Gældende fra 19. februar 2026

NAVIAIRS SIKKERHEDSPOLITIK (SECURITY)

Air Navigation Services

Baggrund
Naviair beskæftiger sig med kritisk infrastruktur, og det er derfor væsentligt for Naviair løbende at have fokus på sikkerheden (Security) i virksomheden. Vigtigheden heraf understøttes af, at forretningsordenen for direktionen foreskriver, at Naviair skal have en sikkerhedspolitik.

På denne baggrund instruerer bestyrelsen i Naviair herved direktionen til at tilrettelægge arbejdet med sikkerheden (Security) efter de retningslinjer, der følger af denne politik.

Sikkerhedspolitikken i Naviair har til formål at fastsætte retningslinjerne og sikkerhedsniveauet for beskyttelsen af Naviair.

Politikkens indhold
Sikkerheden (Security) i Naviair skal have et niveau, der understøtter den højeste flyvesikkerhed ved at forudse, identificere og beskytte tjenesterne mod såvel interne som eksterne sårbarheder og trusler.

Sikkerheden (Security) i Naviair skal sikre tjenesternes tilgængelighed, integritet og fortrolighed for medarbejdere og aktiver i et omfang, der modsvarer det aktuelle trusselsniveau ud fra en risikobaseret tilgang, hvor forretningskritiske processer er beskyttet i henhold til Best Practices.

Der skal være etableret et beredskab, der umiddelbart kan hæve sikkerheden, så det modsvarer det aktuelle trusselsniveau.

Sikkerheden (security) omfatter:

- Fysisk sikkerhed
- Personsikkerhed
- Informations- og cybersikkerhed
- Beredskab (security)

Til styring af sikkerheden (security) skal sikkerhedsledelsessystemet opbygges efter internationale standarder og "best practices", der integrerer fysisk sikkerhed, personsikkerhed samt informations- og cybersikkerhed, herunder nye teknologier og fjernarbejdspladser mm.

Med indførelsen af NIS2 (EU 2022/2555) og Part-IS (EU 2023/203) har Naviair etableret et ledelsessystem for informationssikkerhed (ISMS), der omfatter hele virksomheden, og som er certificerbart i henhold til ISO 27001. Naviair har været ISO 27001 certificeret siden 2020.

Ledelsen i Naviair skal sikre, at sikkerhedsorganisationen har fastlagt ansvar, roller og beføjelser.

Naviair skal råde over de nødvendige kompetencer og ressourcer til at opbygge samt vedligeholde sikkerheden (Security) for tjenesterne i Naviair.

Der skal løbende arbejdes med en sikkerhedskultur på alle niveauer i organisationen, der understøtter intentionen med sikkerhedspolitikken.

Sikkerhedsledelsessystemet skal være forankret i den øverste ledelse i Naviair og i resten af organisationen.

Sikkerhedsledelsessystemets retningslinjer i form af processer, procedurer og instrukser skal;

- være proaktive, så de reducerer risikoen fra trusler eller potentielle sårbarheder,
- integreres og koordineres med Safety (flyvesikkerhed), og
- styrkes via samarbejde med branchespecifikke interessenter og myndigheder.

Sikkerhedsorganisationen i Naviair skal;

- kunne identificere relevante sårbarheder og trusler,
- kunne imødegå trusler og sårbarheder ved rettidige beskyttelses-foranstaltninger,
- fastlægge retningslinjerne for sikkerhedskontroller ud fra en risikobaseret tilgang, og
- have et kriseberedskab til håndtering af brud på sikkerheden.

Sikkerheden (Security) skal som standard tages med i betragtning i alle øvrige politikker og strategier i Naviair.

Sikkerhedspolitik og -strategi i Naviair skal offentliggøres og kommunikeres til alle medarbejdere og relevante eksterne parter.

Organisation, ansvar og rapportering
Politikken administreres af Cyber & IT Security (TS) med support fra Legal (FL), og bestyrelsen har det overordnede ansvar for politikkens godkendelse.

Direktionen i Naviair skal mindst to gange årligt give bestyrelsen en status for sikkerheden (Security) og i den forbindelse orientere om væsentlige brud herpå.

Politikken revideres årligt.

--o0o--