

CYBERSECURITY POLICY

1. Scopo

La presente Cybersecurity Policy definisce i principi, le responsabilità e le misure adottate da GEAC S.p.A. per garantire la protezione dei sistemi informativi e dei dati a supporto delle attività aeroportuali, in conformità:

- alla Direttiva (UE) 2022/2555 (NIS2) e alla normativa italiana di recepimento D.Lgs. 138/2024
- al Reg. (UE) 2022/1645
- al Reg. (UE) 2016/679 (GDPR)
- al Manuale ISMS aziendale

L'obiettivo è garantire la riservatezza, integrità, disponibilità e resilienza dei sistemi e delle informazioni con potenziale impatto sulla sicurezza aerea e sulla continuità operativa.

La politica è finalizzata a preservare:

- la riservatezza delle informazioni;
- l'integrità dei dati e dei sistemi;
- la disponibilità delle informazioni e dei servizi;
- l'autenticità delle informazioni;
- la tracciabilità delle attività;
- la protezione dei dati personali;
- la continuità operativa dei processi aziendali.

2. Ambito di applicazione

La presente politica si applica a:

- dipendenti;
- collaboratori;
- consulenti;
- amministratori;
- fornitori;
- partner commerciali;
- soggetti terzi che accedono a dati, informazioni o sistemi aziendali.

Chiunque utilizzi risorse informative e tecnologiche dell'Organizzazione è tenuto al rispetto delle disposizioni contenute nella presente politica e nelle procedure ad essa collegate.

3. Principi generali

GEAC S.p.A. la sicurezza informatica e delle informazioni come elemento essenziale per il raggiungimento degli obiettivi aziendali e si impegna a garantire:

- **Riservatezza.** Le informazioni sono accessibili esclusivamente ai soggetti autorizzati.
- **Integrità.** I dati e le informazioni sono protetti contro modifiche, alterazioni o cancellazioni non autorizzate.

Rev. 00 del 20/07/2026

- Disponibilità. Le informazioni e i servizi sono disponibili agli utenti autorizzati quando necessario.
- Autenticità. L'origine delle informazioni e delle comunicazioni è verificabile e affidabile.
- Controllo. La gestione delle informazioni avviene attraverso processi formalizzati, sicuri e verificabili.
- Privacy. I dati personali sono trattati nel rispetto della normativa vigente e dei diritti degli interessati.

Il Consiglio di amministrazione, in qualità di organo di amministrazione e controllo, nonché la Direzione generale, sono fortemente impegnati a una grande responsabilizzazione di tutte le persone che lavorano per e con l'Organizzazione nel garantire la rigerosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati. In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:

- il rispetto delle leggi e normative vigenti;
- l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;
- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;
- la riservatezza, la correttezza e la disponibilità dei dati/informazioni gestiti dall'organizzazione e la salvaguardia della proprietà intellettuale;
- l'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

La presente Politica garantisce:

- che l'organizzazione identifichi e protegga i sistemi informatici, le reti, le applicazioni e gli asset tecnologici critici, valutandone periodicamente i rischi e le vulnerabilità;
- che l'accesso ai sistemi informatici e alle risorse digitali avvenga esclusivamente da parte di soggetti autorizzati, secondo i principi di autenticazione, autorizzazione e minimo privilegio;
- che siano adottate misure tecniche e organizzative adeguate a prevenire accessi non autorizzati, alterazioni, perdite, divulgazioni o indisponibilità dei dati e dei sistemi;
- che il personale e i collaboratori siano adeguatamente formati sui rischi cyber, sulle minacce informatiche emergenti e sulle corrette modalità di utilizzo degli strumenti aziendali;
- che i sistemi informatici siano costantemente monitorati al fine di individuare tempestivamente anomalie, vulnerabilità, tentativi di attacco e incidenti di sicurezza;
- che gli incidenti di sicurezza informatica siano gestiti attraverso procedure formalizzate di rilevazione, analisi, contenimento, risoluzione e ripristino delle funzionalità operative;
- che l'infrastruttura tecnologica sia protetta mediante l'adozione di adeguate misure di sicurezza, quali segmentazione delle reti, sistemi di protezione perimetrale, soluzioni antimalware, sistemi di rilevazione delle intrusioni e strumenti di monitoraggio;
- che siano effettuate attività periodiche di gestione delle vulnerabilità, aggiornamento del software e applicazione delle patch di sicurezza;
- che siano implementate procedure di backup, business continuity e disaster recovery idonee a garantire la resilienza operativa e il rapido ripristino dei servizi informatici;
- che i fornitori e i partner che accedono ai sistemi o trattano dati per conto dell'organizzazione rispettino adeguati requisiti di sicurezza informatica;
- che i trattamenti dei dati personali effettuati mediante strumenti informatici siano svolti nel rispetto della normativa vigente in materia di protezione dei dati personali, inclusi i requisiti previsti dal Regolamento (UE) 2016/679 (GDPR);
- che siano definiti, implementati e verificati processi di gestione della sicurezza informatica conformi alle normative applicabili e alle best practice riconosciute a livello nazionale e internazionale;

- che la sicurezza informatica sia oggetto di miglioramento continuo attraverso attività di verifica, audit, monitoraggio delle prestazioni e riesame periodico delle misure adottate.

In attuazione della presente politica e ad essa collegata, GEAC S.p.A. ha adottato e documenta politiche di sicurezza informatica per i seguenti ambiti:

- gestione del rischio;
- ruoli e responsabilità;
- affidabilità delle risorse umane;
- conformità e audit di sicurezza;
- gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
- gestione degli asset;
- gestione delle vulnerabilità;
- continuità operativa, ripristino in caso di disastro e gestione delle crisi;
- gestione dell'autenticazione, delle identità digitali e del controllo accessi;
- sicurezza fisica;
- formazione del personale e consapevolezza;
- sicurezza dei dati;
- sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
- protezione delle reti e delle comunicazioni;
- monitoraggio degli eventi di sicurezza;
- risposta agli incidenti e ripristino.

4. Governance e responsabilità

Il Consiglio di amministrazione e la Direzione aziendale promuovono una cultura della sicurezza e garantiscono la disponibilità delle risorse necessarie per l'attuazione della presente politica.

Sono definiti ruoli e responsabilità per:

- gestione della sicurezza informatica;
- protezione delle informazioni;
- gestione dei rischi;
- gestione degli incidenti;
- continuità operativa;
- monitoraggio della conformità normativa.

Tutto il personale è responsabile dell'utilizzo corretto delle risorse informatiche e della protezione delle informazioni trattate nello svolgimento delle proprie attività.

5. Gestione del rischio

L'Organizzazione adotta un approccio basato sul rischio (risk-based approach) che prevede:

- identificazione degli asset informativi e tecnologici;
- classificazione delle informazioni;

- analisi delle minacce e delle vulnerabilità;
- valutazione e trattamento dei rischi;
- monitoraggio continuo dell'efficacia delle misure adottate;
- riesame periodico dei rischi.

Le misure di sicurezza vengono definite in funzione della criticità degli asset e dell'impatto potenziale sugli obiettivi aziendali.

6. Sicurezza tecnica

L'Organizzazione adotta un modello di difesa multilivello (defence-in-depth) fondato sui seguenti principi:

- minimo privilegio;
- segregazione dei ruoli;
- segregazione delle reti;
- autenticazione e controllo degli accessi;
- monitoraggio continuo;
- protezione delle infrastrutture e degli endpoint;
- gestione delle vulnerabilità;
- registrazione e conservazione dei log di sicurezza.

Tra le principali misure adottate rientrano:

- firewall e sistemi di prevenzione delle intrusioni;
- protezione degli endpoint e dei dispositivi mobili;
- segmentazione delle reti;
- sistemi di monitoraggio e rilevazione degli eventi di sicurezza;
- hardening dei sistemi;
- gestione sicura delle configurazioni;
- aggiornamento e patch management;
- backup periodici con copie protette e, ove applicabile, immutabili;
- protezione fisica delle infrastrutture critiche;
- sistemi di alimentazione e ridondanza per i servizi essenziali.

7. Gestione degli accessi e delle identità digitali

L'accesso alle informazioni e ai sistemi aziendali è concesso esclusivamente agli utenti autorizzati sulla base delle effettive necessità operative. L'Organizzazione garantisce:

- gestione controllata delle identità digitali;
- attribuzione di profili autorizzativi coerenti con le mansioni svolte;
- revisione periodica dei privilegi;
- revoca tempestiva degli accessi non più necessari;
- utilizzo di credenziali sicure e adeguate misure di autenticazione.

8. Gestione degli incidenti di sicurezza

L'Organizzazione mantiene processi e procedure per:

- identificare tempestivamente gli incidenti;
- contenerne gli effetti;
- ripristinare i servizi;
- analizzare le cause;
- prevenire il ripetersi degli eventi.

Ogni evento che possa compromettere la sicurezza delle informazioni deve essere segnalato tempestivamente secondo le procedure aziendali.

Nei casi previsti dalla normativa applicabile, l'Organizzazione provvede alle comunicazioni verso le autorità competenti e agli eventuali adempimenti in materia di protezione dei dati personali.

9. Sicurezza della supply chain

I fornitori e i partner che trattano dati o accedono ai sistemi aziendali sono selezionati e gestiti tenendo conto dei requisiti di sicurezza informatica e protezione delle informazioni.

L'Organizzazione:

- valuta i rischi associati ai fornitori critici;
- definisce requisiti contrattuali di sicurezza;
- limita e monitora gli accessi di terze parti;
- verifica periodicamente il livello di conformità dei fornitori ai requisiti applicabili.

10. Formazione e consapevolezza

La consapevolezza del rischio umano è parte integrante della strategia aziendale.

L'Organizzazione promuove la cultura della sicurezza attraverso:

- programmi di formazione periodica;
- attività di sensibilizzazione;
- diffusione di istruzioni operative;
- aggiornamenti sulle minacce emergenti.

Tutto il personale è tenuto a partecipare alle iniziative formative previste e ad applicare le buone pratiche di sicurezza.

11. Business Continuity e Disaster Recovery

L'Organizzazione adotta misure organizzative e tecniche per garantire la continuità operativa e il ripristino delle attività in caso di eventi avversi. Sono previsti:

- piani di Business Continuity;
- procedure di Disaster Recovery;
- sistemi di backup e ripristino dei dati;

- verifiche periodiche dell'efficacia delle misure adottate;
- test di ripristino e simulazioni di emergenza.

Gli obiettivi di ripristino e recupero dei dati sono definiti in funzione della criticità dei processi e riesaminati periodicamente nell'ambito della gestione del rischio.

12. Conformità, monitoraggio e audit

L'Organizzazione verifica periodicamente l'applicazione della presente politica attraverso:

- attività di monitoraggio;
- controlli interni;
- audit;
- riesami della Direzione;
- valutazione dell'efficacia delle misure di sicurezza adottate.

Eventuali non conformità vengono analizzate e gestite mediante adeguate azioni correttive e di miglioramento.

13. Miglioramento continuo

La sicurezza informatica e delle informazioni è oggetto di miglioramento continuo attraverso:

- monitoraggio delle minacce emergenti;
- aggiornamento delle tecnologie;
- revisione delle procedure;
- apprendimento derivante da incidenti ed eventi significativi;
- adeguamento alle evoluzioni normative e organizzative.

La presente politica è riesaminata almeno annualmente o in occasione di modifiche significative del contesto organizzativo, tecnologico o normativo.