Avio Aero
a GE Aerospace company



Part-IS Information Security Policy

Politica inerente ai principi guida di sicurezza delle informazioni per la gestione dei rischi con potenziale impatto sulla Aviation Safety, con la definizione di obiettivi, ruoli, responsabilità e metodologie.

Policy relating to the guiding principles of information security for the management of risks with a potential impact on Aviation Safety, defining objectives, roles, responsibilities and methodologies.

Avio Aero Proprietary Information
The information contained in this document is GE Avio S.r.l. and its subsidiaries (hereinafter collectively referred to as “Avio Aero”) proprietary information and is disclosed in confidence. It is the property of Avio Aero and shall not be used, disclosed to others or reproduced without the express written consent of Avio Aero, including, but without limitation, it is not to be used in the creation, manufacture, development, or derivation of any repairs, modifications, spare parts, designs, or configuration changes or to obtain EASA, FAA or any other government or regulatory approval to do so. If consent is given for reproduction in whole or in part, this notice and the notice set forth on each page of this document shall appear in any such reproduction in whole or in part.
This document is considered to contain No Technical Data

Preparato da/*Prepared by*:

Gianluca Tirone
Cyber Risk Manager
(CTR Governance, Risk and compliance)

Paola Giordano
(Policy, Management system)

Controllato da/*Checked by*:

Ivano Di Conca
(Information Security Manager)
(CISO)

Giulio Favilla
(Company Safety Manager)

Approvato da/A*pproved by*:

Francesco Maciariello
(Head of Design DOA)

Riccardo Procacci
(CEO, Accountable Manager POA, MOA)

Gestione delle Modifiche / Modification History

Ediz.	Rev.	Data Modifica	Oggetto	Approvazione GE Avio
1	-	Ott-2025 *Oct-2025*	Prima Edizione *First Edition*	Vedasi prima pagina *See cover page*
			-	
			-	

Sommario / Summary

Gestione delle Modifiche / Modification History 3
Sommario / Summary 3
1. Politica per la Sicurezza delle Informazioni / Information Security Policy 4
1.1. Applicabilità e limitazioni / Applicability and limitations 6
1.2. Documenti applicabili e correlazioni / Applicable documents and correlations 6
2. Principi di Sicurezza delle informazioni / Information Security Principles 7
3. Obiettivi di Sicurezza delle informazioni / Information Security Objectives 9
4. Impegno della Direzione / Management Commitment 10
5. Monitoraggio e Miglioramento Continuo / Monitoring and Continuous Improvement 13

1. Politica per la Sicurezza delle Informazioni / Information Security Policy

Avio Aero (termine che in questo documento raggruppa le legal entites del gruppo: GE Avio S.r.l. e Avio Polska z.o.o.) è un business di GE Aerospace che opera nella progettazione, produzione e manutenzione di componenti e sistemi di propulsione per l'aeronautica civile e militare. La principale sfida è quella di sviluppare nuove tecnologie per applicazioni su architetture in grado di ridurre i consumi energetici, rendere i motori aerei sempre più leggeri e consentire migliori prestazioni. Avio Aero è da sempre impegnata nel raggiungimento di risultati e di obbiettivi basati su alti standard di sicurezza dei propri prodotti e servizi, nel totale rispetto di normative internazionali e in conformità a leggi e regolamenti.

La primaria importanza che riveste la sicurezza di prodotti e dei servizi non è avulsa da una rigorosa politica della sicurezza delle informazioni, così come richiesto dal Delegated Regulation (EU) 2022/1645 e dal Implementing Regulation (EU) 2023/203, conosciuti come "Part-IS".

Infatti, come l'investimento in tecnologie dell'informazione e della comunicazione sempre più innovative è diventato fondamentale per lo svolgimento delle proprie attività e per la costruzione del proprio know-how, altrettanto fondamentale è diventato l'investimento in tecnologie sicure e in misure sempre più efficaci in grado di minimizzare i rischi di Information Security che possono avere impatti sulla Aviation Safety.

A tal fine Avio Aero ha implementato un ISMS definendo procedure, ruoli e responsabilità per garantire l'adempimento ai requisiti Part-IS; in casi specifici sono inoltre utilizzate delle istruzioni mirate a dettagliare come devono essere implementate le regole specificate nelle procedure.

Tutto il contenuto del ISMS è in linea con il Codice di condotta aziendale inerente le regole di conformità e di integrità (The Spirit and The Letter) e con le Policy che regolamentano le modalità di utilizzo delle risorse informatiche (Acceptable Use Policy).

Avio Aero si impegna alla diffusione e applicazione della presente Policy e dei suoi principi. Essa viene rivista almeno annualmente ed aggiornata per assicurare che rimanga in linea con l'organizzazione e le normative di riferimento.

Avio Aero (a term that in this document encompasses the legal entities of the group: GE Avio S.r.l. and Avio Polska z.o.o.) is a business of GE Aerospace that operates in the design, production, and maintenance of components and propulsion systems for civil and military aviation. The main challenge is to develop new technologies for applications on architectures capable of reducing energy consumption, making aircraft engines increasingly lighter, and enabling better performance. Avio Aero has always been committed to achieving results and objectives based on high safety standards for its products and services, in full compliance with international regulations and in conformity with laws and regulations.

The primary importance of product and service safety is closely tied to a rigorous information security policy, as required by Delegated Regulation (EU) 2022/1645 and Implementing Regulation (EU) 2023/203, also known as "Part-IS".

In fact, just as investment in increasingly innovative information and communication technologies has become essential for carrying out activities and building know-how, equally essential has become investment in secure technologies and increasingly effective measures capable of minimizing Information Security risks that could impact Aviation Safety.

To this end, Avio Aero has implemented an ISMS (Information Security Management System), defining procedures, roles, and responsibilities to ensure compliance with Part-IS requirements. In specific cases, targeted instructions are also used to detail how the rules specified in the procedures should be implemented.

The entire content of the ISMS aligns with the corporate Code of Conduct regarding compliance and integrity rules (The Spirit and The Letter) and with the Policies governing the use of IT resources (Acceptable Use Policy).

Avio Aero is committed to the dissemination and application of this Policy and its principles. This Policy is reviewed at least annually and updated to ensure it remains aligned with the organization and applicable regulations.

1.1. Applicabilità e limitazioni / Applicability and limitations

La presente Policy copre tutto il patrimonio informativo aziendale per il quale la mancanza di sicurezza può avere impatto sulla l'Aviation Safety. Ciò include processi, mezzi tecnici, materiali e attività umane atti al trattamento[1] delle informazioni all'interno di Avio Aero.

This Policy covers all corporate information assets for which a lack of security could impact Aviation Safety. This includes processes, technical means, materials, and human activities used to process[1] information within Avio Aero.

1.2. Documenti applicabili e correlazioni / Applicable documents and correlations

[1] 0095Q Safety Policy and Safety Objectives
[2] S&L (Spirit & Letter)
[3] Acceptable Use Policy (Policy per l'uso accettabile risorse informatiche di GE)
[4] IP01 Managing Proprietary Information & Intellectual Property Protection
[5] European Commission Delegated Regulation (EU) 2022/1645
[6] European Commission Implementing Regulation (EU) 2023/203

[1] Con il termine "trattamento" si intende qualunque operazione o complesso di operazioni, effettuati con l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati e informazioni
The term processing is hereby used to mean any operation performed on an IT system to the collect, record, organize, store, consult, process, modify, select, extract, compare, use, interconnect, block, communicate, disseminate, erase and destruct of data both in partial form and aggregate form (information / macro data).

2. Principi di Sicurezza delle informazioni / Information Security Principles

Il patrimonio informativo in scope per la presente Policy è reso sicuro garantendo i tre attributi di sicurezza fondamentali:

- RISERVATEZZA: deve essere garantita l'accessibilità dell'informazione solo alle persone autorizzate, sulla base del principio del "Need-to-know" – necessità di conoscere.
- INTEGRITÀ: deve essere garantita l'accuratezza, la completezza e la protezione dell'informazione contro modifiche non autorizzate.
- DISPONIBILITÀ: deve essere garantita l'accessibilità dell'informazione agli utenti autorizzati sempre e ovunque ne abbiano bisogno.

Per alcune particolari categorie di informazioni può rendersi necessario anche garantire l'AUTENTICITA' delle informazioni, cioè la possibilità di verificare con certezza l'identità dell'origine dell'informazione.

Avio Aero garantisce la sicurezza delle informazioni in ambito attraverso l'implementazione di controlli che rispettano i seguenti principi:

1. **Risk Analysis per nuovi progetti IT/DT:** in occasione di ogni nuovo progetto IT/DT, deve essere svolta un'analisi dei rischi, al fine di implementare le misure di protezione idonee, già nella fase di test del progetto. Ciò anche al fine di valutare eventuali potenziali impatti sulla safety causati da minacce alla sicurezza delle informazioni.
2. **Risk Analysis periodica:** una idonea analisi dei rischi sulla sicurezza delle informazioni deve essere ripetuta periodicamente. L'ambito delle minacce, gli asset e le minacce considerate dovranno essere commisurate alle esigenze alla base della necessità dell'analisi (alcuni esempi non esaustivi sono: compliance alla direttiva NIS2, analisi dei rischi inerenti un particolare insieme di dati affidato da un cliente all'azienda, analisi di tutti gli eventuali potenziali impatti sulla safety causati da minacce alla sicurezza delle informazioni).
3. **Controllo accessi fisici**: tutti gli accessi fisici, in particolar modo alle aree più critiche, devono essere sottoposti a controllo dell'accesso e tutte le risorse informatiche che supportano i processi critici devono essere ubicate in locali sicuri, secondo i criteri propri del "Disaster Recovery" e della "Business Continuity".
4. **Controllo accessi logici**: l'accesso logico al sistema informativo deve avvenire tramite l'assegnazione e l'utilizzo di credenziali di identificazione ed autenticazione personali.
5. **Need-to-Know e Least Privilege***:* l'accesso logico e/o fisico è stabilito sulla base della necessità di conoscere e del minimo privilegio (in modo tale da consentire solo l'accesso e l'utilizzo delle risorse strettamente indispensabili) e la sua gestione è garantita dal principio della SoD – Segregation of Duties (separazione di compiti e responsabilità in modo tale che

azioni critiche non siano svolte per intero dalla stessa persona ma siano divise tra più soggetti (a titolo di esempio si cita il caso della separazione tra l'implementazione di modifiche ad un software, la loro messa in opera e il loro controllo).

6. **Tracciabilità**: gli strumenti di controllo degli accessi devono garantire la tracciabilità delle azioni effettuate a tutela delle attività svolte e nel rispetto delle normative di legge.
7. **Incident Identification and Mitigation**: devono essere implementati strumenti e procedure in grado di consentire l'identificazione degli incidenti di sicurezza delle informazioni e la misura del loro impatto, al fine di poter controllare e mitigare gli effetti, ripristinare al più presto il normale funzionamento dei servizi impattati e prevenire la loro riproposizione.
8. **Security by Design**: devono essere rispettati i principi di "Security by Design" come richiesto nelle principali normative e standard internazionali.

The information assets in scope for this Policy are secured by guaranteeing the three fundamental security attributes:

- *CONFIDENTIALITY: Accessibility to information must be guaranteed only to authorized individuals, based on the principle of "Need-to-know" – the necessity to know.*
- *INTEGRITY: Accuracy, completeness, and protection of information against unauthorized modifications must be guaranteed.*
- *AVAILABILITY: Accessibility to information must be guaranteed to authorized users whenever and wherever they need it.*

For certain specific categories of information, it may also be necessary to ensure the AUTHENTICITY of the information, meaning the ability to verify with certainty the identity of the information's origin.

Avio Aero ensures security of the information in scope through the implementation of controls that adhere to the following principles:

1. ***Risk Analysis for New IT/DT Projects**: For every new IT/DT project, a risk analysis must be conducted to implement appropriate protection measures during the testing phase of the project. This also serves to evaluate potential impacts on safety caused by information security threats.*
2. ***Periodic Risk Analysis**: A suitable risk analysis for information security must be repeated periodically. The scope of threats, assets, and risks considered should be proportional to the needs underlying the analysis. Examples include compliance with the NIS2 directive, risk analysis for specific datasets entrusted by a customer to the company, and evaluation of potential impacts on safety caused by information security threats.*

3. ***Physical Access Control****: All physical access, especially to critical areas, must be subject to access control. All IT resources supporting critical processes must be located in secure facilities, in accordance with "Disaster Recovery" and "Business Continuity" criteria.*
4. ***Logical Access Control****: Logical access to the information system must occur through the assignment and use of personal identification and authentication credentials.*
5. ***Need-to-Know and Least Privilege****: Logical and/or physical access is established based on the principles of "Need-to-know" and "Least Privilege," allowing access only to resources strictly necessary. Its management is ensured by the principle of SoD – Segregation of Duties (separation of tasks and responsibilities so that critical actions are not performed entirely by one person but are divided among multiple individuals, e.g., separating software modification implementation, deployment, and control).*
6. ***Access Control Traceability****: Access control tools must ensure traceability of actions performed to safeguard activities and comply with legal regulations.*
7. ***Incident Identification and Mitigation****: Tools and procedures must be implemented to identify information security incidents and measure their impact, enabling control and mitigation of effects, prompt restoration of normal service operations, and prevention of recurrence.*
8. ***Security by Design:*** *The principles of "Security by Design" must be respected, as required by major international regulations and standards.*

3. Obiettivi di Sicurezza delle informazioni / Information Security Objectives

Avio Aero ha individuato i seguenti obiettivi per la sicurezza delle informazioni:

1. incoraggiare la diffusione della “Just Culture” anche in relazione alla sicurezza delle informazioni. Tutti gli utenti del sistema informativo di AvioAero devono essere incoraggiati a riportare, attraverso gli opportuni canali, eventi anomali o sospetti e incidenti osservati, riguardanti la sicurezza delle informazioni;
2. promuovere la consapevolezza e la formazione degli utenti sensibilizzandoli sugli aspetti relativi alle minacce ed alla sicurezza dell’informazione;

3. assicurare una gestione proattiva dei rischi che ne garantisca un'adeguata mitigazione, anche in accordo con le policy di Aviation Safety;
4. favorire il coinvolgimento delle terze parti nella gestione dei rischi di Information Security;
5. favorire una pronta gestione degli incidenti di sicurezza delle informazioni, assicurando la condivisione dei dettagli rilevanti con le parti interessate e le Autorità competenti.

Il raggiungimento di tali obiettivi viene monitorato tramite opportuni KPI, come specificato nel paragrafo 5, dedicato al monitoraggio dell' Information Security Management System e al suo miglioramento continuo.

Avio Aero has identified the following objectives for information security:

1. *encourage the dissemination of "Just Culture" in relation to information security. All users of Avio Aero's information system should be encouraged to report, through appropriate channels, any observed anomalous or suspicious events and incidents related to information security;*
2. *promote user awareness and training by raising awareness of threats and information security aspects;*
3. *ensure proactive risk management that guarantees adequate mitigation, in alignment with Aviation Safety policies;*
4. *facilitate the involvement of third parties in Information Security risk management;*
5. *support prompt management of Information Security incidents, ensuring the sharing of relevant details with stakeholders and competent authorities.*

The achievement of these objectives is monitored through appropriate KPIs, as specified in paragraph 5, which is dedicated to monitoring the Information Security Management System and its continuous improvement.

4. Impegno della Direzione / Management Commitment

La Direzione di Avio Aero si impegna a garantire il perseguimento degli obiettivi elencati nel paragrafo 3 e il rispetto dei principi esposti nel paragrafo 2. A questo scopo la Direzione:

1. Comunica e rende disponibili i contenuti e principi della presente Policy ai dipendenti e alle Terze Parti coinvolte nel processo, in modo da renderli consapevoli dell'importanza del proprio patrimonio informativo. A tal proposito, promuove campagne di Information Security Awareness e programmi di training periodici, in collaborazione con gli enti aziendali preposti.

2. Predispone tutti i mezzi necessari e tutte le risorse per assicurare la protezione dell'informazione, definendo chiaramente i ruoli associati alla sicurezza delle informazioni, necessari a contrastare proattivamente, con un approccio risk-based le minacce provenienti sia dall'interno che dall'esterno.
3. Riconosce che la sicurezza delle informazioni rappresenta un elemento fondamentale della propria gestione operativa e strategica. Di conseguenza, la Direzione si impegna ad assegnare la sicurezza delle informazioni come una responsabilità essenziale per tutti i manager, agendo in modo tale che le considerazioni di sicurezza siano integrate nei processi decisionali, nelle attività operative quotidiane e nella supervisione del personale all'interno delle rispettive aree di competenza.
4. Si assicura che gli obiettivi di sicurezza definiti nella presente Policy siano perfettamente allineati con gli obiettivi strategici di business e ai fabbisogni di Avio Aero. Pertanto, facilita il raggiungimento di un equilibrio tra il livello di rischio accettato ed il livello di investimento necessario alla riduzione di tale rischio.
5. Si assicura che le attività dell'azienda siano svolte nel rispetto:
    a. di leggi e regolamenti nazionali ed internazionali applicabili e di eventuali modifiche/aggiornamenti;
    b. dei regolamenti e disposizioni interne;
    c. degli obblighi contrattuali.
6. Favorisce l'adozione e il mantenimento di una Just Culture, nella quale le persone siano motivate a segnalare eventi, vulnerabilità e debolezze ed anche errori commessi da loro stesse in ambito sicurezza delle informazioni senza timore di ritorsioni o punizioni, quando le azioni compiute sono generate da errori non intenzionali. Questo approccio è ritenuto essenziale per favorire l'apprendimento organizzativo e il miglioramento continuo della sicurezza.
7. Implementa periodiche analisi del rischio, condotte in modo conforme alle normative di riferimento del contesto, al fine di individuare le misure di sicurezza atte a rilevare, prevenire, contrastare le minacce che possono avere impatto sulla Aviation Safety.
8. Promuove il miglioramento continuo.

The Management of Avio Aero is committed to ensuring the achievement of the objectives listed in paragraph 3 and adherence to the principles outlined in paragraph 2. To this end, the Management:

1. *Communicates and makes the contents and principles of this Policy available to employees and Third Parties involved in the process, raising awareness of the importance of their informational assets. To this purpose, it promotes Information Security Awareness campaigns and periodic training programs in collaboration with the relevant corporate entities.*
2. *Provides all necessary means and resources to ensure the protection of information, clearly defining the roles associated with information security, necessary to proactively counter, with a risk-based approach, threats originating both internally and externally.*
3. *Recognizes that information security is a fundamental element of its operational and strategic management. Consequently, Management commits to assigning information security as an essential responsibility for all managers, ensuring that security considerations are integrated into decision-making processes, daily operational activities, and personnel supervision within their respective areas of competence.*
4. *Ensures that the security objectives defined in this Policy are perfectly aligned with Avio Aero's strategic business goals and needs. Therefore, it facilitates achieving a balance between the accepted risk level and the investment level needed to reduce that risk.*
5. *Ensures that the company's activities comply with:*
    a. *applicable national and international laws and regulations, including any modifications/updates;*
    b. *internal regulations and provisions;*
    c. *contractual obligations.*
6. *Encourages the adoption and maintenance of a Just Culture, where individuals are motivated to report events, vulnerabilities, weaknesses, and even errors they have made in the context of information security without fear of retaliation or punishment, provided the actions were unintentional errors. This approach is considered essential for fostering organizational learning and continuous security improvement.*

7. *Conducts periodic risk analyses in compliance with relevant regulatory frameworks to identify security measures aimed at detecting, preventing, and countering threats that could impact Aviation Safety.*

8. *Promotes continuous improvement.*

5. Monitoraggio e Miglioramento Continuo / Monitoring and Continuous Improvement

Avio Aero adotta un processo di monitoraggio continuo del proprio ISMS per comprendere se e quanto le misure di sicurezza implementate risultano efficaci ed efficienti, riuscendo a tradurre in modalità misurabile, confrontabile e ripetibile nel tempo lo “stato di salute” del sistema.

Avio Aero è dotata di un sistema di indicatori (KPI) che consentono di valutare il raggiungimento degli obiettivi elencati nel paragrafo 3. Ciò è fondamentale per determinare l’andamento del ISMS e delle relative iniziative; sono inoltre condotti degli audit interni periodici per monitorare l’adozione delle corrette procedure nei vari processi aziendali interessati dal dover garantire la sicurezza delle informazioni. Una revisione periodica è attuata dalla Direzione, al fine di individuare azioni di miglioramento continuo da svolgere sul ISMS. La revisione tiene conto dei risultati della fase di controllo e monitoraggio della sicurezza delle informazioni e delle evoluzioni potenziali nelle minacce e nei rischi.

Avio Aero adopts a continuous monitoring process for its ISMS (Information Security Management System) to assess whether and how effectively and efficiently the implemented security measures are performing. This process translates the "health status" of the system into a measurable, comparable, and repeatable format over time.

Avio Aero has a system of indicators (KPIs) that allow the evaluation of the achievement of the objectives listed in paragraph 3. This is essential for determining the performance of the ISMS and its related initiatives. Additionally, periodic internal audits are conducted to monitor the adoption of correct procedures across various business processes involved in ensuring information security. A periodic review is carried out by Management to identify continuous improvement actions for the ISMS. This review takes into account the results of the Information Security control and monitoring phase, as well as potential developments in threats and risks.