# Part IS

podle Prováděcího nařízení Komise (EU) č. 2023/203

# Proč?

- Letectví je v současnosti výrazně závislé na IT technologiích.
- Vyřazení IT technologií může výrazně ochromit činnost organizací činných v leteckém průmyslu (provoz, ŘZLZ, údržba)
- Nepřátelské útoky na IT infrastrukturu se bohužel staly běžnou součástí našeho života

# Koho se týká?

- Organizace 145 a CAMO s výjimkou těch, které se zabývají pouze letadly podléhajícími Partu ML.
- Letečtí provozovatelé podléhající Annexu III (Part ORO), kromě těch, kteří provozují:
- Letadla ELA2 (do MTOM 2000kg)
- Jednomotorová vrtulová letadla pro max. 5 cestujících, která nejsou složitá a létají z bodu A do bodu A za podmínek VFR
- Jednomotorové vrtulníky pro max. 5 cestujících, které nejsou složité a létají z bodu A do bodu A za podmínek VFR
- Schválené výcvikové organizace ATO, kromě těch, které se poskytují výcvik pouze na letadlech ELA2 nebo poskytují pouze teoretický výcvik
- Letecká zdravotnická centra oprávněná podle Nařízení (EU) 1178/2011
- Provozovatelé simulátorů, kromě provozovatelů simulátorů pro letadla ELA2
- Organizace pro výcvik řídících letového provozu
- Organizace řízení letového provozu, kromě držitelů omezeného oprávnění a poskytovatelů letecké informační služby
- Národní letecké úřady včetně EASA

- Od kdy: nejpozději od 22. února 2026

# Koho se netýká ! (IS.I.OR.200(e)

- Úřad může schválit, že organizace nemusí implementovat Part IS, pokud organizace prokáže, že její aktivity , zařízení, zdroje a služby, které poskytuje, nepředstavují žádné riziko ohledně bezpečnosti informací pro bezpečnost letectví. Toto schválení musí být založeno na zdokumentovaném vyhodnocení informačních rizik, které provedla organizace , nebo třetí strana podle IS.I.OR 205, a které chválil Úřad.

# Kde najdeme?

- Na webu EASA.Europa.eu

https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-information-security?page=6#_Toc256000097

- Nařízení je i v ČJ, AMC jenom v AJ

# Příručka řízení bezpečnosti informací (ISSM) - IS.I.OR.250

- Možno udělat separátní  příručku
- Možno začlenit do Příručky systému řízení (SSM)
- Možno začlenit do MOE/CAME

- <u>Obsahuje (Viz IS.I.OR.250):</u>

- Prohlášení odpovědného vedoucího

- Jmenování  Information Safety Manažera a případně dalších jmenovaných vedoucích  – viz  IS.I.OR.250 (a) (4)

- Seznam klíčových osob (funkcí) odpovědných za provádění aktivit podle IS.I.OR.200

# Příručka řízení bezpečnosti informací (ISSM) - IS.I.OR.250

- Organizační schéma
- Popis systému interních hlášení
- Postupy upřesňující dokumentaci, kontrolu smluvních činností, změny ISSM

*AMC se strukturou příručky zatím vydáno nebylo*

# Co to obnáší? (IS.I.OR.200)

- Analogicky s SMS systémem implementovat specifický SMS systém orientovaný na  bezpečnost informatiky, který se skládá z:

1) Zavedení politiky bezpečnosti informací

2) Identifikování a přezkoumávání rizik bezpečnosti informací (IS.I.OR.205)

3) Definování a provádění opatření k řešení těchto rizik (IS.I.OR.210)

4) Implementování systému hlášení událostí (IS.I.OR.215)

5) Definování a implementace opatření pro zjištění bezpečnostních událostí , které mohou mít dopad na bezpečnost letectví (IS.I.OR.245)

# Co to obnáší? (IS.I.OR.200)

6) Implementace opatření  stanovených úřadem jako okamžitou reakci na bezpečnostní incident

7) Přijetí opatření podle IS.I.OR.225 k vyřešení nálezů, které učinil příslušný úřad

8) Zavedení systému externích bezpečnostních hlášení podle IS.I.OR.230

9) Zajištění souladu s IS.I.OR.235 v případě , že organizace zadává  externí firmě provedení některých opatření podle IS.I.OR.200

10) Zajištění souladu personálních požadavků s IS.I.OR.240

11) Zajištění souladu s požadavky na uchovávání záznamů podle  IS.I.OR.245

# Co to obnáší? (IS.I.OR.200)

12) Monitorování souladu s požadavky nařízení a zajištění zpětné vazby odpovědnému vedoucímu.

13) Zajištění bezpečnosti informací, které organizace převzala od jiného subjektu.

Organizace musí zavést:

- Systém neustálého zlepšování (IS.I.OR 260)
- Dokumentování  všech klíčových procesů, procedur rolí a odpovědností, uchovávání těchto záznamů

# Vyhodnocování rizik (IS.I.OR.205)

a) Organizace vyhodnotí prvky (aktivity, zařízení, zdroje, data), které mohou být vystaveny nebezpečí bezpečnostní události.

b) Organizace identifikuje rozhraní, která mohou tvořit bezpečnostní riziko

c) Na základě analýz a) a b) organizace identifikuje rizika s potenciálním dopadem na bezpečnost letectví, pro tato rizika provede zhodnocení jejich úrovně a spojí každé riziko s konkrétním rozhraním.

d) Organizace zreviduje svou analýzu rizik pokaždé, když dojde ke:

- Změně bodů, které jsou vystaveny rizikům
- Změně rozhraní
- Změně informací o daném riziku
- Získání zkušeností z proběhlých bezpečnostních událostí

# Posouzení rizik- prakticky

- Analogicky s SMS systémem provádět posouzení rizik souvisejících s bezpečností informací:
- Technická rizika spojená s hardwarem ( porucha HW, přepětí v el. síti, úder blesku ….)
- Seznam rozhraní  s vnějším světem a nimi spojená rizika pro informační systém  (viry , hackerské útoky….)
- Připojení na veřejnou internetovou síť
- Používání přenosných datových uložišť (flash disky, přenosné externí disky …)
- E-maily
- Činnost vlastního personálu (navštěvování rizikových stránek)

# Posouzení rizik a jejich redukce

- Analogicky s SMS zjištěná rizika posoudit co do pravděpodobnosti a závažnosti a podle výsledku přijímat opatření a sledovat jejich realizaci a účinnost.
- Při posuzování rizik brát v úvahu jejich dopad na bezpečnost letectví.

# Systém interního hlášení (IS.I.OR.230)

- Organizace vytvoří systém interního hlášení – lze integrovat se systémem hlášení v rámci SMS

# Opatření k odhalení incidentů (IS.I.OR.220)

- Zpracovat technická opatření zajišťující zjištění incidentů a spuštění varování
- Připravit scénáře pro realizaci opatření jako reakce na jednotlivé typy incidentů
- Připravit scénáře opatření, jak bude organizace pracovat po dobu, než je incident vyřešen, jak organizace obnoví ztracená data.

# Reakce na nálezy provedené Úřadem (IS.I.OR.225)

- Analogicky s nálezy běžných auditů

- Identifikovat kořenové příčiny
- Definovat plán nápravných opatření
- Prokázat odstranění neshody

# Systém externího hlášení (IS.I.OR.230)

- Organizace zavede systém podávání hlášení o bezpečnosti informací, který splňuje požadavky stanovené v nařízení (EU) č. 376/2014
- Každý incident v oblasti bezpečnosti informací, který může představovat významné riziko musí být oznámen příslušnému orgánu (ÚCL, UZPLN, NÚKIB?) nejdéle do 72 hodin
- Pokud se incident týká systémů letadla nebo LC- organizace informuje držitele typu letadla/LC
- Pokud se incident týká systémů používaných organizací -organizace informuje firmu odpovídající za design těchto systémů

# Subdodávky aktivit bezpečnosti informací (IS.I.OR.235)

- Pokud organizace zadá některé aktivity  externí firmě, musí být tyto aktivity v souladu s Part IS a zadavatel musí dodavatele dozorovat a musí řídit vzniklá rizika.
- Zadavatel musí zajistit přístup Úřadu k dodavateli za účelem provedení auditu.

# Personální požadavky (IS.I.OR.240)

- AM organizace

- Zajistí potřebné zdroje pro vyhovění požadavkům Part IS
- Vyhlásí a bude prosazovat bezpečnostní politiku
- Prokáže základní porozumění požadavkům Part IS
- Jmenuje osobu/skupinu osob, která zajistí, že organizace bude v souladu s požadavky Part IS, stanoví její pravomoci. Tato osoba/skupina osob bude podléhat přímo AM, musí mít  přiměřené znalosti a zkušenosti.

Detaily viz příslušná AMC

# Uchování záznamů (IS.I.OR.245)

- Viz text nařízení +AMC

# Příručka řízení bezpečnosti informaci (IS.I.OR.250)

- Zatím nejsou žádná AMC
- Prvotní vydání Příručky musí být schváleno úřadem.

# Závěrem

- Termín pro zavedení Part IS- 22.2.2026

- Nenechávat na poslední chvíli- 22.2.2026 už musíte mít Part IS od ÚCL schválený