POLITICA SISTEMA GESTIONE E SICUREZZA DELLE FORMAZIONI
PLANT INFORMATION SECURITY MANAGEMENT SYSTEM
STABILIMENTO DEL GRUPPO SATA
SATA GROUP PLANT
SATA S.p.A.

La Politica per la Sicurezza delle Informazioni

La Direzione di SATA S.p.A. ha definito, ha divulgato e si impegna a mantenere aggiornata e attiva a tutti i livelli della propria organizzazione la presente Politica per la Sicurezza delle Informazioni, con il fine di promuovere e attuare efficaci misure di tutela e di protezione dalle potenziali minacce, interne o esterne, intenzionali o accidentali, rivolte alle informazioni gestite, archiviate e trasmesse nell'ambito dei processi aziendali, in conformità con le prescrizioni della norma tecnica ISO/IEC 27001.
L'osservanza e l'attuazione della presente Politica, che si realizza concretamente attraverso la costituzione e il mantenimento di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) ai sensi della norma tecnica internazionale ISO/IEC 27001, è pertanto obbligatoria per tutto il personale interno ed è prevista negli accordi con qualsiasi soggetto esterno che, a qualunque titolo, sia coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione di tale Sistema di Gestione.

Information Security Policy

The Management of SATA S.p.A. has defined, disseminated, and is committed to keeping this Information Security Policy up to date and active at all levels of its organization. The Policy is designed to promote and implement effective measures to protect against potential threats, internal or external, intentional or accidental, aimed at the information managed, stored, and transmitted within company processes, in accordance with the requirements of the ISO/IEC 27001 technical standard.

Compliance with and implementation of this Policy, which is concretely achieved through the establishment and maintenance of an Information Security Management System (ISMS) pursuant to the international technical standard ISO/IEC 27001, is therefore mandatory for all internal personnel and is required in agreements with any external party who, in any capacity, is involved in the processing of information falling within the scope of application of this Management System.

Il contesto e i principi della Politica per la Sicurezza delle Informazioni

Il patrimonio informativo oggetto di tutela è costituito dall'insieme delle informazioni proprie o di terzi, generate, gestite, archiviate e trasmesse nell'ambito dei processi aziendali attuati in tutte le sedi dell'azienda.

In particolare, tale tutela si realizza attraverso l'attuazione dei seguenti principi:

1. La confidenzialità delle informazioni: le informazioni devono essere accessibili solo da chi è autorizzato;
2. L'integrità delle informazioni: le informazioni devono essere protette, in quanto ad accuratezza e completezza, così come i metodi utilizzati per la loro elaborazione;

The context and principles of the Information Security Policy

The information assets subject to protection consist of all proprietary or third-party information generated, managed, archived, and transmitted as part of the company's business processes implemented across all locations.

Specifically, this protection is achieved through the implementation of the following principles:

1. *Confidentiality of information: information must be accessible only by authorized persons;*
2. *Integrity of information: information must be protected in terms of accuracy and completeness, as well as the methods used to process it;*

3. La disponibilità delle informazioni: gli utenti autorizzati devono poter accedere alle informazioni nel momento in cui lo richiedono.

3. *Availability of information: authorized users must be able to access information when they request it.*

La Società concretizza ed attua tali principi identificando le proprie esigenze di sicurezza tramite una specifica analisi dei rischi, che consente di acquisire consapevolezza rispetto al livello di esposizione a minacce del proprio sistema informativo, permette di valutare le potenziali conseguenze e i danni che possono derivare al sistema informativo a seguito della mancata applicazione di adeguate misure di sicurezza e quale sia la realistica probabilità di attuazione delle minacce identificate.
I risultati di tale valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee, che prevedono:

The Company implements these principles by identifying its security needs through a specific risk analysis. This analysis allows for awareness of the level of exposure to threats affecting its information system, allows for assessment of the potential consequences and damage that may result from the failure to implement adequate security measures, and allows for the realistic likelihood of the identified threats being implemented.

The results of this assessment determine the actions necessary to manage the identified risks and the most suitable security measures, which include:

1. La disponibilità di un inventario costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno è individuato un responsabile;
2. La classificazione delle informazioni in base al rispettivo livello di criticità, in modo da poter essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati;
3. Ogni accesso alle informazioni è sottoposto a una procedura d'identificazione e autenticazione, e le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti;
4. La definizione di opportune procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni;
5. La promozione della piena consapevolezza rispetto alle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
6. La messa a disposizione di un canale per la pronta segnalazione di eventuali

1. *Availability of a constantly updated inventory of company assets relevant to information management, with a designated manager for each asset;*
2. *Classification of information based on its criticality level, so that it can be managed with consistent and appropriate levels of confidentiality and integrity;*
3. *All access to information is subject to an identification and authentication procedure, and information access authorizations are differentiated based on the role and duties held;*
4. *Establishing appropriate procedures for the secure use of company assets and information;*
5. *Promoting full awareness of information security issues among all personnel (employees and collaborators) from the moment of selection and throughout their employment.*
6. *Providing a channel for the prompt reporting of any incidents impacting*

incidenti che impattano sulla sicurezza delle informazioni, che saranno gestiti secondo specifiche procedure
7. Il monitoraggio degli accessi alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e/o apparecchiature.
8. La conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
9. La predisposizione di un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
10. L'inclusione degli aspetti di sicurezza in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.

information security, which will be managed according to specific procedures.
7. *Monitoring access to the company offices and individual locations where information and/or equipment are managed.*
8. *Compliance with legal requirements and information security principles in contracts with third parties.*
9. *Preparation of a continuity plan that allows the company to effectively address an unforeseen event, ensuring the restoration of critical services in a timely manner and in a manner that limits negative consequences for the company's mission.*
10. *The inclusion of security aspects in all phases of design, development, operation, maintenance, assistance and decommissioning of IT systems and services.*

Il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

Compliance with legal provisions, statutes, regulations, or contractual obligations and any information security requirements, minimizing the risk of legal or administrative sanctions, significant losses, or damage to reputation.

Responsabilità di osservanza e attuazione

Responsibility for compliance and implementation

L'osservanza e l'attuazione delle misure di sicurezza sopra elencate, compreso l'obbligo di segnalazione delle eventuali anomalie e violazioni di cui si dovesse venire a conoscenza, sono responsabilità di tutti i soggetti, interni o esterni, che, a qualsiasi titolo, collaborano con l'azienda e sono in qualche modo coinvolti con il trattamento di dati e informazioni che rientrano nel campo di applicazione del Sistema di Gestione.
Il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni, nell'ambito del campo di applicazione dello stesso e attraverso norme e procedure appropriate, vigila e opera affinché tale Sistema sia costantemente ed

Compliance and implementation of the above security measures, including the obligation to report any anomalies or violations of which they become aware, are the responsibility of all individuals, internal or external, who, in any capacity, collaborate with the company and are in any way involved in the processing of data and information falling within the scope of the Management System.
The Information Security Management System Manager, within the scope of the Management System and through appropriate standards and procedures, monitors and ensures that the System is consistently and effectively implemented, updated, and adapted to the

efficacemente attuato, aggiornato e adeguato alla realtà aziendale, anche organizzando adeguati interventi di formazione e promuovendo la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni.
Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

company's needs. This includes organizing appropriate training programs and promoting staff awareness of all aspects of information security.

Any employee, consultant, and/or external collaborator of the company who intentionally or negligently disregards the established security rules and thereby causes damage to the company may be prosecuted through appropriate channels and in full compliance with legal and contractual obligations.

Impegno della Direzione

La Direzione sostiene e promuove attivamente la sicurezza delle informazioni all'interno dell'azienda tramite un chiaro indirizzo, un impegno costante, l'assegnazione di incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
La Direzione inoltre verifica e riesamina, periodicamente o in concomitanza di cambiamenti significativi, l'adeguatezza della presente Politica e l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, assicurando un supporto costante e idoneo ai fini della sua applicazione e promuovendo l'introduzione delle eventuali integrazioni e rettifiche necessarie per adeguarlo ai cambiamenti che possono influenzare l'approccio dell'azienda rispetto alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e i risultati dei precedenti riesami.
Il risultato di tale riesame include le decisioni e le azioni relative al miglioramento dell'approccio aziendale inerente alla gestione della sicurezza delle informazioni.

Management Commitment

Management actively supports and promotes information security within the company through clear direction, ongoing commitment, the assignment of explicit tasks, and the recognition of responsibilities related to information security.
Management also assesses and reviews, periodically or in conjunction with significant changes, the adequacy of this Policy and the effectiveness and efficiency of the Information Security Management System, ensuring ongoing and appropriate support for its implementation and promoting the introduction of any necessary additions and adjustments to adapt it to changes that may impact the company's approach to information security management, including organizational changes, the technical environment, resource availability, legal, regulatory, or contractual conditions, and the results of previous reviews.
The outcome of this review includes decisions and actions related to improving the company's approach to information security management.

Valperga (TO), 11/10/2024

Responsabile ICT Gruppo SATA
SATA Group ICT Manager
Marco MELLINI

Direzione Generale Gruppo SATA
SATA Group Managing Director
Michele CINOTTO