, individua funzioni e figure specialistiche dotate delle competenze e delle responsabilità necessarie a garantire che l'attuazione della strategia di sicurezza informatica del Gruppo sia coerente alle specificità operative delle singole realtà, nel rispetto delle accountability locali.

In tale contesto:

- Il **Consiglio di Amministrazione** di Fincantieri (CdA), esercita funzioni di indirizzo e supervisione nell'ambito delle tematiche di cyber security.

  In tale ambito, il CdA:

  - Fornisce indirizzo strategico e vigila sul modello di governance e sull'assetto organizzativo della sicurezza informatica del Gruppo;
  - Supervisiona il piano di attuazione delle misure di gestione dei rischi per la sicurezza informatica e il rispetto degli obblighi normativi applicabili, verificandone periodicamente l'efficacia e l'adeguatezza rispetto all'evoluzione del contesto di rischio, delle minacce e del quadro regolatorio di riferimento;
  - Riceve informativa periodica in merito al livello di esposizione ai rischi cyber del Gruppo, agli incidenti di sicurezza informatica più rilevanti, allo stato di attuazione delle misure di mitigazione e alle notifiche effettuate alle autorità e alle istituzioni competenti;
  - Promuove la diffusione di una cultura della sicurezza informatica, favorendo altresì iniziative di formazione e sensibilizzazione rivolte al personale;

- L'**Amministratore Delegato** di Fincantieri (AD), nell'ambito dei poteri conferiti dal CdA, svolge un ruolo di direzione, coordinamento, supervisione e attuazione delle misure di gestione dei rischi per la sicurezza informatica, definite a livello di Gruppo.

  In tale ambito, l'AD:

  - Sovrintende all'attuazione delle misure di gestione dei rischi per la sicurezza informatica, secondo i principi espressi nella presente Policy, garantendone l'integrazione nei processi aziendali e nelle attività del Gruppo;

- Assicura i flussi informativi verso gli organi di amministrazione e controllo (*i.e.* il CdA, il Comitato Controllo e Rischi e il Collegio Sindacale) con riferimento alle tematiche di cyber security e compliance di rilevanza strategica.

- Il **Chief Information Security Officer (CISO) di Gruppo**:
  - Coordina il processo di identificazione, valutazione, trattamento e monitoraggio dei rischi cyber, promuovendo l'adozione, a livello di Gruppo e filiera, delle misure necessarie alla loro mitigazione, proporzionali al livello di esposizione alla minaccia;
  - Definisce gli standard di cyber security, in coerenza agli obiettivi strategici del Gruppo, ne monitora l'attuazione e individua i criteri di rilevanza cyber per categorizzare i core business delle società controllate;
  - Assicura la disponibilità, a livello di Gruppo, di adeguate capacità di prevenzione, rilevazione, gestione e risposta agli incidenti di sicurezza informatica, anche attraverso specifici programmi di awareness;
  - Esamina periodicamente il livello di esposizione ai rischi cyber del Gruppo, l'evoluzione delle minacce e delle vulnerabilità rilevanti, formulando indirizzi, priorità di trattamento e il rafforzamento delle misure di sicurezza in ottica di miglioramento continuo;
  - Cura i rapporti di collaborazione in materia di cyber security con le autorità competenti, favorendo lo scambio informativo, le notifiche obbligatorie, il coordinamento operativo e la partecipazione alle iniziative volte al rafforzamento della resilienza cyber dei Paesi e dei settori strategici in cui il Gruppo opera;

- Gli **organi di amministrazione delle società controllate**, nell'ambito degli indirizzi, delle politiche e degli standard definiti a livello di Gruppo, supervisionano l'attuazione dei programmi di cyber security nelle rispettive realtà aziendali, anche avvalendosi, se del caso, di organi delegati. In tale contesto, gli organi amministrativi delle società controllate restano responsabili per la conformità delle rispettive società alla normativa applicabile in materia di cyber security pro tempore vigente.

- Il **CISO Locale** ha il ruolo di:
  - Assicurare l'attuazione delle misure di gestione dei rischi per la sicurezza informatica e presidiare la conformità agli obblighi normativi applicabili nella società di appartenenza;
  - Assicurare il recepimento e l'applicazione degli standard, delle politiche e dei requisiti di cyber security definiti a livello di Gruppo nella società di appartenenza e nelle società da essa controllate;
  - Costituire il punto di coordinamento locale per le iniziative e i servizi di cyber security erogati a livello di Gruppo o da terze parti, monitorandone l'efficacia e i livelli di servizio in raccordo con le competenti funzioni aziendali;
  - Assolve agli obblighi di notifica obbligatoria degli incidenti, garantendo il tempestivo flusso informativo verso la Capogruppo, in merito ai rischi cyber, agli incidenti di sicurezza, alle vulnerabilità rilevanti e allo stato di attuazione delle misure di sicurezza, nel rispetto della normativa applicabile e degli eventuali vincoli di natura regolatoria, contrattuale o di sicurezza vigenti nella geografia di riferimento.

L'allocazione di ulteriori figure specialistiche all'interno delle Società del Gruppo avviene secondo un principio di progressiva declinazione delle responsabilità, in funzione della rilevanza cyber, del profilo di rischio e delle caratteristiche organizzative delle singole realtà.

7. RESPONSABILITÀ E AGGIORNAMENTO

La Capogruppo, per il tramite del CISO di Gruppo, è responsabile del monitoraggio e del controllo della Policy "Cyber Security".

La Policy sarà sottoposta a revisioni periodiche (al verificarsi di cambiamenti rilevanti nel contesto normativo, organizzativo o tecnologico) e validata da parte del Comitato per la Sostenibilità e dal Comitato Controllo e Rischi e, al fine di garantirne l'effettiva attuazione e l'adeguatezza, sarà adattata a eventuali mutamenti del contesto esterno.

La Policy e le successive revisioni saranno oggetto di approvazione del Consiglio di Amministrazione di Fincantieri.

Versione approvata dal Consiglio di Amministrazione in data 29 luglio 2026