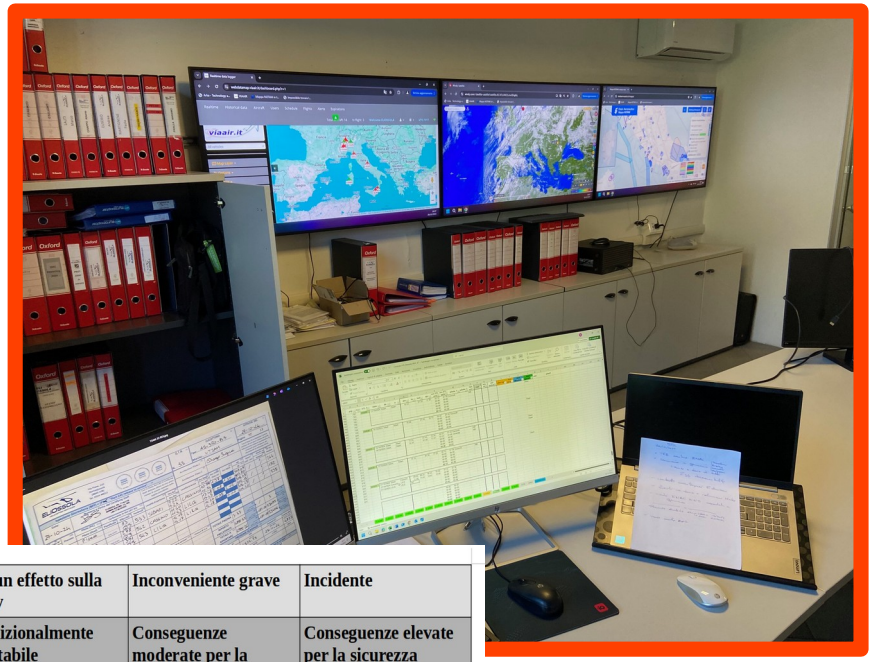
ELIOSSOLA
HELICOPTER SERVICES

Continuous Safety®

Parte-IS

Segnalazione Interna

1) **Accesso non autorizzato:** Qualsiasi istanza in cui un individuo o un sistema non autorizzato ottiene accesso a dati o altri sistemi.
2) **Violazione dei dati:** L'esposizione di informazioni riservate a parti non autorizzate, sia accidentalmente che attraverso azioni malevole.
3) **Infezione da malware:** Rilevamento di virus, worm, ransomware o altro software malevolo sulla rete o sui dispositivi dell'organizzazione.
4) **Attacco di phishing:** Tentativi di ingannare i dipendenti affinché forniscano informazioni sensibili tramite email o siti web fraudolenti.
5) **Perdita o furto di dispositivi:** Incidenti che coinvolgono la perdita o il furto di laptop, smartphone o altri dispositivi contenenti informazioni sensibili.
6) **Modifiche illegali:** Cambiamenti non autorizzati a software, dati o configurazioni di rete.
7) **Account utente compromessi:** Rilevamento di account utente che sono stati accessi o utilizzati senza autorizzazione.
8) **Attività di rete sospetta:** Pattern insoliti di traffico di rete che potrebbero indicare una potenziale minaccia alla sicurezza.
9) **Ingegneria sociale:** Tentativi di manipolare i dipendenti affinché divulghino informazioni riservate o eseguano azioni che compromettono la sicurezza.
10) **Violazioni delle policy:** Istanze in cui dipendenti o appaltatori violano le policy o le procedure di sicurezza dell'organizzazione.
11) **Vulnerabilità di sicurezza delle informazioni:** Identificazione di debolezze in software, hardware o configurazioni di rete che potrebbero essere sfruttate dagli attaccanti.
12) **Minaccia interna:** Azioni malevole o negligenti da parte di dipendenti o appaltatori che compromettono la sicurezza delle informazioni dell'organizzazione.
13) **Controlli di sicurezza falliti:** Rilevamento di controlli di sicurezza che non hanno funzionato come previsto, esponendo potenzialmente l'organizzazione al rischio.



	Nessun effetto sulla safety	Inconveniente grave	Incidente
Scenario di minaccia del potenziale di accadimento	**Condizionalmente accettabile**	**Conseguenze moderate per la sicurezza**	**Conseguenze elevate per la sicurezza**
Alto	Condizionalmente accettabile	Non accettabile	Non accettabile
Medio	Accettabile	Condizionalmente accettabile	Non accettabile
Basso	Accettabile	Accettabile	Condizionalmente accettabile

Costo/beneficio: enorme!

mycs.swiss | *sms@mycs.swiss*

- Volare sicuri, volare meglio – insieme decolliamo verso l'eccellenza!

ELIOSSOLA
HELICOPTER SERVICES

Parte-IS

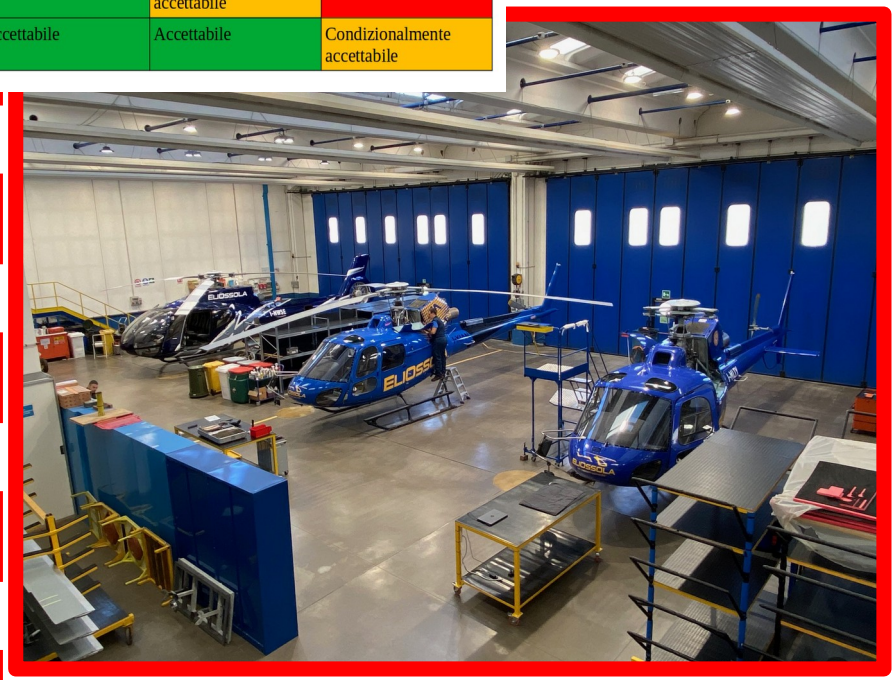
Segnalazione ESTERNA

Continuous Safety®

1) **Tutti gli esempi** sopra elencati (**segnalazioni interne**), che sono considerati avere un potenziale impatto sulla **safety**.
2) **Dirottamento Remoto:** Acquisizione di accesso e controllo di un sistema critico dell'aviazione che porta a informazioni compromesse.
3) **Attacchi alla Catena di Approvvigionamento:** Il compromesso della catena di approvvigionamento per parti di aeromobili può comportare l'introduzione di componenti difettosi o malevoli, impattando sulla **safety** dell'aeromobile.
4) **Compromesso del Sistema di Manutenzione**: L'accesso non autorizzato ai registri di manutenzione degli aeromobili può comportare dati di manutenzione errati o falsificati, portando a potenziali guasti meccanici.
5) **Violazione del Sistema di Intrattenimento di Volo (IFE, se applicabile)**: Sebbene principalmente destinato all'uso dei passeggeri, una violazione nel sistema IFE può fornire una via d'accesso a sistemi più critici dell'aeromobile, ponendo un rischio per la **safety**.
6) **Hacking del Sistema di Indirizzamento e Segnalazione delle Comunicazioni Aeronautiche (ACARS) o simile**: L'accesso non autorizzato all'ACARS può portare alla manipolazione dei piani di volo e delle comunicazioni tra aeromobili e stazioni di terra, potenzialmente causando errori di navigazione e rischi per la **safety**.
7) **Manomissione del Sistema di Gestione del Volo (FMS) o simile sistema**: Gli attacchi informatici mirati all'FMS possono alterare i percorsi di volo, i calcoli del carburante e altri parametri critici di volo, mettendo in pericolo l'operatività sicura dell'aeromobile.

NB: Qualora un software approvato ai sensi della Parte 21 venga compromesso, la segnalazione deve essere effettuata anche presso la POA o la DOA.

	Nessun effetto sulla safety	Inconveniente grave	Incidente
Scenario di minaccia del potenziale di accadimento	**Condizionalmente accettabile**	**Conseguenze moderate per la sicurezza**	**Conseguenze elevate per la sicurezza**
Alto	Condizionalmente accettabile	Non accettabile	Non accettabile
Medio	Accettabile	Condizionalmente accettabile	Non accettabile
Basso	Accettabile	Accettabile	Condizionalmente accettabile



Costo/beneficio: enorme!

mycs.swiss | *sms@mycs.swiss*

- Volare sicuri, volare meglio – insieme decolliamo verso l'eccellenza!