SDU IT

Referat

10. december 2025

truelsen@sdu.dk

Emne	Møde i Udvalget for Informationssikkerhed og Databeskyttelse
Dato og tidspunkt	10. december 2025 kl. 10-12
Sted	O TEK Johnson Meetingroom (Ø21-613a-2)
Inviterede	Bue Raun Andersen, Janni Lee B. Bang Brodersen, Mads Niemann-Christensen, Jan I. Kristensen, Peder Thusgaard Ruhoff, Martin Svensson, Rune Nørgaard Jørgensen, Morten Hulvej Rod, Simon Kamber
Mødeleder	Bue Raun Andersen

Dagsorden

1. Indledende punkter	1.1 **Godkendelse af dagsorden for mødet** 1.2 **Godkendelse af referat fra sidst** Referat af UID 28. 1.3 **Kort nyt** 1.4 **Hændelsesrapporter** Rapporterne ligger i mødemappen til orientering. På mødet vil der blive lavet enkelte nedslag i de mest relevante hændelsesrapporter, men de er primært til orientering og vil ikke blive systematisk gennemgået.
2. Godkendelser	2.1 **Risikovurdering 2025** Bilag: Indstilling Bilag: Risikovurderinger på SDU 2025 Punktet omhandler afrapportering af SDU's risikovurderinger i 2025. Udvalget bedes drøfte afrapporteringen og tage stilling til SDU's risikoappetit samt godkende sagen kan forelægges direktionen med henblik på endelig godkendelse.
3. Orienteringer	3.1 **Indberetning af NIS2 omfattede aktiviteter og tilsyn fra Digst.** Bilag: Indstilling. SDU skulle senest den 1. oktober 2025 indmelde aktiviteter, der er omfattet af NIS2-loven (lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau). Derudover er det en orientering om, at SDU har modtaget tilsyn fra Digitaliseringsstyrelsen vedrørende overholdelse af NIS2-loven.

Syddansk Universitet
Campusvej 55
5230 Odense M
T +45 6550 1000
www.sdu.dk

	3.2 **UFS-opfølgning på Rigsrevisionens beretning vedr. forskningssikkerhed** Bilag: Indstilling Bilag: Notat fra SDU IT Punktet omhandler Uddannelses- og Forskningsstyrelsens opfølgning på Rigsrevisionens beretning om forskningssikkerhed. Anmodningen sker på baggrund af at statsrevisorerne har bedt om en ministerredegørelse vedr. universiteternes beskyttelse af forskningsdata mod ukendt udstyr på netværket. 3.3 **Trusselsvurdering fra SAMSIK** Bilag: Indstilling. Sagen omhandler den nyeste trusselsvurdering fra Styrelsen for Samfundssikkerhed (SAMSIK) vedr. cybertruslen mod Danmark.
4. Evt.	

Referat

Indledende punkter

1.1 Dagsorden – tak for feedback – godkendt.

1.2 Referat godkendt.

1.3 Kort nyt:

Udvikling på URIS retningslinje
SAFE beretter om, at der udvikles på URIS retningslinjen. Styrelsen indikerer, at retningslinjen vil blive mere bindende end hidtil, hvor den har båret præg af soft law status. Der er løbende dialog mellem styrelsen og institutioner. Den hidtidige ordning kører et år mere.

Tunnelmail
Mange offentlige myndigheder og store virksomheder bruger tunnelmail til at sende sikker post med. UID har tidligere tilladt automatisk videresendelse af mail. Opgradering af sikkerheden i tunnelmail forhindrer dog nu videresendelse. Derfor vil der målrettes kommunikation til dem, som har brugt automatisk videresendelse til en anden mail. Der er ca. 1.200 konti ud af 60.000 konti, som har brugt videresendelse og disse er primært

medarbejdere med dobbeltansættelser, masterstuderende og eksterne lektorer. Der arbejdes på en løsning med notifikation om modtaget mail.

Møde med Region Syddanmarks IT-direktør
SDU IT har afholdt møde med IT-direktøren ved Region Syddanmark om samarbejde ved dobbeltansættelser særligt på OUH. Ikke mange nemme løsninger. Vi bedriver sikkerhed på forskellig vis.

1.4 Hændelsesrapporter:
Ved hændelser ses en tendens til, at opdateringer ved leverandører knækker integrationer. Systemerne er mere sårbare, når der laves lokale tilpasninger.
Erfaringen er, at SDU IT i nogle tilfælde har haft svært ved at få kontakt til leverandøren for at få kvalificeret hjælp til løsninger. Dette giver anledning til at undersøge bedre supportaftaler. SDU har mange kritiske ydelser i Microsofts univers. Der opfordres til at undersøge mulighed for koordinering mellem SDU og leverandør om valg af tidspunkt for opdateringer. .
Orientering om at hændelse af 5. oktober ikke nåede at medtages på dette møde.

Godkendelser.

2.1 Risikovurderingsrapport.

Risikovurderingsprocessen er fornyet og der er lavet kompetenceforløb.
Risikovurderingerne er et vigtigt redskab fordi de fleste eksterne standarder vi skal leve op til, er risikobaserede.
Næste år vil der blive lavet kurser for systemejere og GRC vil gå i samarbejde med fakulteterne om, hvad der giver mening for dem at risikovurdere.

Den store observation omkring forældet nødstrømsforsyninger m.v. i SDU's driftscenter allerede håndteret, idet indstillingen omkring bevilling til opdatering er godkendt.

Et emne har også været frigørelse af big-tech, som er et højaktuelt diskussionsemne på tværs af sektoren og i informationssikkerhedsbranchen. Løsningerne lider dog af meget symbolpolitik, og der er ikke meget glæde og tilfredshed i de eksperimenter der udføres. Det vil være naivt at forestille sig, at vi kommer ud af MS i de næste par år.

SDU IT laver en infrastrukturstrategi om, hvad der skal ligge i sky eller i kælder.

DPO'en udtaler, at SDU skal huske på, at der er flere nuancer end blot sort/hvid ift. brug af Microsoft. Det behøver ikke at være enten eller. Man kan fx bruge office-pakken

og samtidigt bruge en anden løsning end azure. Der blev udtrykt et ønske om at der kommunikeres ud, at strategien ikke er MS first.
DPO'en gør også opmærksom på, at der er en restore-test, står stadig er i rød efter accept af mitigerende tiltag, hvortil CIO understreger, at indstillingen til direktionen skal laves tydelig i forhold til, hvad der er den røde restrisiko.

Risikovurderingsrapporten blev godkendt. Rapporten bliver forelagt universitetsdirektøren, som sikrer passende behandling i rektoratet eller direktionen.

Orienteringer.

3.1 NIS2 og Digst.
SDU har indmeldt NIS2 omfattede aktiviteter og har allerede modtaget det første tilsyn fra Digitaliseringsstyrelsen. Undervisnings- og forskningsministeriet er fortsat uafklaret i forhold til, om de skal udstede en bekendtgørelse, som omfatter alle universiteter af NIS2. Det forlyder sig, at de nu har engageret faglig hjælp og bistand til at undersøge om sektoren skal omfattes.

3.2 Rigsrevisionens beretning om forskningssikkerhed, som UFS har fulgt op på.
Udskiftningen af de resterende dele af netværksudstyret involverer primært de tre parter, SDU IT, Teknisk service og fakulteterne. Udskiftning afhænger i høj grad om af, at den skal planlægges med laboratorierne for at undgå problemer ved forsøg. SDU forventer at være i mål i første del af 2027.

3.3 SAMSIK cybertrusselsvurdering
Et væsentligt fokuspunkt i SAMSIK's cybertrusselsvurdering omhandler OT. For at formindske, at OT kan blive en angrebsvinkel, opfordres der til at have større fokus på dette.

4. Eventuelt.
Der blev spurgt til arbejdet med IT-sikkerhedsstrategien. Der er blevet afholdt workshops og samtaler med forskere med særlige behov og administrative kollegaer.
Der blev identificeret nogle lavthængende frugter og nogle use-cases, som vil blive kategoriseret.
Der forventes en kortsigtet to-be-oversigt og en mere langsigtet plan.
Kommende: Workshop med ledergruppen for at blive enige om pejlemærker.
It-sikkerhedsstrategien forventes at være nået langt ved udgangen af januar.

Med venlig hilsen

Anna Randi á Valinum og Brian Truelsen
GRC-konsulenter