Standarder og kritiske systemer

A. INDLEDENDE OPLYSNINGER	
Aktivitetsområde	Indsatsområdet Digital sikkerhed, tillid og dataetik
Institut	Alexandra Instituttet (Lead) og FORCE Technology
Titel *Dækker indholdet af aktiviteterne*	Standarder og kritiske systemer
Nummerering *Af beskrivelsen*	2
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?	Denne aktivitet vil fortsætte Alexandra Instituttets og FORCE Technology's involvering i certificering, og standardisering af, nye avancerede digitale teknologier for øget cybersikkerhed. Når virksomheder begynder at arbejde mere seriøst med sikkerhed, bliver forskellige standarder ofte involveret. Dette gøres for både at sikre at det implementerede sikkerhedsniveau ligger på niveau med best practice og for at kunne dokumentere sikkerhedsniveauet for eksterne interessenter. EU har de senere år haft et øget fokus på cybersikkerhed, set eksempelvis i NIS og NIS2 direktiverne, men også produktsikkerhed er et fokusområde hvilket ses i opdateringen af Radioudstyrs direktivet (RED) og det kommende Cyber Resilience Act (CRA). Disse to nye lovstykker vil tilsammen omfatte alle produkter med digitale komponenter der sælges på det indre marked og stiller en række krav mht. cybersikkerhed. Disse krav konkretiseres gennem en række standarder, der i de kommende år skal implementeres af alle, som sælger digitale produkter på det indre marked. Konkret vil aktivitetsområdet have et primært fokus på hvordan virksomheder kan anvende standarder i praksis, hvorved de kan dokumentere deres implementerede sikkerhed. Dette vil opnås gennem virksomhedscases, hvor virksomheder bl.a. hjælpes med at udvikle den nødvendige dokumentation således forskellige, almene sikkerhedsfunktioner kan valideres ud fra en dertil udviklet testplan. De resulterende værktøjer, processer og erfaringer vil være grundlaget for aktivitetens videnspredning.
2. Indhold *Hvad* skal der ske? Hvilke(n) konkret(e) aktiviteter udføres?	Fortsat standardiseringsarbejde – Arbejde i standardiseringsudvalg i Dansk Standard, i EU-regi (f.eks. CEN/CELEC) og internationalt (f.eks. ISO), gennem S-441 udvalget, både som bidrag til og overvågning af relevant standarder. Vi vil også deltage som eksperter, på vegne af DI, i Orgalims taskforce, der giver EU kommisionen input i forbindelse med udarbejdelsen af Cyber Resilience Act.

	For at hjælpe virksomheder med at komme i gang med arbejdet omkring validering af deres sikkerhedsfunktioner vil der blive udviklet en række eksempler på fremgangsmåder og dokumentationsformer for hvordan dette kan opnås. Her er der fokus på hvordan men kommer fra kravspecifikation til en testet, valideret og dokumenteret funktion. Som nævnt tidligere, vil en række EU love stille krav til virksomhedernes cybersikkerhed i den kommende tid, men samtidigt har virksomhederne relativt kort tid til at implementerede de nødvendige tiltag. Eksempelvis har RED effekt fra August 2024, men de beskrivende standarder der skal implementeres, bliver først færdigarbejdet i løbet af 2023. Vi vil i den forbindelse udgive et overblik over, og vejledning til hvordan, virksomheder bliver berørt af lovene og hvordan virksomhederne allerede nu kan begynde på arbejdet omkring compliance. Indgåelse af nyt samarbejde med en eller flere aktører indenfor kritisk infrastruktur, eksempelvis sundhedsdatastyrelsens DCIS, andre DCIS'er, kommercielle virksomheder eller interesseorganisationer. Formålet med disse samarbejder er at identificere konkrete udfordringer for virksomhederne indenfor kritisk infrastruktur. Samarbejdet forventes at have et overlap med sporet "AI og data governance", idet opsamling af data til beskyttelse af (kritiske) systemer i sig selv kan indebære en risiko, der kan mitigeres ved brug af teknikker beskrevet i "AI og Data governance" sporet. Arbejdet indenfor kritisk infrastruktur ligger derudover i forlængelse i de eksisterende projekter Crucial og CyPro, der fokuserer på hhv. overvågning af kritisk infrastruktur og cybersikkerhed i produktionsvirksomheder. Færdiggøre arbejdet omkring en DANAK-akkreditering af processerne ved en ETSI EN 303 645 evaluering efter ETSI EN 103 701. Akkrediteringen gør det muligt at lave en service, hvor virksomhederne kan få lavet en testrapport, der kan danne grundlag for en certificering af produkter efter ETSI EN 303 645. Vi vil så vidt muligt aligne diverse guides med D-mærket og sikkerdigital.dk, således processer og dokumentation kan kan genbruges hvor muligt.
3. Aktører *Hvem* udfører aktiviteterne? Hvilken afdeling af instituttet? Evt. hvilke eksterne parter er med (videninstitutioner, virksomheder, erhvervsorganisationer, myndigheder, klyngeorganisationer eller andre).	Direkte involverede GTS Institutter: • Alexandra Instituttet A/S: Security Lab, Insights Lab, Artificial Intelligence and Data Analysis Lab samt Strategic Business & Governance dept. • FORCE Technology Product Compliance. • Samarbejde gennem Nordic IoT Center. Eksterne samarbejdspartnere: • Dansk Standard • Klyngerne MADE, CenSec og DigitalLead • D-Mærket • Erhvervsstyrelsen /CFCS – i forbindelse med EU's cybersikkerhedsforordning. • Erhvervsorganisationerne DI og DE • Universiteter, vi allerede har samarbejder med: AAU, DTU, ITU og AU • Orgalim – Europe's Technology Industries
4. Sammenhæng med andre projekter (evt.) Indgår aktiviteten i andre eksternt finansierede projekter?	Denne aktivitet har sammenhæng med disse RK-indsatsområder: Digitale teknologier til datadrevet, bæredygtig vækst (Alexandra Instituttet) IoT-drevet forretningsdesign (FORCE Technology og Alexandra Instituttet. Eksternt finansierede 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 formal er værktøjer til risikoanalyser indenfor cybersikkerhed. • Crucial: Projektets formål bl.a. opdagelse af kompromitterede systemer indenfor kritisk infrastruktur, primært vand og el. • Nyt projekt - Der vil i dette projekt være afsat midler til en mulig ansøgning indenfor området.
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).	D. 7. november 2022 er der afholdt møde med følgegegruppen, hvor aktiviteten og delaktiviteterne blev præsenteret og diskuteret. Aktivitetsbeskrivelsen er efterfølgende blevet tilpasset på baggrund af følgegruppens kommentarer. Følgegruppen består i dette spor følgende organisationer: Dansk Standard, EnergiNet, Hounö, Erhvervsstyrelsen, Censec, EnergiCert.
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.).	Hovedparten af resultater og erfaringer i denne aktivitet vil blive formidlet gennem aktiviteten *Demonstration af anvendelighed og værdiskabelse* ift. indsatsområdet *Digital sikkerhed, tillid og dataetik,* i form af videnskabelige artikler, white papers, blog posts og oplæg på konferencer eller webinarer hvortil denne aktivitet leverer fagligt indhold. En del af formidlingen vil dog ske direkte gennem standardiseringsarbejdet. De udviklede ydelser vil også stilles til rådighed for markedet gennem den digitale TDU.