INFORMATION SECURITY POLICY

Document: **ANX-000440**

Issue: 1 17-03-2022

Secondo Mona (hereinafter, "SM" or "organization" or "the Company") information security policy is designed to provide adequate protection and clear accountability in the management of all SM's assets and information. SM recognizes that ICT systems and information are valuable assets, which are essential in supporting organization's strategic objectives and, therefore, recognizes its obligations to protect information from internal and external threats and recognizes that effective information security management is critical in order to ensure the successful enablement of ICT and delivery of business functions and services.
SM is committed to preserve the confidentiality, integrity and availability of all physical and electronic assets, throughout the complete information lifecycle, from acquisition/creation, through to utilization, storage, transfer and disposal. This comprehensive protection of all information assets is accomplished through the establishment, maintenance and continuous update of an information security management system that must be:

- Appropriate to the organization's business purpose
- Commensurate against the inherent risk to and/or value of the information
- Continually monitored, evaluated for every performance and improved

SM's information security policy objectives are:

- to provide direction and support for ICT security in accordance with business requirements, regulations and legal requirements;
- to state the responsibilities of staff, partners, contractors and any other individual or organization having access to the Company's ICT systems;
- to state management intent to support the goals and principles of security in line with business strategy and objectives;
- to provide a framework by which the confidentiality, integrity and availability of ICT resources can be protected;
- to optimize the management of risks, by preventing and minimizing the impact of ICT security incidents;
- to ensure that all breaches of ICT security are properly reported, investigated and appropriate action taken where required;
- to ensure that supporting ICT security policies and procedures are regularly reviewed to guarantee continuous respect of good security practices and protection against new threats;
- to ensure ICT information security requirements are regularly notified to all relevant parties.

SM with the aim of ensuring the abovementioned objectives and certifying the security of information related to the services provided to its customers, is committed to maintain an Information Security Management System (ISMS), in accordance with the standard ISO 27001, which allows the Company to:

- guarantee the security of information and its exchange, whether internal or external to the Company;
- define the roles and responsibilities of users with regard to ICT security, also through the promotion of the culture of ICT security, as well as through the issuance and updating of related rules and procedures;
- prepare adequate measures to prevent unauthorized access, mitigating the risk of data loss, damage, theft, compromise of electronic data;
- manage in a timely and effective way the events related to ICT security, guaranteeing the protection of Company processes and activities;
- ensure the compliance of the system with the mandatory regulations and the objectives of the Management.

The processes that will be subject to certification have been identified among the activities carried out by the Company. These processes are the design, production, maintenance and technical assistance of equipment

for on-board systems of aircraft and military vehicles. For the definition of the scope of the certification, the Company considered the following elements:

- services provided by the Company;
- external and internal factors that have a bearing on the definition of the Company's goals and strategic directions;
- stakeholder requirements relevant to the ISMS.

While carrying out the services and activities for its Customers, SM aims at creating value for Internal Customers and Stakeholders, in strict compliance with current regulations and fundamental principles such as:

- assurance of continuity and reliability of service;
- timeliness and effectiveness of ordinary and extraordinary management, as well as the management of emergencies;
- managerial and holistic approach to the processes;
- management and care of risks intercepted by continuous analyses of the context of the organization, of the needs and expectations of the interested parties;
- high technological and professional level;
- customer focus;
- habitual and widespread use of control and information systems;
- adoption of safety management systems in compliance with international standards, together with a constant commitment to the continuous improvement of their effectiveness.

Therefore, the Company is committed to optimizing business processes and investing in research and innovation in order to ensure the management according to criteria of efficiency, effectiveness and economy, increasing the security of information technology related to the services provided.
The management promotes the involvement of the personnel, because convinced and aware participation is a necessary condition for the implementation of any prevention program and for the diffusion of the safety culture. In addition, the Company's management is committed to ensure that all employees are educated and updated on safety issues.
The Company also undertakes to maintain an open and constructive attitude towards Customers, Public Authorities and other interested parties, also through the implementation of communication campaigns suited to the various interlocutors, identifying appropriate and effective communication channels.

La politica di sicurezza delle informazioni di Secondo Mona (di seguito, "SM" o "organizzazione" o "la Società") è progettata per fornire una protezione adeguata e una chiara responsabilità nella gestione di tutti i beni e di tutte le informazioni di SM.

SM ritiene che i sistemi e le informazioni ICT siano risorse essenziali per sostenere gli obiettivi strategici dell'organizzazione e, pertanto, ha ritenuto necessario potenziare il proprio sistema di protezione delle informazioni da minacce interne ed esterne.
La gestione efficace della sicurezza delle informazioni è fondamentale per garantire una corretta comunicazione e conservazione delle stesse.

SM si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutte le risorse fisiche ed elettroniche, durante l'intero ciclo di vita delle informazioni, dall'acquisizione/creazione, attraverso l'utilizzo, lo stoccaggio, il trasferimento e lo smaltimento. Questa protezione completa di tutte le risorse informative si realizza attraverso la creazione, il mantenimento e l'aggiornamento continuo di un sistema di gestione della sicurezza delle informazioni che deve essere:
- Adeguato allo scopo commerciale dell'organizzazione
- Commisurato al rischio intrinseco e/o al valore delle informazioni
- Continuamente monitorato, valutato per ogni prestazione ed eventualmente migliorato

Gli obiettivi della politica di sicurezza delle informazioni di SM sono:

- fornire supporto per la sicurezza ICT in conformità con i requisiti aziendali, i regolamenti e i requisiti legali;
- dichiarare le responsabilità del personale e di qualsiasi altro individuo o organizzazione che abbia accesso ai sistemi ICT dell'azienda;
- dichiarare l'intento del management di sostenere gli scopi e i principi della sicurezza in linea con la strategia e gli obiettivi aziendali;
- fornire un quadro di riferimento per proteggere la riservatezza, l'integrità e la disponibilità delle risorse ICT;
- ottimizzare la gestione dei rischi, prevenendo e minimizzando l'impatto degli incidenti di sicurezza ICT;
- assicurare che tutte le violazioni della sicurezza ICT siano adeguatamente segnalate, investigate e che siano intraprese azioni appropriate ove richiesto;
- assicurare che le politiche e le procedure di sicurezza ICT di supporto siano regolarmente aggiornate per garantire il continuo rispetto delle buone pratiche di sicurezza e la protezione contro nuove minacce;
- assicurare che i requisiti di sicurezza delle informazioni ICT siano regolarmente notificati a tutte le parti interessate.

SM con l'obiettivo di garantire i suddetti obiettivi e certificare la sicurezza delle informazioni relative ai servizi forniti ai propri clienti, si impegna a mantenere un Sistema di Gestione della Sicurezza delle Informazioni (ISMS), in conformità con la norma ISO 27001, che le permette di:

- garantire la sicurezza delle informazioni e il loro scambio, sia interno che esterno all'azienda;
- definire i ruoli e le responsabilità degli utenti in materia di sicurezza informatica, anche attraverso la promozione della cultura della sicurezza informatica, nonché attraverso l'emanazione e l'aggiornamento delle relative regole e procedure
- predisporre adeguate misure per prevenire accessi non autorizzati, mitigando il rischio di perdita di dati, danneggiamento, furto, compromissione dei dati elettronici;

- gestire in modo tempestivo ed efficace gli eventi legati alla sicurezza informatica, garantendo la protezione dei processi e delle attività aziendali;
- assicurare la conformità del sistema con le normative obbligatorie e gli obiettivi della Direzione.

I processi che saranno soggetti a certificazione sono stati identificati tra le attività svolte dall'azienda. Tali processi sono la progettazione, la produzione, la manutenzione e l'assistenza tecnica di equipaggiamenti per impianti di bordo di aeromobili e di veicoli militari. Per la definizione dello scopo della certificazione, la Società ha considerato i seguenti elementi:

- servizi forniti dalla Società;
- fattori esterni ed interni che influiscono sulla definizione degli obiettivi e degli indirizzi strategici della Società;
- requisiti degli stakeholder rilevanti per l'ISMS.

Nello svolgimento dei servizi e delle attività SM mira a creare valore per i clienti e per gli stakeholder, nel rigoroso rispetto delle normative vigenti e dei principi fondamentali quali:

- garanzia di continuità e affidabilità del servizio;
- tempestività ed efficacia della gestione ordinaria e straordinaria, nonché della gestione delle emergenze;
- approccio manageriale e olistico dei processi;
- gestione e cura dei rischi intercettati da continue analisi del contesto dell'organizzazione, dei bisogni e delle aspettative delle parti interessate;
- alto livello tecnologico e professionale;
- attenzione al cliente;
- utilizzo abituale e diffuso di sistemi di controllo e di informazione;
- adozione di sistemi di gestione della sicurezza conformi agli standard internazionali, unitamente ad un costante impegno al miglioramento continuo della loro efficacia.

Pertanto, la Società si impegna ad ottimizzare i processi aziendali e ad investire nella ricerca e nell'innovazione al fine di garantire la gestione secondo criteri di efficienza, efficacia ed economicità, aumentando la sicurezza delle tecnologie informatiche relative ai servizi erogati.

La direzione promuove il coinvolgimento del personale, perché la partecipazione convinta e consapevole è condizione necessaria per l'attuazione di qualsiasi programma di prevenzione e per la diffusione della cultura della sicurezza. Inoltre, la direzione della Società si impegna a garantire la formazione e l'aggiornamento di tutti i dipendenti sui temi della sicurezza.

La Società si impegna a mantenere un atteggiamento aperto e costruttivo nei confronti dei clienti, delle Pubbliche Autorità e delle altre parti interessate, anche attraverso la realizzazione di campagne di comunicazione adeguate ai diversi interlocutori, individuando canali di comunicazione adeguati ed efficaci.