Bestyrelsesmøde nr. 134 den 10. april 2026
Pkt. 8, bilag 3

Nationalt Forsvars-teknologisk Center

Sikkerhedsramme for NFC-projekter

1. FORMÅL OG ANSVAR

Nationalt Forsvarsteknologisk Center (NFC)[1] er etableret med henblik på at opbygge forskernetværket hos NFC's partnere på forsvarsområdet samt styrke samarbejdet mellem vidensinstitutioner og virksomheder/myndigheder. Disse formål nødvendiggør en ensartet tilgang til sikkerhed.

NFC's sikkerhedsramme danner et fælles grundlag for NFC's partnere til at håndtere sikkerhedsmæssige perspektiver på tværs af projekter og aktiviteter i NFC-regi[2]. Rammen tager udgangspunkt i de regler og retningslinjer, som universiteter og GTS'er i forvejen er underlagt. På det NFC-definerede *sensitive* sikkerhedsniveau fastsætter sikkerhedsrammen herudover fælles minimumskrav og løsninger. Den enkelte NFC-partner er fortsat ansvarlig for at holde sig opdateret om relevante regelgrundlag og ændringer. Sikkerhedsrammen opdateres ved større regelændringer.

Formålet med rammen er at understøtte en koordineret tilgang til sikkerhed og skabe transparens om de sikkerhedsmæssige foranstaltninger og overvejelser, der er påkrævet for at gennemføre projekter i NFC-regi. Fordi projekter ofte overgår fra ét sikkerhedsniveau til det næste, er det centralt med tidlig opmærksomhed på sikkerhed for at sikre projekternes fremdrift og værdiskabelse.

URIS-retningslinjerne udgør et fundament for sikkerhedsrammen. Eftersom NFC's forskningsprojekter udvikles mhp. en forsvarsmæssig anvendelse og derfor kan have betydning for national sikkerhed, må forskningen som udgangspunkt forventes at kunne betegnes som "kritisk". Der vil dog kunne være nuancer i forskningens modenhed og dermed muligheden for direkte anvendelse i en forsvarsmæssig applikation, som har betydning for risiko og sikkerhedsforanstaltninger.

Sikkerhedsrammen danner grundlag for udarbejdelse af projektspecifikke sikkerhedsinstrukser for hhv. *sensitive* og *klassificerede* projekter. Disse indeholder lokale regler for sikkerhedsmiljøet på de enkelte videninstitutioner og skal sikre, at videninstitutionen lever op til eksterne og interne krav og anses for en professionel og attraktiv samarbejdspartner for myndigheder/virksomheder.

NFC's sikkerhedsramme udgør et særlig relevant hjælpeværktøj for NFC-partnere og forskere, der ikke tidligere har beskæftiget sig med dual use- og forsvarsforskning, da rammen tydeliggør, hvad der kræves for at kunne agere på de tre sikkerhedsniveauer. Forsvarsforskning kan indebære begrænsninger ift. traditionel "forskning og udvikling", men kan også give adgang til ny fundingområder, nye samarbejdspartnere samt muligheder for at arbejde med nye applikationer af forskning i komplekse scenarier. Institutionerne bør i den forbindelse være opmærksomme på, at en professionel håndtering af sikkerhed er en vigtig forudsætning for tillid og partnerskaber i sektoren.

Læsevejledning for sikkerhedsrammen:

- I afsnit 2 uddybes NFC's tre sikkerhedsniveauer og bagvedliggende regelsæt samt overordnede spørgsmål for indplacering af projekter på et givent sikkerhedsniveau
- I afsnit 3 gives en kort introduktion til de syv temaer for sikkerhedsforanstaltninger, ligesom koblingen mellem projektets risikovurdering og sikkerhedsforanstaltninger beskrives
- I afsnit 4, 5 og 6 gennemgås *åbent*, *sensitivt* og (militær) *klassificeret* sikkerhedsniveau.

[1] NFC's partnere udgøres af universiteter og Godkendte Teknologiske Serviceinstitutter (GTS'er) - tilsammen videninstitution(erne).

[2] Med NFC-regi forstås aktiviteter og projekter, som NFC enten finansierer eller indgår som partner i.

Nationalt Forsvars-teknologisk Center

Sikkerhedsrammen er opbygget akkumulativt. Det betyder, at de enkelte sikkerhedsniveauer bygger gradvis ovenpå hinanden. Krav til sikkerhedsorganisationen, kompleksitet og omkostninger stiger således i takt med de tre sikkerhedsniveauer.

2. SIKKERHEDSNIVEAUER OG RISIKOVURDERING

Sikkerhedsrammen består af tre sikkerhedsniveauer, *jf. figur 1*.

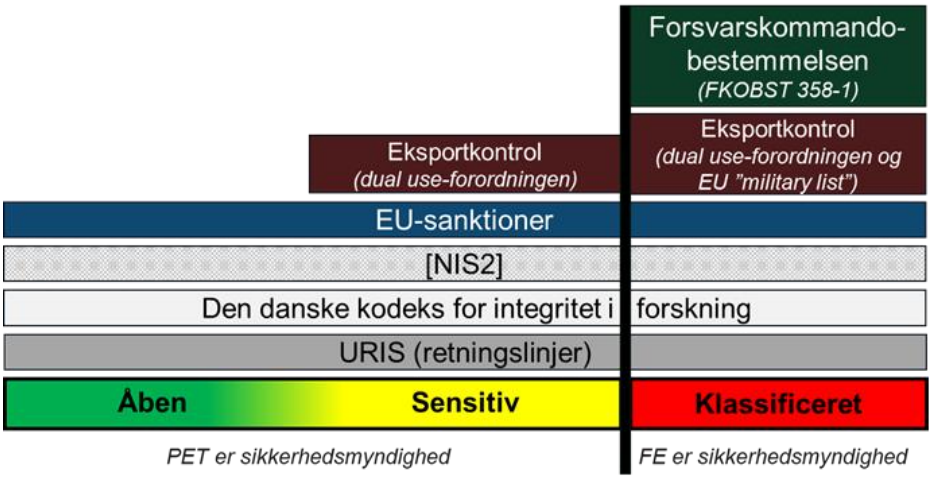
Figur 1: NFC's tre sikkerhedsniveauer

Åbent *(del 1)*	Udover URIS-retningslinjerne gælder ingen særlige sikkerhedsforanstaltninger eller eksportbegrænsninger for projektet. Sikkerhedsforanstaltninger skal altid vurderes fra gang til gang på baggrund af en konkret risikovurdering.
Sensitivt *(del 2)*	Der indgår fortrolige og/eller følsomme informationer i projektet, der kan udgøre en national sikkerhedsrisiko, hvis disse falder i de forkerte hænder. Projektets baggrundsviden og resultater kan være omfattet af eksportkontrol. Sikkerhedsrammen definerer en række minimumssikkerhedsforanstaltninger og standarder, som gælder på tværs af *alle* sensitive projekter. Den konkrete risikovurdering kan imidlertid altid udløse yderligere krav til sikkerhedsforanstaltninger, som ligger udover de fælles minimumssikkerhedsforanstaltninger.
Klassificeret *(del 3)*	Der indgår militær klassificerede informationer i projektet - ofte i form af data eller viden, der leveres af forsvarsmyndighederne. Derudover kan projektets baggrundsviden og resultater være omfattet af eksportkontrol. Forsvarets krav til sikkerhed reguleres i Forsvarskommandobestemmelse 358-1

Så længe videninstitutionen udelukkende bevæger sig i *åbent* og *sensitivt* sikkerhedsniveau, skal videninstitutionen kun forholde sig til del 1 og del 2 i sikkerhedsrammen. Del 3 i sikkerhedsrammen om militær klassificerede projekter indeholder en opsummering af initiale forudsætninger og centrale sikkerhedsforanstaltninger for at kunne operere på klassificeret niveau. Bilag 1 indeholder en uddybende beskrivelse af Forsvarskommandobestemmelsen ift. vidensinstitutioner *(NFC afventer en ny version af denne, før bilag 1 inkluderes i NFC's sikkerhedsramme)*.

De mest centrale regelgrundlag for de tre sikkerhedsniveauer er vist i figur 2:

Figur 2: Kobling mellem regelsæt og sikkerhedsniveauer



Det er altid den enkelte vidensinstitutionens ansvar at overholde love, regler, bekendtgørelser, aftalemæssige betingelser mv., som institutionen er underlagt.

Nationalt Forsvars-teknologisk Center

Som figur 2 viser, danner hhv. *URIS, Den danske kodeks for integritet i forskning, [NIS2]*[3] og *EU-sanktioner* et fælles fundament, som NFC-partnere - uagtet sikkerhedsniveau, skal kunne håndtere. Disse generelle regelsæt er uddybet i afsnit 4 under *åbent* sikkerhedsniveau.

Projekter i det *sensitive* sikkerhedsniveau er omfattet af enten eksportkontrol eller indeholder informationer, der kan udgøre en national sikkerhedsrisiko, hvis disse falder i de forkerte hænder. *Klassificerede* projekter er omfattet af Forsvarskommandobestemmelsen og kan indeholde elementer fra EU's "millitary list" i relation til eksportkontrol.

Overgangen mellem *sensitive* og *klassificerede* projekter er relativ klar, mens overgangen mellem *åbne* og *sensitive* projekter er mere flydende.

Det er altid en konkret risikovurdering af det enkelte projekt, som danner grundlag for indplacering ift. sikkerhedsniveau og de påkrævede sikkerhedsforanstaltninger, *jf. figur 3.*

Figur 3: Overordnet model for risikovurdering op indplacering af sikkerhedsniveau

Som figur 3 viser, skal der foretages løbende risikovurderinger i hele projektets levetid. Denne risikovurdering skal bl.a. ske ved væsentlige ændringer i projektet og i forbindelse med de halvårlige faglige rapporteringer på projektniveau i dialogen mellem den projektansvarlige og NFC.

Indplacering af sikkerhedsniveau kan (udover den konkrete risikovurdering) bl.a. foretages med udgangspunkt i en række overordnede spørgsmål til projektet, *jf. figur 4:*

Figur 4: Overordnede spørgsmål ifm. projektets indplacering på sikkerhedsniveau

I bilag 2 er der udarbejdet en vejledende spørgeguide, som NFC's partnere kan anvende i forbindelse med risikovurderingen af NFC-projekter og indplacering på sikkerhedsniveau.

[3] Det er under afklaring, hvorvidt og hvordan NIS2 skal implementeres hos NFC's partnere

Nationalt Forsvars-teknologisk Center

Det bør som udgangspunkt være et mål at designe projekter på et så lavt sikkerhedsniveau som muligt, hvis en tilsvarende værdi kan skabes, som hvis projektet havde haft et højere sikkerhedsniveau. Dette skyldes, at omkostninger, risiko og kompleksitet i håndtering af projektet typisk stiger i takt med øget sikkerhedsniveau. Projektdesign og databehov er derfor vigtige elementer, hvis et lavere sikkerhedsniveau ønskes.

3. SIKKERHEDSFORANSTALTNINGER

Der er defineret syv temaer for sikkerhedsforanstaltninger i NFC-projekter, *jf. figur 5:*

Figur 5: Temaer for sikkerhedsforanstaltninger

- Publicering: Omhandler evt. begrænsninger til publicering af resultater fra projektet.
- Kommunikation: Omhandler mulighederne for at kommunikere og formidle information om projekter mundtligt og skriftligt.
- Informationssikkerhed: Omhandler krav til it-løsninger fx ift. opbevaring og deling af data samt skriftlig og virtuel kommunikation inden for projektet.
- Fysisk sikkerhed: Omhandler fx krav til lokaler samt opbevaring af fysiske dokumenter.
- Personsikkerhed: Omhandler dels eventuelle statsborgerskabsbegrænsninger ift. bemanding af projektet og dels beskyttelse af forskeres personlige sikkerhed.
- Organisering: Omhandler krav til vidensinstitutionernes sikkerhedsorganisation.
- Samarbejdspartnere: Omhandler eventuelle landebegrænsninger på samarbejdspartnerniveau.

For *alle* projekter afgøres sikkerhedsforanstaltninger på baggrund af en risikovurdering. Derudover er der for klassificerede projekter initialt også en række minimumskrav for at opnå virksomheds- og evt. facilitetsgodkendelse fra FE. Disse er uddybet senere i del 3.

For *sensitive* projekter er der på udvalgte områder defineret en række fælles minimumssikkerhedsforanstaltninger, som er påkrævet på tværs af alle sensitive projekter. Den konkrete risikovurdering, som er obligatorisk for alle projekter, kan imidlertid altid ”overrule” minimumskravene, hvis den konkrete risikovurdering foreskriver mere restriktive sikkerhedsforanstaltninger.

Formålet med at definere en fælles ramme med minimumssikkerhedsforanstaltninger for det sensitive sikkerhedsniveau er at højne det generelle sikkerhedsniveau for kritisk forskning *(jf. URIS-retningslinjerne)* samt skabe en mere enkel sikkerhedsmodel, der lettere kan kommunikeres internt såvel som eksternt. Minimumssikkerhedsforanstaltninger kan bl.a. tage form af standarder, fælles it-løsninger samt retningslinjer og vejledninger.

Som tidligere nævnt overgår mange projekter fra et sikkerhedsniveau til et højere. Ved at definere minimumsforanstaltninger med inspiration fra bl.a. den militærklassificerede forskning og kravene fra den Europæiske Forsvarsfond (EDF), er det muligt at lette overgangen til klassificeret forskning eller EDF-projekter, da rammen for sensitive projekter indeholder ”light”-elementer herfra.

Det er et helt centralt hensyn, at den fælles ramme med minimumssikkerhedsforanstaltninger for de sensitive projekter skal skabe merværdi for de deltagende vidensinstitutioner og ikke indebære væsentlige administrative byrder eller uforholdsmæssige investeringer på institutionsniveau.

Nationalt Forsvars-teknologisk Center

Den overordnede logik bag sikkerhedsforanstaltninger er overordnet forklaret i tabel 1 og uddybes yderligere i de respektive afsnit.

Tabel 1: Overordnet logik for sikkerhedsforanstaltninger på de tre sikkerhedsniveauer

Tema	**Åben** *Sikkerhedsforanstaltninger ud fra konkret risikovurdering*	**Sensitiv** *Fælles minimumssikkerheds-foranstaltninger på udvalgte områder*	**Klassificeret** *Sikkerhedsforanstaltninger på baggrund af risikovurdering og klassificeringsniveau jf. FKOBST 358-1*
Publicering	Ikke særlige sikkerhedsmæssige foranstaltninger *(Følger risikovurdering)*	Begrænsninger forventes *(Følger risikovurdering)*	Yderligere begrænsninger forventes *(Følger risikovurdering)*
Kommunikation	Ikke særlige sikkerhedsmæssige foranstaltninger *(Følger risikovurdering)*	Sektor- og netværksbaseret kommunikation *(Fælles retningslinjer for forskellige målgrupper)*	Klassificeret materiale kan ikke deles. Øvrigt materiale kan kommunikeres sektor- og netværksbaseret *(Følger risikovurdering)*
Informations-sikkerhed	Institutionens dataklassificeringsmodeller *(Følger risikovurdering)*	Løsninger til at *opbevare*, *dele* og *kommunikere* oplysninger *(Fælles minimumsstandarder og fælles it-systemløsninger)*	Høje informationssikkerheds-mæssige foranstaltninger *(Følger risikovurdering)*
Fysisk sikkerhed	Ikke særlige sikkerhedsmæssige foranstaltninger *(Følger risikovurdering)*	Øgede sikkerhedsforanstaltninger for fysisk sikkerhed *(Fælles retningslinjer ift. fysisk sikkerhed)*	Høje sikkerhedsmæssige foranstaltninger *(Følger risikovurdering)*
Person-sikkerhed	Statsborgerskabssbegrænsninger på individniveau overvejes *(Følger risikovurdering)*	Statsborgerskabsbegrænsninger på individniveau og øget personsikkerhed *(Fælles minimumssikkerhedsforanstaltninger)*	FE-Sikkerhedsgodkendelse påkrævet og øget personsikkerhed *(Følger risikovurdering)*
Organisering	Sikkerhedsorganisation til risikostyring og vurdering af eksportkontrol og sanktioner *(Fælles minimumskrav til sikkerhedsorganisation)*	Sikkerhedsorganisation skal kunne håndtere eksportkontrol og sanktioner. *(Fælles minimumskrav til sikkerhedsorganisation)*	Høje krav til sikkerhedsorganisation. *(Følger risikovurdering)*
Samarbejds-partnere	Samarbejdslande og samarbejdsorganisationer overvejes *(Følger risikovurdering)*	Landebegrænsninger ift. samarbejdsorganisationer *(Fælles minimumskrav til samarbejdspartnere)*	Begrænsninger afgøres af FE *(Følger risikovurdering)*

Den svagt gule markering i det sensitive sikkerhedsniveau illustrerer, at NFC definerer fælles minimumsstandarder, retningslinjer eller løsninger på tværs af alle *sensitive* projekter. Der er fastlagt minimumssikkerhedsstandarder på overordnet niveau for næsten alle områderne. Dette gælder imidlertid ikke på informationssikkerhedsområdet, hvor fastlæggelsen af fælles it-løsninger forudsætter en større analyseproces med involvering af NFC's partnere med henblik på at afdække behov og muligheder.

Derudover er det i relation til det åbne sikkerhedsniveau et krav, at der skal være en minimumssikkerhedsorganisation, der kan foretage risikostyring og vurdering af eksportkontrol og sanktioner. Denne minimumsstandard er markeret med lysegrøn i tabel 1. Dette krav til sikkerhedsorganisation skal desuden ses som en direkte udløber af URIS-anbefalingerne.