Politica della sicurezza delle informazioni
Information security policy

1 Ambito di applicazione / Scope

La politica per la sicurezza delle informazioni di IHI Charging Systems International S.p.A. (di seguito ITY) si applica a tutto il personale interno nonché a persone che ad altro titolo intrattengono rapporti con ITY (collaboratori esterni, stagisti, fornitori, clienti, etc.) e trattano informazioni della Società.

The information security policy of IHI Charging Systems International S.p.A. (hereinafter ITY) applies to all internal staff as well as to persons who, for other reasons, have relations with ITY (external collaborators, interns, suppliers, customers, etc.) and manage or treat information of the Company.

2 Scopo / Purpose

Il patrimonio informativo di ITY costituito da informazioni relative all'organizzazione e ai propri stakeholder rappresenta per l'organizzazione un valore strategico che necessita di essere adeguatamente gestito e tutelato. Per questo motivo portiamo avanti da tempo un programma atto a:

- Conoscere e classificare le informazioni in relazione al valore nei confronti del business (Classificazione dei dati e Analisi di Impatto "BIA");
- Valutare i rischi connessi alle violazioni delle proprietà delle informazioni (Riservatezza, Integrità e Disponibilità);
- Contenere i rischi individuati attraverso l'implementazione di opportune misure di sicurezza tecniche ed organizzative volte a prevenire e/o a limitare i danni.

In quest'ottica, la Direzione fornisce un mandato chiaro circa l'istituzione e l'applicazione di un Sistema di Gestione della Sicurezza delle Informazioni ("SGSI"), promuovendo l'emissione di direttive e linee di indirizzo aziendali, con lo scopo di fornire un quadro complessivo dell'approccio alla sicurezza delle informazioni, secondo regole, criteri e standard di riferimento riconosciuti a livello internazionale come la norma UNI CEI EN ISO/IEC 27001. Tutte le persone che lavorano e/o collaborano con ITY sono impegnate a rispettare i seguenti principi:

- **Riservatezza**: assicurare che una determinata informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati;
- **Integrità**: mantenere e assicurare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, in modo non autorizzato o non individuato;
- **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e ai sistemi informativi aziendali quando ne fanno richiesta, salvaguardandone il patrimonio informativo nella garanzia di accesso e confidenzialità dei dati;
- **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati, rappresenta la misura che modifica il rischio;
- **Autenticità:** garantire una provenienza affidabile dell'informazione;
- **Privacy:** garantire la protezione e il controllo dei dati personali.

The information assets of ITY consisting of information related to the organization and its stakeholders, it represents a strategic value for the organization that needs to be properly managed and protected. For this reason, we carry on a continuous program aimed to:

- Identify and Classify information in relation to its value towards the business (Data classification and Business Impact Analysis)
- Evaluate the risks associated with violations of the information properties (Confidentiality, Integrity and Availability)
- Containing the risks identified through the implementation of proper technological and organizational security measures to prevent and limit damages to the company.

In this perspective, the Management provides a clear mandate regarding the establishment and application of an Information Security Management System ("ISMS"), promoting company regulations, policies and guidelines, with the purpose of providing an overall picture of the information security approach, according to international know rules, criteria and standards in reference to UNI CEI EN ISO / IEC 27001.

All the people who work and / or collaborate with ITY are committed to respecting the following principles:

- **Confidentiality**: ensure that certain information is accessible only to duly authorized persons and / or processes and that the information is not made available or disclosed to unauthorized individuals, entities or processes;
- **Integrity**: maintain and ensure the consistency of the information from unauthorized changes and ensure that the information does not undergo changes or deletions as a result of errors or voluntary actions, in an unauthorized or undetected manner;
- **Availability**: ensure that authorized users have access to company information and information systems when they request it, safeguarding their information assets by guaranteeing access and confidentiality of data;
- **Control**: ensuring that data management always takes place through safe and tested processes and tools, represents the measure that modifies the risk;
- **Authenticity**: guarantee a reliable source of information;
- **Privacy**: ensure the protection and control of personal data.

3 Riferimenti normativi / Normative references

In tema di sicurezza delle informazioni, valgono e sono garantiti i seguenti principi normativi:

- Ai sensi delle Norme **ISO/IEC 27001:2022** "Information security, cybersecurity and privacy protection - Information security management systems - Requirements" e ISO/IEC 27002:2022 "Information security, cybersecurity and privacy protection - Information security controls", è compito della Società adottare idonee misure di sicurezza tecniche ed organizzative per assicurare il rispetto dei requisiti della Norma, in termini di riservatezza, integrità e disponibilità delle informazioni e dei relativi asset di supporto;
- Ai sensi del **Regolamento Europeo per la protezione dei dati personali 2016/679 (nel seguito "GDPR**"), applicabile in tutti gli Stati membri dell'Unione Europea a decorrere dal 25 maggio 2018 e, ai sensi del Codice Privacy D. Lgs. 196/2003 e successive modifiche ed integrazioni (in seguito per brevità "Codice Privacy"), è compito della Società verificare che i Dati Personali oggetto di trattamento siano protetti tramite misure di sicurezza tecniche e organizzative, dai rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- In riferimento alle figure di **Amministratori di Sistema**, valgono i provvedimenti emessi sul tema dal Garante, che risultano attualmente non incompatibili con la normativa europea (GDPR);
- Ai sensi del **D. Lgs. 231/01** in materia di responsabilità amministrativa delle persone giuridiche, ed in particolare riferimento ai Reati Informatici, dalla stessa norma contemplati, è compito della Società adottare idonee misure di sicurezza per prevenire utilizzi indebiti che possono essere fonte di reato (in seguito per brevità "231 Reati Informatici");
- In riferimento allo standard di settore **TISAX® - Trusted Information Security Assessment Exchange** è uno standard di audit basato sulla ISO/IEC 27001 e rappresenta una lista di controlli di autovalutazione da condurre su fornitori e prestatori di servizi
- In riferimento alla Direttiva Europea 2022/2555 del 14/12/2022 "**Direttiva NIS2"** relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, e al relativo recepimento nazionale (D.Lgs. 4 settembre 2024, n. 138) nonché alle determinazioni attuative dell'Autorità nazionale competente (ACN) applicabili, la Società adotta e mantiene misure tecniche e organizzative adeguate e un modello di governance coerente con gli obblighi di legge.

Tale documento è pertanto redatto in conformità con tali principi e nel rispetto di tali normative, nonché a altre specifiche richieste normative richiamate nei paragrafi successivi.

In terms of information security, the following regulatory principles are applied and are guaranteed:

- In accordance with **ISO/IEC 27001:2022** “Information security, cybersecurity and privacy protection - Information security management systems - Requirements” and ISO/IEC 27002:2022 “Information security, cybersecurity and privacy protection - Information security controls” standards , the Company is responsible for adopting suitable technological and organizational security measures to ensure compliance with the requirements of the norm, in terms of confidentiality, integrity and availability of information and related support assets;
- In accordance with the **European General Data Protection Regulation 2016/679** (hereinafter "**GDPR**"), applicable in all Member States of the European Union starting from 25 May 2018 and in accordance to the Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003) as amended by Legislative Decree No. 101 of 10 August 2018 (hereinafter "Privacy Code" for brevity), it is the Company's responsibility to verify that the Personal Data being processed are protected by technological and organizational security measures, from the risks of destruction or loss, even accidental, of the data itself, of unauthorized access or processing that is not permitted or does not comply with the purposes of the collection;
- With reference to the figures of **System Administrators**, are valid and apply the legal provisions issued by the Italian Data Protection, which is currently not incompatible with European legislation (GDPR);
- In accordance with the **Legislative Decree 231/01** introduced the principle of the administrative responsibility of legal entities, and in particular with reference to IT crimes, the same rule contemplated, it is the duty of the Company to adopt suitable security measures to prevent improper use that may be a source of a crime (hereinafter referred to as “231 IT Crimes”);
- With reference to the industry standard **TISAX® - Trusted Information Security Assessment Exchange** is an audit standard based on ISO/IEC 27001 and represents a list of self-assessment checks to be conducted on suppliers and service providers
- With reference to European Directive 2022/2555 of December 14, 2022, " **NIS2 Directive**" on measures for a high common level of cybersecurity across the Union, and its national transposition (Legislative Decree No. 138 of September 4, 2024), as well as the applicable implementing decisions of the competent national authority (ACN), the Company adopts and maintains appropriate technical and organizational measures and a governance model consistent with legal obligations.

This document has therefore been drawn up in compliance with these principles and in compliance with these regulations, as well as with other specific regulatory requests referred to in the following paragraphs.

4 Responsabilità della politica di sicurezza delle informazioni / Responsibility for information security policy

La Direzione è responsabile dei contenuti della politica di sicurezza delle informazioni, della sua emanazione, attuazione, divulgazione, aggiornamento e riesame almeno annuale in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

La presente politica e il regolamento aziendale per l'utilizzo degli strumenti informatici sono comunicati all'interno dell'organizzazione attraverso il portale intranet aziendale v@lentina.

La presente politica è resa pubblica a tutte le parti interessate attraverso il sito della società all'indirizzo **https://www.ihi-csi.it**

Management is responsible for the content of the information security policy, its issuance, implementation, dissemination, updating, and review at least once a year in line with developments in the company and market context, assessing any actions to be taken in response to events such as:

- significant business developments/changes;
- new threats compared to those considered in the risk analysis activity;
- significant security incidents;
- evolution of the regulatory or legislative context regarding the secure processing of information.

This policy and the company regulations for the use of IT tools are communicated within the organization through the v@lentina company portal.

This policy is published to all interested parties via the company's website at **https://www.ihi-csi.it/en/**.

5 Principi e obiettivi generali / Principles and objectives

La politica per la sicurezza delle informazioni di ITY rappresenta l'impegno a garantire un Sistema di Gestione della Sicurezza delle Informazioni efficace e in costante miglioramento, e si ispira ai seguenti principi e obiettivi generali:

a. Garantire la protezione delle informazioni, dei sistemi informativi e di rete e dell'operatività, proporzionata rispetto ai rischi a cui ITY è esposta e alla loro criticità;

b. Garantire il rispetto della normativa vigente e applicabile alla realtà in cui ITY opera;

c. Definire e comunicare ruoli e responsabilità legate alla sicurezza delle informazioni e alla cybersecurity, chiarendo le responsabilità di tutti gli attori coinvolti secondo il principio del need-to-know, inclusi i ruoli preposti alla gestione degli adempimenti e delle comunicazioni verso l'Autorità competente.

d. Definire processi e standard che assicurano un adeguato livello di protezione;

e. Garantire un monitoraggio costante dei livelli di sicurezza e definire processi che consentano il loro miglioramento, nonché il costante aggiornamento di nuove minacce e rischi;

f. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale (in termini di Riservatezza, Integrità e Disponibilità e livelli di servizio) siano tempestivamente riconosciuti e correttamente gestiti incluse, ove applicabile, le comunicazioni e notifiche previste dalla normativa vigente, attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business (Business continuity);

g. Garantire l'accesso sicuro alle informazioni, ai servizi informativi e di rete, in modo da prevenire trattamenti non autorizzati realizzati senza i diritti necessari;

h. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza, operando con piena consapevolezza delle problematiche relative alla sicurezza;

i. Garantire che l'accesso alle sedi e ai singoli locali aziendali critici avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;

j. I trattamenti dei dati personali di cui ITY è titolare, avvengano nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 2016/679.

k. Assicurare, ove applicabile, la conformità agli obblighi in materia di cibersicurezza previsti dalla Direttiva (UE) 2022/2555 (NIS2) e dalla normativa nazionale di recepimento, con particolare riferimento alla protezione dei sistemi informativi e di rete rilevanti a supporto dei processi e servizi critici.

The information security policy of ITY represents the commitment to ensure an effective and constantly improving Information Security Management System, and is inspired by the following general principles and objectives:

a. Ensure the protection of information, information systems, networks, and operations, proportionate to the risks to which ITY is exposed and their criticality;

b. Ensure compliance with current legislation applicable to the context in which ITY operates;

c. Define and communicate roles and responsibilities related to information security and cybersecurity, clarifying the responsibilities of all actors involved according to the need-to-know principle, including the roles responsible for managing compliance and communications with the competent authority.

d. Define processes and standards that ensure an adequate level of protection;

e. Ensure constant monitoring of security levels and define processes that allow for their improvement, as well as constant updating of new threats and risks;

f. Ensure that anomalies and incidents affecting the information system and corporate security levels (in terms of Confidentiality, Integrity, and Availability and service levels) are promptly recognized and correctly managed, including, where applicable, communications and notifications required by current legislation, through efficient prevention, communication, and response systems in order to minimize the impact on the business (Business continuity);

g. Ensure secure access to information, information services, and networks in order to prevent unauthorized processing without the necessary rights;

h. Ensure that the organization and third parties collaborate in the processing of information by adopting procedures aimed at complying with adequate security levels, operating with full awareness of security issues;

i. Ensure that access to critical company premises and individual rooms is restricted to authorized personnel only, in order to guarantee the security of the areas and assets present;

j. The processing of personal data held by ITY is carried out in compliance with the European General Data Protection Regulation GDPR 2016/679.

k. Ensure, where applicable, compliance with the cybersecurity obligations set out in Directive (EU) 2022/2555 (NIS2) and the national transposition legislation, with particular reference to the protection of relevant information and network systems supporting critical processes and services.

6 Documenti di riferimento / Referenced documents

La Società adotta, comunica e applica politiche documentate almeno per i seguenti ambiti: gestione del rischio; ruoli e responsabilità; sicurezza e affidabilità delle risorse umane; conformità e audit; sicurezza della catena di approvvigionamento; gestione degli asset; gestione vulnerabilità; continuità operativa/DR/gestione crisi; identità e controllo accessi; sicurezza fisica; formazione e consapevolezza; sicurezza dei dati; sviluppo/configurazione/manutenzione/dismissione dei sistemi.

Tali politiche sono definite e mantenute nei documenti interni di riferimento e riesaminate periodicamente.

Le politiche e procedure interne richiamate costituiscono l'attuazione operativa dei requisiti normativi applicabili e sono disponibili alle funzioni competenti e, ove richiesto, alle Autorità.

The Company adopts, communicates, and applies documented policies for at least the following areas: risk management; roles and responsibilities; human resources security and reliability; compliance and audit; supply chain security; asset management; vulnerability management; business continuity/DR/crisis management; identity and access control; physical security; training and awareness; data security; system development/configuration/maintenance/decommissioning.

These policies are defined and maintained in internal reference documents and reviewed periodically.

The internal policies and procedures referred to constitute the operational implementation of the applicable regulatory requirements and are available to the relevant departments and, where requested, to the Authorities.

- SP.C4.01.P.018.xx Policy generale di sicurezza / General Information Security Policy
- MP.7C.00.M.002.xx Regolamento aziendale-ALLEGATO 3 Utilizzo strumenti Informatici-Internet-sicurezza dei dati aziendali / Company regulation - ATTACHMENT 3 Use of IT asset - Internet - security of company data

IHI Charging Systems International S.p.A.

Chairman & CEO

Firmato da:
Giovanni Ortolan
596DF712A18C4CA...