Demonstration af anvendelighed og værdiskabelse

A. INDLEDENDE OPLYSNINGER	
Aktivitetsområde	Indsatsområdet Digital Sikkerhed, Tillid og Dataetik
Institut	Alexandra Instituttet
Titel *Dækker indholdet af aktiviteterne*	Demonstration af anvendelighed og værdiskabelse
Nummerering *Af beskrivelsen*	5
Version	1
Periode *Forventet start og slut*	01.01.2023 – 31.12.2023
Kontaktperson	Kristian Krämer

B. ÆNDRINGER
Angiv her, hvis en planlagt aktivitet er ændret i forhold til den forudgående version af beskrivelsen.

C. BESKRIVELSE	
1. Mål *Hvorfor?* Hvad er målet for aktiviteterne? Hvordan bidrager de til det overordnede mål for aktivitetsområdet?	Aktiviteterne i denne aktivitetsbeskrivelse bidrager til det overordnede mål for indsatsen ved at sikre at danske virksomheder, via inddragelse i både casesamarbejder og videnspredningsaktiviteter samt videreudviklingen af en test-, demonstrations- og udviklingsfacilitet (TDU), kan holde sig i front i den globale konkurrence ved at opnå dyb viden om og kompetencer inden for bl.a. cybersikkerhed, kritiske systemer, standarder, sensitive data og AI & data governance m.m. Målet med aktiviteterne i indeværende aktivitetsperiode vil dels være en videreudvikling af TDU'en og systematisk opsamling og formidling af de teknologiske services og ydelser, som udvikles på tværs af de øvrige aktivitetsplaner under indsatsområdet, samt at involvere mere end 100 virksomheder i konkrete videnspredningsaktiviteter.
2. Indhold *Hvad* skal der ske? Hvilke(n) konkret(e) aktiviteter udføres?	Vi videreudvikler den digitale test-, demonstrations- og udviklingsfacilitet (TDU), som skal være med til sikre, at danske virksomheder kan skabe forretning og spille ind i danske og europæiske initiativer for sikker og ansvarlig brug af digitale teknologier. TDU'en vil indeholde en samling af teknologiske services, således at de virksomheder, der har behov for rådgivning og hjælp til ideer eller tekniske udfordringer inden for cybersikkerhed, kritiske systemer, standarder, sensitive data og AI & data governance, kan henvende sig og få hjælp til at komme videre. I den indeværende periode vil der blive lanceret teknologiske services inden for følgende TDU'er: • **Dansk data science og integrering af DaNLP** Lancering af TDU for dansk data science - *AIAI (Alexandra Instituttet Artificial Intelligence)*, med fokus på dansk tekst- og taledata. TDU'en er målrettet machine learning udviklere i danske virksomheder, som enten allerede

	arbejder med dansk data science eller gerne vil i gang. • **Cybersikkerhed, sensitiv data og kritisk infrastruktur** Lancering af TDU for cybersikkerhed, sensitiv data og kritisk infrastruktur, der forventes at tilbyde følgende teknologiske services: o Sikkerhedsreview o Rådgivning om udviklingen af EU's Cyber Ressilience Act o Rådgivning om certificering af produkter efter ETSI EN 303 645. o Rådgivning om EU's Radio Equipment Directive (RED), der træder i kraft i 2024 I samarbejde med Alexandras øvrige RK-indsatser arbejdes med modning af hvordan vi konkret mapper TDU-begrebet og de tilhørende services ind i Alexandras værditilbud og kanaler, således at vi kan nå ud til flest muligt i målgruppen. Dette involverer samtidig koordinering med øvrig GTS i forhold til den fælles kanal: https://teknologiskinfrastruktur.dk **Videnspredning:** Formidlingen af viden og resultater vil være en central del af hele aktivitetens formål, og vi vil sikre at tilrettelæggelsen af de enkelte del-aktiviteter i perioden medvirker til at viden og resultater når ud til minimum 90 virksomheder jf. indikatormål og sikre en modning af virksomhedernes tilgang til/arbejde med digital sikkerhed, tillid og dataetik. Videnspredningsaktiviteterne vil bestå af klassiske formidlingsarrangementer, som inspirerer og styrker teknologiforståelsen, såsom workshops og webinarer, hvor vi, sammen med de danske klynger og andre relevante aktører, bringer vores metoder og redskaber i spil og giver virksomhederne vejledning i, hvordan de anvender resultaterne i praksis. Nogle af videnspredningsaktiviteterne vil desuden være en del af konferencer andre organisationer afholder for at nå ud til et bredere publikum. **Governance og risikostyring**: Endelig vil aktiviteten have fokus på den løbende inddragelse af følgegrupper og andre relevante aktører (herunder 1-2 årlige dialogmøder med DI og DE) samt en proaktiv risikostyring og løbende opdatering af risikoanalysen mhp. at undgå aktiviteter af konkurrenceforvridende karakter. Indsatsen bliver ledet af en dedikeret programleder, der vil have det overordnede ansvar for fremdrift, risikostyring, målopfyldelse og økonomi på tværs af alle aktivitetsplanerne. Den overordnede programleder er derudover ansvarlig for udviklingen af indsigter, teknologier, ydelser og services der bliver tilgængeligt gennem TDUen. Denne udvikling sker gennem Alexandra Instituttets udviklingsmodel, hvor hver udviklingsiteration – ud over den teknologiske vinkel – skal indeholde et bruger-/kundeperspektiv samt en forretningsmæssig vinkel, så vi sikrer en iterativ bruger- og forretningsdrevet udvikling af de teknologiske services.
3. Aktører *Hvem* udfører aktiviteterne? Hvilken afdeling af instituttet? Evt. hvilke eksterne parter er med (videninstitutioner, virksomheder, erhvervsorganisationer, myndigheder, klyngeorganisationer eller andre).	De tværgående aktiviteter vil primært blive udført af et team med kompetencer inden for forretningsudvikling og kommunikation, og ikke mindst med teknisk fundering og fokus på brugerinddragelse. Følgende afdelinger deltager fra Alexandra: Insights Lab, Security Lab, AI and Data Analytics Lab samt det tværgående team Strategic Business & Governance. Fra FORCE Technology deltager afdelingen for Technology Product Compliance. Vi vil desuden samarbejde med brancheorganisationer (herunder DI og DE) ift. afholdelse af fælles konferencer, webinarer og netværksarrangementer. Herudover vil Danish Hub for Cybersecurity/DigitalLead, Erhvervshus Midtjylland + Hovedstaden, CenSec og MADE indgå som partnere ift. både videnspredningsaktiviteter samt virksomhedsrekruttering til case-projekter, assistance med afklaring af konkurrenceforhold, behovsafdækning og domæneviden.

4. Sammenhæng med andre projekter (evt.) Indgår aktiviteten i andre eksternt finansierede projekter?	Aktiviteten vil sikre sammenhæng til følgende igangværende projekter: • CyPro: CyberSikker Produktion i Danmark. Projektets formål er at styrke cybersikkerheden indenfor IoT i Danske produktionsvirksomheder – både producenter og aftagere af IoT. • Sb3D: Security by Design in Digital Denmark (Industriens Fond). Projektets formål er at øge brugen af Security by Design i digitale produkter og løsninger. • SIOT: Secure Internet of Things – Risk analysis in design and operation (Innovationsfonden DIREC) projektets formål er værktøjer til risikoanalyser indenfor cybersikkerhed. • Crucial: Projektets formål bl.a. opdagelse af kompromitterede systemer indenfor kritisk infrastruktur, primært vand og el. • Danish Conversational and Read-aloud Speech Dataset (CoRal), Ansøgt Grand Solution projekt om danske tale datasæt. • AI-Matters, Digital Europe, TEF, hvor formålet er at udvikle en europæisk testplatform, hvor fremstillingsvirksomheder kan teste sine AI teknologier. • European Digital Innovation Hubs (EU): Central Denmark European • Følgende er under ansøgning og forventes at kunne opstartes fra og med Q3 2023: Digital Innovation Hub, Greater Copenhagen European Digital Innovation Hub, og Smart Energy Digital Innovation Hub.
5. Følgegruppe Har følgegruppen forholdt sig til aktiviteten? I så fald hvordan? Hvis ikke, hvornår forventes følgegruppen at blive præsenteret for aktiviteten? (Det sidste bør kun gælde under opstarten af indsatsområdet).	I udarbejdelsen af denne aktivitetsbeskrivelse har vi været i dialog med både virksomheder, rådgivere, offentlige organisationer og universiteter gennem indsatsens netværks- og følgegrupper. Vi har fået input til konkrete aktiviteter og bredt identificeret markedsmæssige udfordringer og problemområder, som i dag ikke bliver dækket af teknologiske services. I 2022 har vi etableret følgegrupper for sporene: Standardisering og kritiske systemer: Dansk Standard, EnergiNet, Hounö, Erhvervsstyrelsen, Censec, EnergiCert Følsomme data (fra 2023: Ai & Data Governance): Aalborg Universitet, Data For Good Foundation, Focus Advokater, Secata, BlockDeamon I forhold til sporet om Tillidsskabende AI, (fra 2023 Dansk AI) har vi haft løbende møder med væsentlige aktører indenfor det sprogteknologiske område i Danmark: Omilon, Corti, Dictus, Alvenir, KMD, ATP, Dansk Sprognævn, Digitaliseringsstyrelsen, m.fl. Derudover er der dialog med DI og DE med henblik på at få et bredere perspektiv på markedssituationen inden for cybersikkerhed, ansvarlig AI og digitaliseringen helt generelt. I den kommende periode afholdes der 2-3 følgegruppemøder, samt 1-2 dialogmøder med henholdsvis DI og DE.
6. Formidling af resultater (evt). Hvordan/hvor kan interesserede virksomheder og andre få viden om resultaterne af aktiviteterne? (Anføres/tilføjes hvis det ikke allerede fremgår af beskrivelsen ovenfor, f.eks. ved links til konferencer, hjemmeside, publikationer etc.).	Vi formidler løbende aktivitetens resultater gennem artikler i fagmedier, blogs, konferencer (nationale og internationale), whitepapers og hands-on guides, der helt overordnet vil have til formål at klæde virksomheder på til at udvikle og implementere ansvarlige løsninger. Vi vil desuden udarbejde case-beskrivelser, der formidler erfaringer og opmærksomhedspunkter fra virksomheder. Ligeledes består formidlingen i at poste indsigter og resultater via vores sociale medier, hvor vi linker til faglige indlæg

	på f.eks. blogs og artikler på egne kanaler samt de andre aktørers medieplatforme (eksempelvis Nordic IoT Center; DigitalLead, DI, FORCE Technology m.fl.)