


***POLITICA PUBBLICA PER LA SICUREZZA DELLE
INFORMAZIONI
INFORMATION SECURITY PUBLIC POLICY***

	Tipo documento: Documento Policy per la Sicurezza delle Informazioni
	Identificativo: ISPP-01



AKRONOS TECHNOLOGIES S.R.L. è consapevole che il proprio patrimonio informativo costituisce un ruolo di assoluto rilievo strategico e rappresenta un importante asset aziendale da tutelare.

Per questo motivo, ha approvato la presente politica per la sicurezza delle informazioni, avendo a riferimento standard nazionali e internazionali, quali TISAX e ISO IEC 27001, oltre alle relative normative cogenti di riferimento.

La sicurezza delle informazioni è intesa come il mantenimento di:

- riservatezza, ossia garantire l'accesso alle informazioni solo ai soggetti autorizzati;
- integrità, ossia salvaguardare l'accuratezza e la completezza delle informazioni e delle modalità di trattamento;
- disponibilità, ossia garantire l'accesso alle informazioni e agli asset associati ai soggetti autorizzati che lo richiedono senza ritardi.

AKRONOS TECHNOLOGIES S.R.L. si impegna a garantire la riservatezza, integrità e disponibilità delle informazioni non solo proprie aziendali, ma anche dei propri clienti, dipendenti e stakeholders in genere, applicando come cultura aziendale, i principi del need to know (necessità di sapere), del least privilege (privilegio minimo), risk-based thinking e security by design & by default.

A fronte di questo impegno e sulla base di tali principi, la Società ha implementato un Sistema di Gestione per la Sicurezza delle Informazioni, quale meccanismo di controllo che, tramite misure organizzative, fisiche, tecnologiche e relative alla gestione del personale, permettono alla Direzione di garantire che la sicurezza delle informazioni sia il risultato di una gestione sostenibile piuttosto che quella di una mera coincidenza e di uno sforzo individuale.

Infatti, AKRONOS TECHNOLOGIES S.R.L. crede che la sicurezza raggiungibile solamente attraverso le misure tecniche sia una sicurezza "limitata" e che perciò debba essere supportata anche da procedure di gestione della sicurezza delle informazioni adeguate, da un

AKRONOS TECHNOLOGIES S.R.L. recognizes that its information assets play a role of primary strategic importance and represent a vital corporate asset to be protected.

For this reason, it has approved this Information Security Policy, taking into account national and international standards – such as TISAX and ISO/IEC 27001 - in addition to relevant mandatory regulations.

Information security is defined as the maintenance of:

- *Confidentiality: ensuring that information is accessible only to authorized individuals;*
- *Integrity: safeguarding the accuracy and completeness of information and its processing methods;*
- *Availability: ensuring that authorized users have access to information and associated assets upon request, without delay.*

AKRONOS TECHNOLOGIES S.R.L. is committed to ensuring the confidentiality, integrity, and availability of not only its own corporate information but also that of its customers, employees, and stakeholders in general. This is achieved by embedding the principles of need-to-know, least privilege, risk-based thinking, and security by design & by default into the corporate culture.

In light of this commitment and based on these principles, it has implemented an Information Security Management System (ISMS). This control mechanism, through organizational, physical, technological, and personnel measures, allows management to ensure that information security is the result of sustainable management rather than mere coincidence and individual effort.

In fact, AKRONOS TECHNOLOGIES S.R.L. believes that security achievable through technical measures alone is limited and must be supported by adequate information security management procedures, constant risk-based

monitoraggio costante del Sistema, orientato al rischio e sempre teso al miglioramento, oltreché facendo della formazione adeguata per sensibilizzare tutti gli attori coinvolti.

Gli obiettivi per la sicurezza delle informazioni di AKRONOS TECHNOLOGIES S.R.L. sono:

- Garantire riservatezza, integrità e disponibilità delle informazioni (di business e personali) proprie, dei propri dipendenti, fornitori e clienti, assicurando che siano gestite in accordo con obblighi normativi - nazionali e internazionali -, contrattuali e degli standard cui l'azienda aderisce.
- Integrare i requisiti del sistema di gestione per la sicurezza delle informazioni all'interno dei processi aziendali, mantenendo il sistema sempre aggiornato, monitorato e teso al miglioramento continuo.
- Assegnare ruoli e responsabilità a personale qualificato e competente, privi di conflitti di interesse e subordinazione, al fine di delineare una chiara gestione della sicurezza della informazioni in termini di: governance, gestione degli incidenti, della crisi e della business continuity.
- Essere ricettivi dei rischi e opportunità del contesto esterno ed interno, per favorire una sempre aggiornata comprensione dei possibili impatti che possono ricadere sulle informazioni e favorire una pronta risposta.
- Formare e sensibilizzare i dipendenti sulla sicurezza delle informazioni, sul sistema di gestione implementato e relative policy, procedure e regolamenti, sui rischi potenziali e le modalità per prevenirli.
- Comunicare con le autorità competenti e le parti interessate gli eventi per la sicurezza delle informazioni che possono avere un impatto rilevante sugli stessi, secondo gli accordi contrattuali e le normative nazionali e internazionali, e conservare le registrazioni necessarie alla ricostruzione degli eventi e delle relative cause.
- Adottare idonee misure di prevenzione, e predisporre piani di risposta per la gestione

and improvement-oriented system monitoring, as well as training and awareness-raising among stakeholders.

AKRONOS TECHNOLOGIES S.R.L.'s information security objectives are:

- *Guarantee the confidentiality, integrity, and availability of information (business and personal) belonging to the company, its employees, suppliers, and customers, ensuring it is managed in accordance with national and international regulatory obligations, contractual obligations, and the standards to which the It adheres.*
- *Integrate the requirements of the information security management system into company processes, keeping the system constantly updated, monitored, and striving for continuous improvement.*
- *Assign roles and responsibilities to qualified and competent personnel, free of conflicts of interest and subordination, in order to outline clear information security management in terms of governance, incident management, crisis management, and business continuity.*
- *Be sensitive to external and internal risks and opportunities to foster a constantly updated understanding of the potential impacts that may affect information and facilitate a prompt response.*
- *Train and raise employee awareness of information security, the implemented management system and related policies, procedures, and regulations, potential risks, and ways to prevent them.*
- *Communicate with the competent authorities and interested parties about information security events that may have a significant impact on them, in accordance with contractual agreements and national and international regulations, and maintain*

delle crisi, incidenti o potenziali tali, garantendo misure idonee a preservare la continuità della sicurezza delle informazioni.

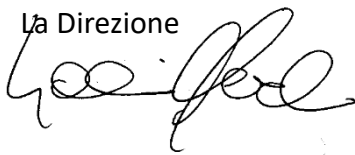
- Assicurare che la sicurezza delle informazioni sia mantenuta anche dalla propria catena di fornitura e dalle tecnologie che l'azienda utilizza, condividendo con i propri collaboratori gli standard di sicurezza che l'organizzazione si aspetta all'interno del rapporto di collaborazione e ripartendo in modo chiaro e trasparente le responsabilità delle parti per la sicurezza delle informazioni scambiate nel rapporto contrattuale di collaborazione.
- Prevenire la perdita del diritto d'autore tramite il monitoraggio dei software utilizzati, siano essi usufruibili online o su licenza, anche in considerazione dell'introduzione dell'AI.
- Valutare il proprio sistema di gestione per la sicurezza delle informazioni anche tramite organismi indipendenti e qualificati.

AKRONOS TECHNOLOGIES S.R.L. adotta la presente politica per la sicurezza delle informazioni e si impegna a perseguirne gli obiettivi.

La politica è revisionata dall'Organizzazione in caso di cambiamenti che possano essere rilevanti o qualora si verificano incidenti sui propri obiettivi di sicurezza delle informazioni.

Luogo e data
Torino, 10 maggio 2026

La Direzione



the records necessary to reconstruct the events and their causes.

- *Adopt appropriate preventive measures and develop response plans for managing crises, incidents, or potential incidents; ensuring appropriate measures to maintain the continuity of information security.*
- *Ensure that information security is maintained throughout the company's supply chain and the technologies it uses, sharing with its employees the security standards the company expects within its collaborative relationship and clearly and transparently dividing the parties' responsibilities for the security of information exchanged under the collaborative contract.*
- *Prevent the loss of copyright by monitoring the software used, whether available online or under license, also considering the introduction of AI.*
- *Evaluate its information security management system, including through independent and qualified bodies.*

AKRONOS TECHNOLOGIES S.R.L. adopts this information security policy and is committed to pursuing its objectives.

The policy is reviewed by the company in the event of changes that may be relevant and impact its information security objectives.