

ALLEGATO – ANNEX

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI INFORMATION SECURITY POLICY

Premessa

A causa di un sempre più esteso utilizzo e scambio di informazioni, e di uno sviluppo tecnologico incentrato su una crescente connettività, anche via Internet, che coinvolge sia sistemi IT che sistemi OT, le potenziali vulnerabilità ed i correlati rischi informatici aumentano conseguentemente. Da ciò la necessità di proteggersi da tali rischi e limitare la vulnerabilità dei propri sistemi. La sicurezza informatica, che si occupa di proteggere i sistemi informatici (IT/OT), i dati e le reti da accessi non autorizzati, danni o attacchi informatici, assume quindi una sempre maggior rilevanza, al fine di prevenire potenziali effetti negativi non solo sull'attività aziendale, sui suoi asset, compreso quelli navali, ma anche, estensivamente, sulla sicurezza della navigazione, sul personale e sull'ambiente.

Scopo e principi generale

La presente Politica esprime l'impegno dell'Alta Direzione di Fratelli Neri S.p.A. a proteggere le informazioni, i sistemi, le reti, le infrastrutture tecnologiche e i servizi digitali utilizzati nell'esercizio delle attività aziendali. La sicurezza delle informazioni è considerata un requisito essenziale per garantire l'affidabilità e la continuità dei servizi di rimorchio portuale, assistenza, salvataggio, recupero, delle attività connesse alla sicurezza e alla funzione di pubblico servizio, dei servizi tecnici e di assistenza alle piattaforme e/o terminal off-shore, delle attività di armamento e noleggio navi, nonché per migliorare la sicurezza della navigazione e del personale marittimo, la salvaguardia dell'ambiente e quella del carico.

La Società adotta un approccio basato sul rischio e persegue la tutela della riservatezza, dell'integrità, della disponibilità e dell'autenticità delle informazioni, unitamente alla resilienza delle reti e dei sistemi informativi. La presente Politica costituisce il quadro di riferimento per la definizione degli obiettivi di sicurezza e per il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

Campo di applicazione

La Politica si applica a tutte le informazioni comprese nel campo di applicazione del SGSI, indipendentemente dal formato, dal supporto, dal luogo di conservazione o dalle modalità di trattamento. Essa si applica al personale dipendente, agli organi societari, ai collaboratori, ai consulenti, ai fornitori e a ogni altro soggetto che acceda alle informazioni, ai sistemi o alle risorse aziendali.

I confini organizzativi, fisici, tecnologici e informativi del SGSI sono definiti nel documento relativo alla determinazione e gestione del campo di applicazione

Premise

Due to the increasingly widespread use and exchange of information, and a technological development centered on growing connectivity—including via the Internet—which involves both IT and OT systems, potential vulnerabilities and related cybersecurity risks consequently increase. Hence the need to protect against these risks and limit system vulnerability. Cybersecurity, which deals with protecting IT/OT computer systems, data, and networks from unauthorized access, damage, or cyberattacks, is therefore assuming ever-greater importance in order to prevent potential negative effects not only on business operations and assets (including maritime ones), but also, extensively, on navigation safety, on personnel and the environment.

Purpose and general principles

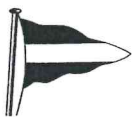
This Policy expresses the commitment of the Senior Management of Fratelli Neri S.p.A. to protect the information, systems, networks, technological infrastructure and digital services used in the conduct of business activities. Information security is considered an essential requirement to ensure the reliability and continuity of towage and port services, assistance, rescue, salvage, activities related to safety and public service functions, technical services and assistance to offshore platforms and/or terminals, ship management and chartering activities, as well as to improve the navigation safety, the safety of maritime personnel, the protection of the environment, and the security of cargo.

The Company adopts a risk-based approach and pursues the protection of the confidentiality, integrity, availability and authenticity of information, together with the resilience of networks and information systems. This Policy constitutes the framework for defining security objectives and for the continual improvement of the Information Security Management System (ISMS).

Scope

The Policy applies to all information included within the scope of the ISMS, regardless of format, medium, storage location or processing method. It applies to employees, corporate bodies, collaborators, consultants, suppliers and any other party accessing Company information, systems or resources.

The organizational, physical, technological and informational boundaries of the ISMS are defined in the document concerning the determination and management of the scope and are reviewed in the event of significant changes.



e sono riesaminati in occasione di cambiamenti rilevanti.

Impegni dell'Alta Direzione

L'Alta Direzione assume la responsabilità complessiva dell'efficacia del SGSI e si impegna a:

- assicurare che la Politica e gli obiettivi di sicurezza siano coerenti con gli indirizzi strategici della Società;
- integrare i requisiti di sicurezza delle informazioni nei processi aziendali e decisionali;
- mettere a disposizione risorse, competenze e strumenti adeguati e proporzionati ai rischi;
- assegnare ruoli, responsabilità e autorità chiare e garantire un adeguato flusso informativo verso gli organi di amministrazione e direzione;
- promuovere la cultura della sicurezza, la responsabilizzazione del personale e il miglioramento continuo;
- assicurare il rispetto dei requisiti legali, regolamentari, contrattuali e volontari applicabili, compresi il D.Lgs. 138/2024, ove applicabile, la normativa in materia di protezione dei dati personali e la ISO/IEC 27001:2022 e quando previsto dall'Autorità di bandiera e dai codici e regolamenti nazionali ed internazionali.

Obiettivi e indirizzi di sicurezza

Fratelli Neri S.p.A. definisce e riesamina obiettivi misurabili e coerenti con i rischi e con le esigenze delle parti interessate. In particolare, la Società orienta il proprio SGSI ai seguenti indirizzi:

- proteggere le informazioni operative, tecniche, commerciali, amministrative, personali e contrattuali da accessi, divulgazioni, alterazioni, perdite o utilizzi non autorizzati;
- garantire la disponibilità dei sistemi e delle comunicazioni necessari ai processi e ai servizi critici;
- identificare, valutare e trattare i rischi di sicurezza delle informazioni con criteri definiti e documentati;
- valuta gli impatti sulla sicurezza correlati alla sicurezza informatica;
- classificare le informazioni e gli asset, attribuendone la responsabilità e applicando misure coerenti con la criticità;
- applicare i principi del minimo privilegio, della necessità di conoscere e della segregazione dei compiti;
- prevenire, rilevare, gestire e analizzare gli incidenti, preservando le evidenze e adempiendo agli obblighi di comunicazione e notifica applicabili;
- assicurare la continuità dei processi e la capacità di ripristino attraverso misure, piani e verifiche proporzionati ai requisiti operativi;
- governare i rischi derivanti da fornitori, servizi ICT, accessi esterni e catena di approvvigionamento;
- garantire che acquisizioni, modifiche, manutenzioni e dismissioni di sistemi e tecnologie siano gestite in modo controllato e sicuro.

Senior Management Commitments

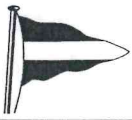
Senior Management assumes overall responsibility for the effectiveness of the ISMS and undertakes to:

- ensure that the Policy and security objectives are consistent with the Company's strategic directions;
- integrate information security requirements into business and decision-making processes;
- make available adequate and proportionate resources, competencies and tools;
- assign clear roles, responsibilities and authority and ensure adequate information flow to administration and management bodies;
- promote a culture of security, staff accountability and continual improvement;
- ensure compliance with applicable legal, regulatory, contractual and voluntary requirements, including Legislative Decree 138/2024, where applicable, data protection legislation and ISO/IEC 27001:2022, and when required by the Flag State and by national and international codes and regulations.

Security objectives and guidelines

Fratelli Neri S.p.A. defines and reviews measurable objectives consistent with risks and stakeholder requirements. In particular, the Company directs its ISMS towards the following guidelines:

- protect operational, technical, commercial, administrative, personal and contractual information from unauthorized access, disclosure, alteration, loss or use;
- ensure the availability of systems and communications necessary for critical processes and services;
- identify, assess and treat information security risks according to defined and documented criteria;
- Evaluate the safety impacts related to cybersecurity;
- classify information and assets, assign ownership and apply measures consistent with criticality;
- apply the principles of least privilege, need-to-know and segregation of duties;
- prevent, detect, manage and analyse incidents, preserving evidence and fulfilling applicable communication and notification obligations;
- ensure process continuity and recovery capability through measures, plans and verifications proportionate to operational requirements;
- govern risks arising from suppliers, ICT services, external access and the supply chain;
- ensure that system and technology acquisitions, changes, maintenance and disposals are managed in a controlled and secure manner.



Gestione del rischio e controlli

La Società mantiene un processo strutturato di identificazione, analisi, valutazione e trattamento dei rischi. Le valutazioni sono aggiornate con periodicità definita e ogniqualvolta intervengano cambiamenti significativi di natura organizzativa, tecnologica, operativa, normativa o contrattuale, nonché a seguito di incidenti rilevanti.

Le misure di sicurezza sono selezionate in funzione del rischio e formalizzate nel piano di trattamento e nella Dichiarazione di Applicabilità. La loro effettiva implementazione è verificata attraverso monitoraggi, controlli, audit e riesami. La presente Politica non presuppone che ogni misura sia applicabile indistintamente, ma richiede che le decisioni di inclusione o esclusione siano motivate e documentate.

La gestione del rischio informatico è una parte intrinseca della cultura della sicurezza e della protezione della Compagnia, che favorisce il funzionamento sicuro ed efficiente della nave e deve essere implementata a vari livelli dell'azienda, compresi i dirigenti a terra ed il personale di bordo e prevede:

- identificazione dei ruoli e delle responsabilità degli utenti, del personale chiave e della direzione, sia a terra che a bordo;
- identificazione dei sistemi, delle risorse dei dati e della capacità che, se interrotti, potrebbero comportare rischi per le operazioni e la sicurezza della nave;
- implementazione di misure tecniche e procedurali per proteggere da un incidente informatico, o rilevarlo tempestivamente, garantendo la continuità delle operazioni;
- la redazione di un piano di emergenza da testare regolarmente.

Gestione degli accessi e delle risorse

Gli accessi fisici e logici sono autorizzati in base alle mansioni e alle effettive necessità operative, sono riesaminati periodicamente e revocati tempestivamente al venir meno dei presupposti. Gli account privilegiati, gli accessi remoti e gli accessi concessi a soggetti esterni sono sottoposti a controlli rafforzati e a tracciamento adeguato al rischio.

Le risorse informative e tecnologiche devono essere utilizzate esclusivamente per finalità autorizzate, nel rispetto delle policy e delle istruzioni aziendali. Il personale è tenuto a proteggere credenziali, dispositivi, documenti e informazioni da uso improprio, perdita, sottrazione o divulgazione non autorizzata.

Incidenti, continuità operativa e resilienza

Tutti gli eventi o le anomalie che possano compromettere la sicurezza delle informazioni o la continuità dei servizi o avere ricadute sulla sicurezza devono essere tempestivamente segnalati e gestiti secondo le procedure aziendali.

Risk Management and controls

The Company maintains a structured process for identifying, analysing, assessing and treating risks. Assessments are updated at defined intervals and whenever significant organizational, technological, operational, regulatory or contractual changes occur, as well as following major incidents.

Security measures are selected based on risk and formalized in the treatment plan and the Statement of Applicability. Their effective implementation is verified through monitoring, controls, audits and reviews. This Policy does not assume that every measure is indiscriminately applicable, but requires that inclusion or exclusion decisions are justified and documented.

Cyber risk management is an intrinsic part of the Company's safety and security culture, which promotes the safe and efficient operation of the ship. It must be implemented at various levels of the company, including shore-based management and onboard personnel, and provides for:

- *identification of the roles and responsibilities of users, key personnel, and management, both ashore and onboard;*
- *identification of systems, data assets, and capabilities that, if disrupted, could pose risks to ship operations and safety;*
- *implementation of technical and procedural measures to protect against or promptly detect a cyber incident, ensuring operational continuity;*
- *the drafting of an emergency plan to be tested regularly.*

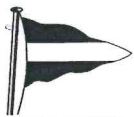
Access and resource management

Physical and logical access is authorized based on duties and actual operational needs, is reviewed periodically and revoked promptly when the relevant conditions cease to exist. Privileged accounts, remote access and access granted to external parties are subject to enhanced controls and tracking commensurate with the risk.

Information and technology resources must be used exclusively for authorized purposes, in compliance with Company policies and instructions. Personnel are required to protect credentials, devices, documents and information from misuse, loss, theft or unauthorized disclosure.

Incidents, Business Continuity and Resilience

All events or anomalies that may compromise information security, or service continuity or to have safety implications, must be promptly reported and managed in accordance with Company procedures. Incidents are classified, contained, resolved and



Gli incidenti sono classificati, contenuti, risolti e analizzati per individuare cause, impatti e azioni correttive, assicurando, ove necessario, il coinvolgimento delle funzioni competenti e delle Autorità.

Per gli incidenti significativi soggetti alla disciplina NIS2, la Società assicura, ove applicabile, l'adempimento degli obblighi di notifica al CSIRT Italia nei termini previsti dalla normativa. La gestione operativa delle notifiche è disciplinata da specifiche procedure e non è demandata alla sola presente Politica.

In ambito marittimo i principali incidenti informatici possono derivare da:

- un incidente di sicurezza informatica, che influisce sulla disponibilità e/o integrità di un sistema OT;
- un errore di sistema non intenzionale che si verifichi durante la manutenzione o riparazione di software;
- perdita o manipolazione dei dati di sensori esterni, fondamentali per l'esercizio della nave;
- guasto di un sistema a causa di "crash" e/o bug del software;
- interazione dell'equipaggio ad attacchi esterni (es. phishing, che il vettore di attacco più comune, che potrebbe portare a perdita di dati sensibili.

ed i principali elementi che influenzano la vulnerabilità dell'azienda agli incidenti informatici possono essere:

- coinvolgimento di più parti interessate nel funzionamento e nel noleggio di una nave che potrebbe comportare una mancanza di responsabilità per l'infrastruttura del sistema IT/OT/Reti della nave;
- utilizzo di sistemi IT/OT non più supportati e/o che si basano su sistemi operativi obsoleti;
- utilizzo di sistemi OT a cui non è possibile applicare patch o eseguire antivirus a causa di problemi di omologazione;
- navi che si interfacciano online con le parti costiere e/o altre parti della catena di fornitura globale;
- apparecchiature della nave che sono monitorate e accessibili a distanza, ad esempio dai produttori e/o dai fornitori di supporto;
- la condivisione di informazioni di business critiche, dati sensibili, anche commerciali, con fornitori di servizi a terra, compresi i terminali marittimi e, ove applicabile, le pubbliche Autorità;
- la disponibilità e l'uso di sistemi critici controllati da computer, che potrebbero non essere aggiornati con le ultime patch e/o non essere adeguatamente protetti, per la sicurezza della nave e la protezione ambientale;
- una cultura della gestione del rischio cibernetico che abbia ancora un potenziale di miglioramento, ad esempio attraverso una formazione più formale, esercitazioni e ruoli e responsabilità chiari;
- installazione a bordo di un sistema di automazione costituito da più sottosistemi di più fornitori che non siano stati integrati dal cantiere senza minimo riguardo ai problemi informatici.

analysed to identify causes, impacts and corrective actions, ensuring, where necessary, the involvement of competent functions and Authorities.

For significant incidents subject to NIS2 regulation, the Company ensures, where applicable, compliance with notification obligations to CSIRT Italy within the time limits provided by law. The operational management of notifications is governed by specific procedures and is not delegated to this Policy alone.

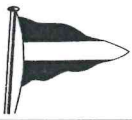
In the maritime sector, the main cybersecurity incidents can stem from:

- *A cybersecurity incident which affects the availability and/or integrity of OT system;*
- *An unintended system failure occurring during software maintenance and/or patching;*
- *Loss or manipulation of external sensor data, critical for ship operations;*
- *failure of system due to software crashes and/or "bugs";*
- *Crew interaction with external attacks (e.g., phishing, which is the most common attack vector by threat actors), which could lead to the loss of sensitive data.*

and the main elements influencing the company's vulnerability to cyber incidents can be:

- *Involvement of multiple stakeholders in the operation and chartering of a ship, potentially resulting in lack of accountability for the IT and OT system infrastructure and ship's networks.*
- *Use of IT/OT systems that are no longer supported and/or that rely on obsolete operating systems;*
- *Use of OT systems that cannot be patched or run antivirus software due to type-approval issues;*
- *Ships interfacing online with shore-based parties and/or other parts of the global supply chain;*
- *Ship equipment that is remotely monitored and accessed, e.g. by manufacturers and/or support providers;*
- *Sharing of critical business information and sensitive data, including commercial data, with shore-based service providers, including marine terminals and, where applicable, public authorities;*
- *Availability and use of computer controlled critical systems, which may not have the latest patches installed or be properly secured, for the ship's safety and for environmental protection;*
- *A cyber risk management culture that still has potential for improvement, e.g. through more formalized training, drills, and clarified roles and responsibilities;*
- *Frequently the automation system comprises of multiple sub-system from numerous vendors that are integrated by shipyards with minimal regard to cyber issues.*

The Company identifies critical processes and services, defines continuity and recovery requirements and adopts backup, redundancy, emergency response and disaster recovery measures proportionate to the risks. The effectiveness of measures is verified through



La Società identifica i processi e i servizi critici, definisce requisiti di continuità e ripristino e adotta misure di backup, ridondanza, risposta alle emergenze e disaster recovery proporzionate ai rischi. L'efficacia delle misure è verificata mediante controlli e prove pianificate, con registrazione degli esiti e gestione delle eventuali carenze.

Sicurezza dei fornitori e della catena di approvvigionamento

I fornitori e i servizi esternalizzati che possono incidere sulla sicurezza delle informazioni sono valutati in funzione della criticità, dell'accesso alle informazioni, della dipendenza operativa e dei potenziali impatti. I requisiti di sicurezza, riservatezza, protezione dei dati, continuità, gestione degli incidenti e restituzione o cancellazione delle informazioni sono definiti, ove pertinenti, negli accordi contrattuali e sottoposti a monitoraggio.

Personale, formazione e consapevolezza

La sicurezza delle informazioni è una responsabilità condivisa. La Società assicura che il personale e i soggetti rilevanti ricevano informazioni, istruzioni e formazione adeguate al ruolo e ai rischi. Le attività di sensibilizzazione sono pianificate, aggiornate in funzione delle minacce e verificate per valutarne l'efficacia.

Le violazioni delle regole di sicurezza sono gestite secondo le disposizioni contrattuali, disciplinari e normative applicabili, nel rispetto dei principi di proporzionalità e delle responsabilità individuali.

Monitoraggio, audit e miglioramento continuo

La Società monitora le prestazioni del SGSI mediante indicatori, verifiche tecniche e organizzative, audit interni, valutazioni dei fornitori, analisi degli incidenti e riesami della Direzione. Le non conformità e le debolezze individuate sono gestite attraverso correzioni, azioni correttive e piani di miglioramento con responsabilità e scadenze definite.

Comunicazione, riesame e approvazione

La presente Politica è comunicata al personale e resa disponibile alle parti interessate per quanto appropriato. È riesaminata almeno annualmente e ogniqualvolta intervengano cambiamenti significativi del contesto, del campo di applicazione, dei rischi, dei requisiti applicabili o a seguito di incidenti rilevanti.

La responsabilità di coordinare l'attuazione, il monitoraggio e l'aggiornamento della presente Politica è attribuita al Responsabile della Sicurezza delle Informazioni formalmente nominato dalla Direzione, fermo restando che la responsabilità complessiva del SGSI rimane in capo all'Alta Direzione.

planned checks and tests, with recording of results and management of any deficiencies.

Supplier and supply chain security

Suppliers and outsourced services that may affect information security are assessed based on criticality, access to information, operational dependency and potential impacts. Security, confidentiality, data protection, continuity, incident management and information return or erasure requirements are defined, where relevant, in contractual agreements and subject to monitoring.

Personnel, training and awareness

Information security is a shared responsibility. The Company ensures that personnel and relevant parties receive information, instructions and training adequate to their role and risks. Awareness activities are planned, updated in response to threats and verified to assess their effectiveness.

Breaches of security rules are managed in accordance with applicable contractual, disciplinary and regulatory provisions, respecting the principles of proportionality and individual accountability.

Monitoring, auditing and continual improvement

The Company monitors ISMS performance through indicators, technical and organizational checks, internal audits, supplier assessments, incident analysis and Management reviews. Nonconformities and weaknesses identified are addressed through corrections, corrective actions and improvement plans with defined responsibilities and deadlines.

Communication, review and approval

This Policy is communicated to personnel and made available to interested parties as appropriate. It is reviewed at least annually and whenever significant changes occur in the context, scope, risks, applicable requirements or following major incidents.

Responsibility for coordinating the implementation, monitoring and updating of this Policy is assigned to the formally appointed Information Security Manager by the Management, without prejudice to the overall responsibility for the ISMS remaining with Senior Management.

Livorno li 18.08.2026