HELGELANDSSYKEHUSET
HELGELAANTEN SKÏEMTJEGÅETIE

Informasjonssikkerhet i forsknings- og kvalitetsprosjekter

Hvem jobber med informasjonssikkerhet?


90

Hver enkelt jobber med informasjonssikkerhet – *hver dag*!

Informasjonssikkerhet i Helgelandssykehuset

Øystein Sekse Øie
Informasjonssikkerhetsansvarlig
Mobil: 90824497

Svein Arne Soløy-Ervik
Rådgiver informasjonssikkerhet
Mobil: 99486564

Organisert under Drift og eiendom, avdeling IKT, eHelse og informasjonssikkerhet.

Felles kontaktinfo: Informasjonssikkerhet@Helgelandssykehuset.no

Informasjonssikkerhet i Helgelandssykehuset

Handlingsplan

Bygger på følgende: • Regional handlingsplan • Oppdragsdokument	**Omfatter følgende områder:** • Innkjøpspolicy • Dokumentasjon • Risikovurdering • Verdivurdering • Trusselvurdering • Sårbarheter • Sikkerhetskultur og opplæring • Revisjonsplan • Beredskap • Organisering • Prosjekt • Kompetanseheving
Referanser til: • Felles styringssystem for info.sikkerhet i HN • NSM Grunnprinsipper	

Informasjonssikkerhet er ikke det viktigste!

Informasjonssikkerhet vs. brukervennlighet

Information security is a cost of doing business…

Dette gjelder også for forskning!

Etiske prinsipper

Forskning skal styres av etiske prinsipper som:

Respekt: Personer som deltar i forskning, som informanter eller på annen måte, skal behandles med respekt.

Gode konsekvenser: Som forsker skal man etterstrebe at ens aktivitet har gode konsekvenser, og at mulige uheldige konsekvenser er akseptable.

Rettferdighet: Ethvert forskningsprosjekt skal være rettferdig utformet og utført.

Integritet: Forskeren plikter å følge anerkjente normer og å opptre ansvarlig, åpent og ærlig overfor kolleger og offentlighet.

Kilde: helgelandssykehuset.no

Samtykke

Helseforskningsloven, § 13:

«Det kreves samtykke fra deltakere i medisinsk og helsefaglig forskning, med mindre annet følger av lov.

Med samtykke menes enhver frivillig, spesifikk, informert og utvetydig viljesytring fra deltakeren der vedkommende ved en erklæring eller tydelig bekreftelse gir sitt samtykke til behandling av helseopplysninger eller humant biologisk materiale.»

Samtykke - CNN

Our use of cookies and other technologies

We, our **Affiliates** and **Vendors** use cookies and other technologies to process personal data (including device identifiers and IP addresses) for the following purposes: Store and/or access information on a device, Select personalised ads, Create a personalised ads profile, Create a personalised content profile, Select personalised content, Measure content performance, Apply market research to generate audience insights, Develop and improve products, Select basic ads and Measure ad performance. **Privacy Policy**

By clicking "Accept All" you agree to these purposes. For more information, to provide or withdraw consents, and in some cases object to legitimate interest purposes for processing your personal data, click "Manage Cookies+". Additionally, you may exercise your preferences for consent or object to legitimate interest processing at a vendor level in the "Vendors" link. These settings are accessible on a site or app specific basis, at any time through the 'Manage Cookies+' link located on webpages or in application settings. We work in coordination with an industry framework which will signal your preferences to our participating**Vendors**

Accept All

Manage Cookies+

Samtykke - Snapchat

3. Rettigheter du gir oss

Mange av våre Tjenester lar deg skape, laste opp, publisere, sende, motta og lagre innhold. Når du gjør det, beholder du all eierskapsrettigheter i det innholdet som du hadde i utgangspunktet. Men du gir oss tillatelse til å bruke innholdet. Omfanget av lisensen avhenger av hvilke tjenester du bruker og innstillingene du har valgt.

For alt innhold du sender inn til Tjenestene, gir du Snap og våre tilknyttede selskaper en verdensomspennende, royalty-fri, underlisensierbar, og overførbar lisens til å drifte, lagre, bruke, vise, reprodusere, modifisere, tilpasse, redigere, publisere, analysere, overføre og distribuere dette innholdet. Denne lisensen har det formål å drive, utvikle, levere, markedsføre og forbedre Tjenestene, samt utforske og utvikle nye. Denne lisensen inkluderer vår rettighet til å gjøre ditt innhold tilgjengelig for, og gi disse rettighetene videre til, tjenesteleverandører som vi har avtalefestede forhold med relatert til levering av Tjenestene, utelukkende for formålet å levere disse Tjenestene.

Vi kaller innleveringer til Story som er innstilt for å kunne bli sett av alle, og innhold du sender inn til offentlige tjenester, som for eksempel Offentlige profiler, Snap-kart eller Lens Studio, for "Offentlig Innhold". Fordi Offentlig innhold er offentlig av natur, gir du Snap, våre tilknyttede selskaper, andre brukere av Tjenestene, og våre forretningspartnere de samme rettighetene du gir for ikke-Offentlig innhold i forrige avsnitt, samt en ubegrenset, verdensomspennende, royalty-fri, ugjenkallelig, og evigvarende rett og lisens til å skape avledede verk fra, promotere, utstille, kringkaste, syndikere, reprodusere, distribuere, synkronisere, legge til grafikk og lydeffekter, offentlig fremføre, og offentlig vise frem alle eller enhver del av ditt Offentlige innhold (inkludert den separate videoen, bilde, lydinnspillingen, eller musikalske komposisjoner som finnes i det) i enhver form, og i alle medier eller distribusjonsmetoder, nå kjent eller senere utviklet. Når du fremstår i, skaper, laster opp, legger ut eller sender Offentlig innhold (inkludert din Bitmoji), gir du også Snap, våre tilknyttede selskaper, andre brukere av Tjenestene og våre forretningspartnere en ubegrenset, verdensomspennende, royalty-fri, ugjenkallelig og evigvarende rett og lisens til å bruke navnet, skikkelsen og stemmen til alle som er i ditt Offentlige innhold i kommersielle eller ikke-kommersielle formål. Dette betyr blant annet at du ikke har krav på kompensasjon hvis ditt innhold, videoer, bilder, lydopptak, musikalske komposisjoner, navn, likhet eller stemme brukes av oss, våre tilknyttede selskaper, brukere av Tjenestene, eller våre forretningspartnere. For mer informasjon om hvordan du tilpasser hvem som kan se på innholdet ditt, vennligst ta en titt på våre Personvernbetingelser og Supportnettsted. Offentlig innhold må være egnet for personer i alderen 13 år og eldre.

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «En studie av arbeidsoppgaver for en informasjonssikkerhetsansvarlig i spesialisthelsetjenesten i Norge», og har fått anledning til å stille spørsmål. Jeg samtykker til:

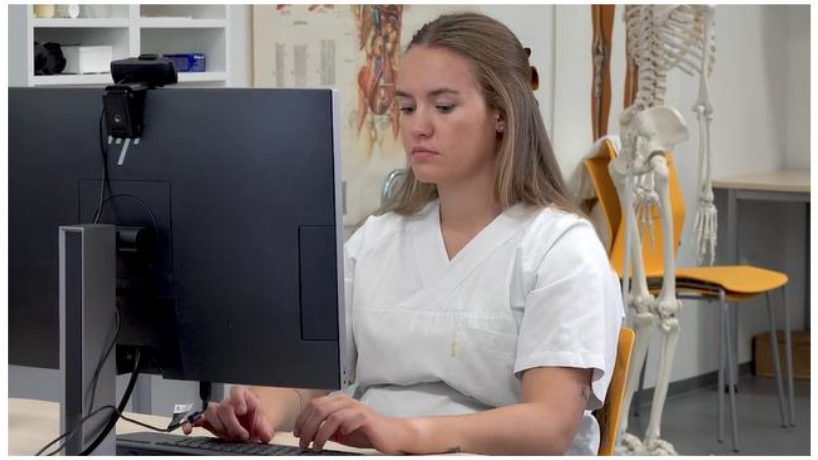
- ☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Informasjonssikkerhet er en viktig del av forskningsprosjekter!



Hva er datasikkerhet? Det handler om pasientens liv og helse!

Bruk 15 minutter i en ledig stund, link via:
https://intranett.helsenord.no/beredskap-felles/informasjonssikkerhet-felles/

Pasientsikkerhet

«Det har kanskje vært en tradisjon for å tenke at datasikkerhet, det er nok ikke kobla opp mot at det har med liv og helse å gjøre – for det er jo det vi har erfart nå. Det går jo direkte inn på liv og helse.»

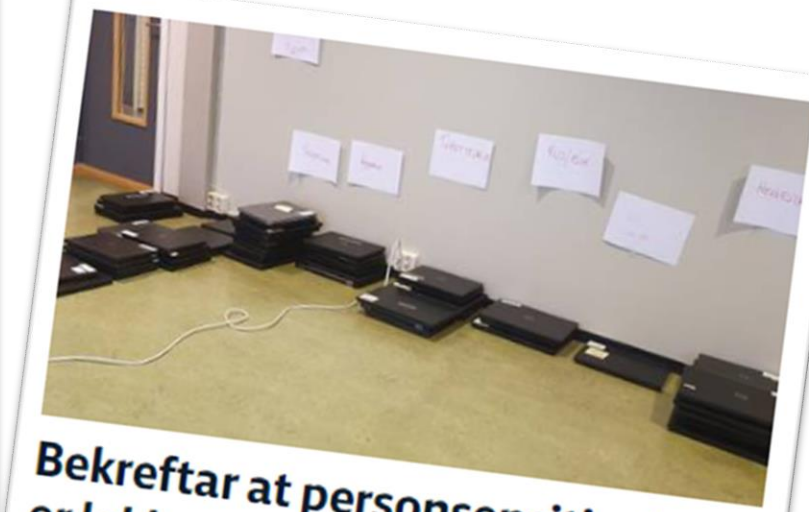
Pasientsikkerhet

«Det har kanskje vært en tradisjon for å tenke at datasikkerhet, det er nok ikke kobla opp mot at det har med liv og helse å gjøre – for det er jo det vi har erfart nå. Det går jo direkte inn på liv og helse.»

- Øyvind Sandvoll, enhetsleder Labo sykehjem, Østre Toten kommune.

GJENOPPRETTING: Alle desse datamaskinene måtte gjenopprettast etter angrepet. Kommunen var framleis utan alle system på plass ein månad etterpå.

FOTO: ANDERS BAKKERUD LARSEN / NRK



Bekreftar at personsensitiv data er lekka etter dataangrep i Østre Toten

Etterforskinga dei siste dagane har vist at data ligg ute på det mørke nettet. Kommunen seier persondata har hamna på «det mørke nettet».

Hva er informasjonssikkerhet?

Konfidensialitet (Confidentiality)
Integritet (Integrity)
Tilgjengelighet (Availability)

Konfidensialitet

«Med konfidensialitet menes i Normen at helse- og personopplysninger må være **sikret mot at uvedkommende får kjennskap til opplysningene**.

Konfidensialitet bidrar til ivaretagelse av taushetsplikt og personvern, noe som er viktig for innbyggernes tillit til helse- om omsorgstjenesten.»

Konfidensialitet

Dataangrep på ambulansesystem: Vet fortsatt ikke om data er hentet ut

Jobber fortsatt med å finne ut om noe er hentet ut etter dataangrepet før påske.

Det var kommunikasjonssystemene mellom ambulanser og AMK-sentralen i Helse Nord som ble rammet av dataangrepet. *Foto: Jon Olav Nesvold/NTB*

Oskar Hope-Paulsrud Sikkerhet

21. apr. 2022 - 13:00

Facebook Twitter Linkedin

Helse Nord jobber fortsatt med å undersøke dataangrepet de ble utsatt for for påske.

Ansatt snoket i kvinnens journaler: – Tilliten er lik null

TRONDHEIM (VG) Det var en rutinekontroll som først avdekket at en ansatt hadde snoket i 42-åringens journaler. Siden begynnelsen av 2019 er det gitt til sammen 13 advarsler for journalsnoking til helsepersonell.

Av JENNY-LINN LOHNE og DAVID ENGMO (FOTO)
9. september 2020

– Tilliten er lik null, sier kvinnen om forholdet sitt til Østmarka avdeling på St. Olavs hospital.

Integritet

«Med integritet menes i Normen at helse- og personopplysninger må være **sikret mot utilsiktet eller uautorisert endring eller sletting**.

Integritet er en forutsetning for god og forsvarlig helsehjelp.»

Integritet

Norge

Oldemor fikk vite at hun var gravid med tvillinger

En oldemor på 76 år i Asker fikk nylig beskjed fra sykehuset om at hun var gravid - og det med tvillinger. Fadesen skyldes trolig at legens innleste notater har blitt feiltolket.

Sykehuset i Asker og Bærum er en del av Vestre Viken helseforetak. *Foto: STIAN LYSBERG SOLUM / NTB SCANPIX*

Tilgjengelighet

«Med tilgjengelighet menes i Normen at helse- og personopplysninger som skal behandles, er **tilgjengelig til den tid og på det sted det er behov for** opplysningene.

Tilgjengelig informasjon for helsepersonell er en forutsetning for god og forsvarlig helsehjelp.»

Tilgjengelighet

Kvinne døde etter løsepengevirus-angrep

Skal være første gang denne typen angrep har fått fatale konsekvenser.

En kvinne døde etter at hun måtte sendes til en annen by da sykehuset ble rammet av et løsepengevirusangrep. *Illustrasjonsfoto: Marius Jørgenrud*

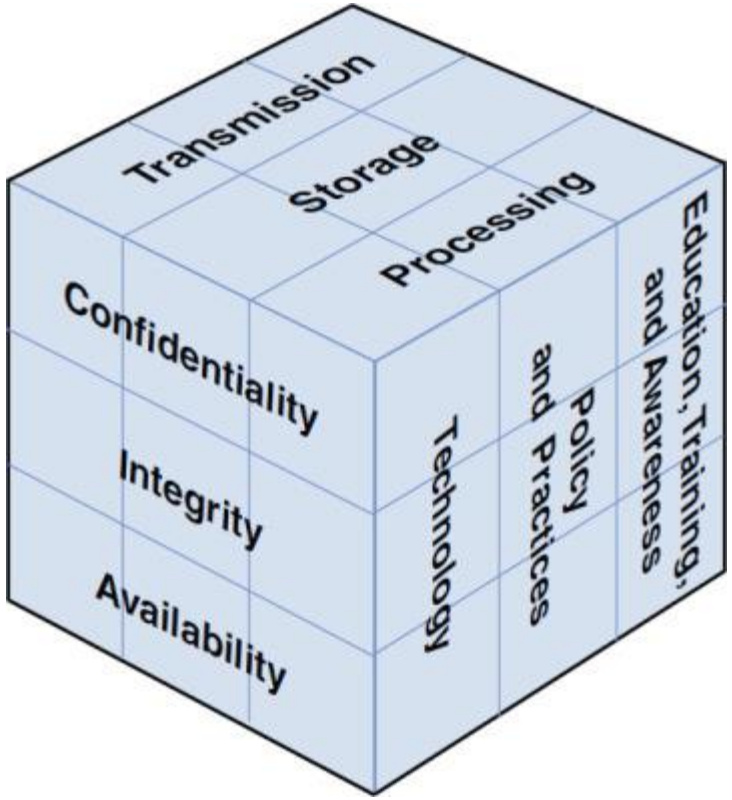
Redaksjon Sikkerhet

18. sep.. 2020 - 11:52

Facebook Twitter Linkedin

En kvinnelig pasient måtte omdirigeres til et annet sykehus etter at sykehuset i Düsseldorf ble rammet av et såkalt løsepengevirus-angrep. Det førte til at kvinnen ikke fikk hjelp i tide, og døde.

Mange dimensjoner



Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

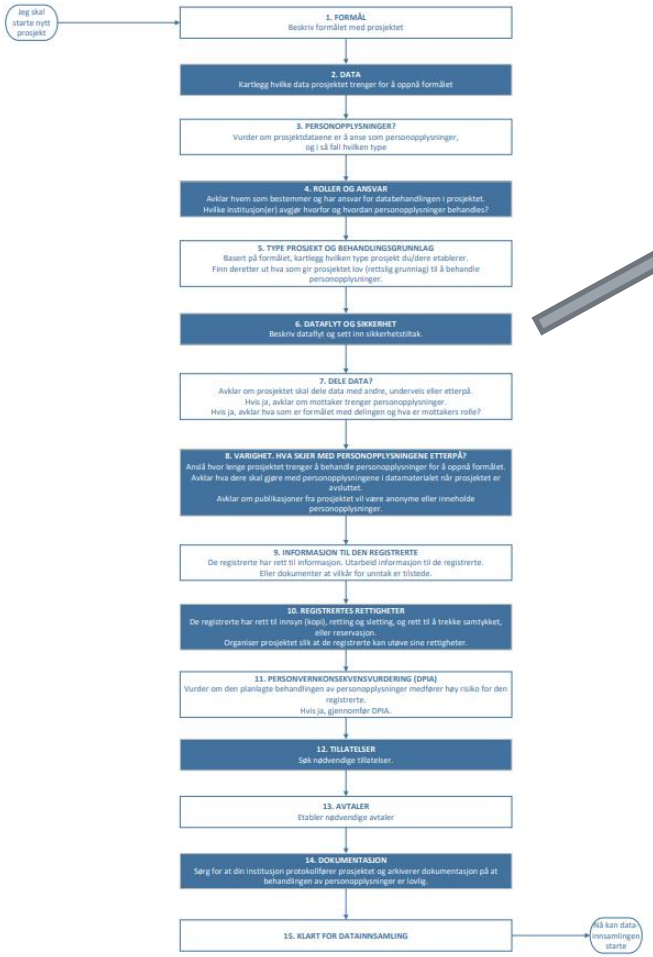
«Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern hos den enkelte virksomhet, i felles systemer og infrastruktur, og i sektoren generelt.»

https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

Normen

https://www.ehelse.no/normen/normen-dokumenter/Veileder-i-personvern-og-informasjonssikkerhet-i-forskningsprosjekter

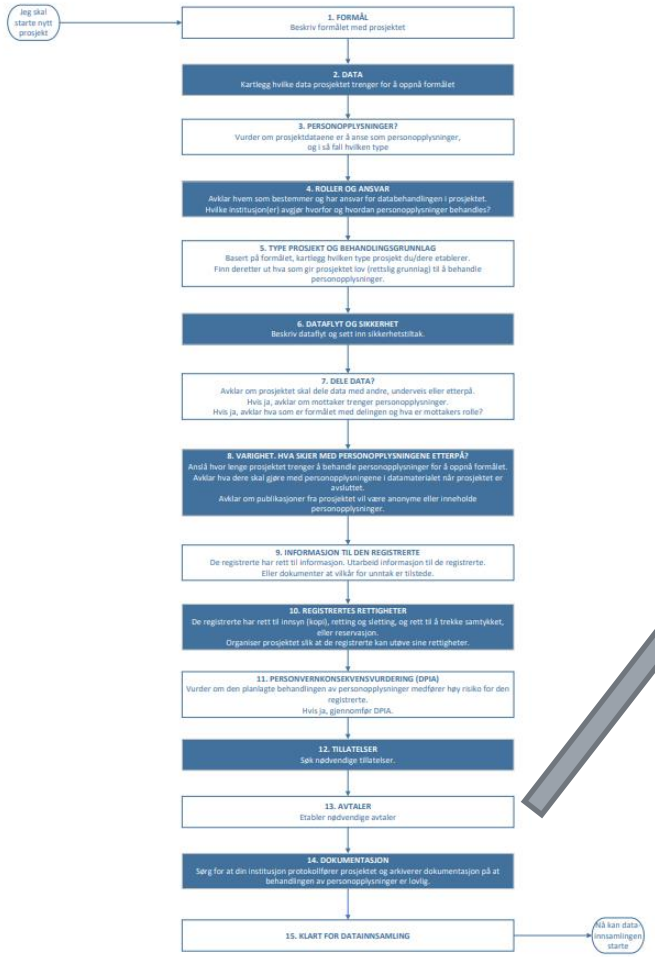
Normen - flytskjema



6. DATAFLYT OG SIKKERHET
Beskriv dataflyt og sett inn sikkerhetstiltak.

Beskrivelsen av dataflyt og vurderingen av sikkerhetstiltak må være god og riktig. Det kan være hensiktsmessig og i noen tilfeller nødvendig, å be om bistand fra IT-ressurser ved din institusjon for å sikre dette, særlig når dataflyten er kompleks og/eller kan innebære høy risiko. Du bør også rådføre deg med din institusjon dersom prosjektet skal bruke nytt utstyr, løsning eller leverandør som ikke allerede er vurdert av institusjonen. Vi anbefaler at du gjør dette i god tid før datainnsamling.

Normen - flytskjema



13. AVTALER
Etabler nødvendige avtaler

15.3 Databehandleravtale

Når det tas i bruk leverandører av f. eks laboratorietjenester, lagringstjenester ol., der leverandøren vil behandle personopplysninger på vegne av prosjektet, må det inngås en databehandleravtale. Denne avtalen vil sette rammen for behandlingen av personopplysninger. Merk også at det kan være tilfeller der din institusjon kan behandle personopplysninger på instruks fra andre og derfor vil ha rollen som databehandler, også da er det nødvendig å inngå en databehandleravtale.

https://www.sykehuspartner.no/nyheter/trusselvurdering-2023--det-digitale-trusselbildet-mot-spesialisthelsetjenesten/

Trusselvurdering – relevant for forskning?

Relevant? Ja, absolutt!

«Forskningsinformasjon kan være spesielt attraktiv for videresalg, men kan også brukes i digital utpressing (informasjonslekkasje). Sikkerhetsselskapet Mandiant trekker frem forskningsinformasjon som en sentral driver for trusselaktørers aktivitet mot helsesektoren globalt.»

Relevant? Ja, absolutt!

Vurdering av aktører spesialisert på å hente ut informasjon for videresalg

Vurderingen av disse aktørene har et lavt til medium konfidensnivå. Det vurderes som **mulig** at organiserte kriminelle aktører vil utføre angrep mot spesialisthelsetjenesten med formål kompromittering og videresalg av informasjon som en metode for økonomisk vinning. Vi vurderer **sannsynlige** informasjonsmål å være forskning og innovasjon, samt finansiell og økonomisk informasjon. **Mulige** mål vurderes å være person- og helseopplysninger og påloggingsopplysninger.

Forskningsdata er også interessant for statlige aktører, og flere stater søker aktivt etter informasjon som kan bidra til at egen industri tar teknologiske steg raskere [2]. Norske universiteter og forskningsinstitusjoner vil ifølge PST bli forsøkt utnyttet for ulovlig kunnskapsoverføring, og Russland, Kina og Iran vil representere en særskilt utfordring [1].

Statlige aktører vurderes å utgjøre en betydelig trussel for spionasje mot spesialisthelsetjenesten. Det vurderes som **meget sannsynlig** at Russland og Kina er de statlige aktørene med størst vilje til å utøve spionasje mot spesialisthelsetjenestens verdier. Samlet vurderes det som **meget sannsynlig** at fremmede staters sikkerhets- og etterretningstjenester har vilje til å drive spionasje mot spesialisthelsetjenestens forskningsmiljøer. Videre vur-

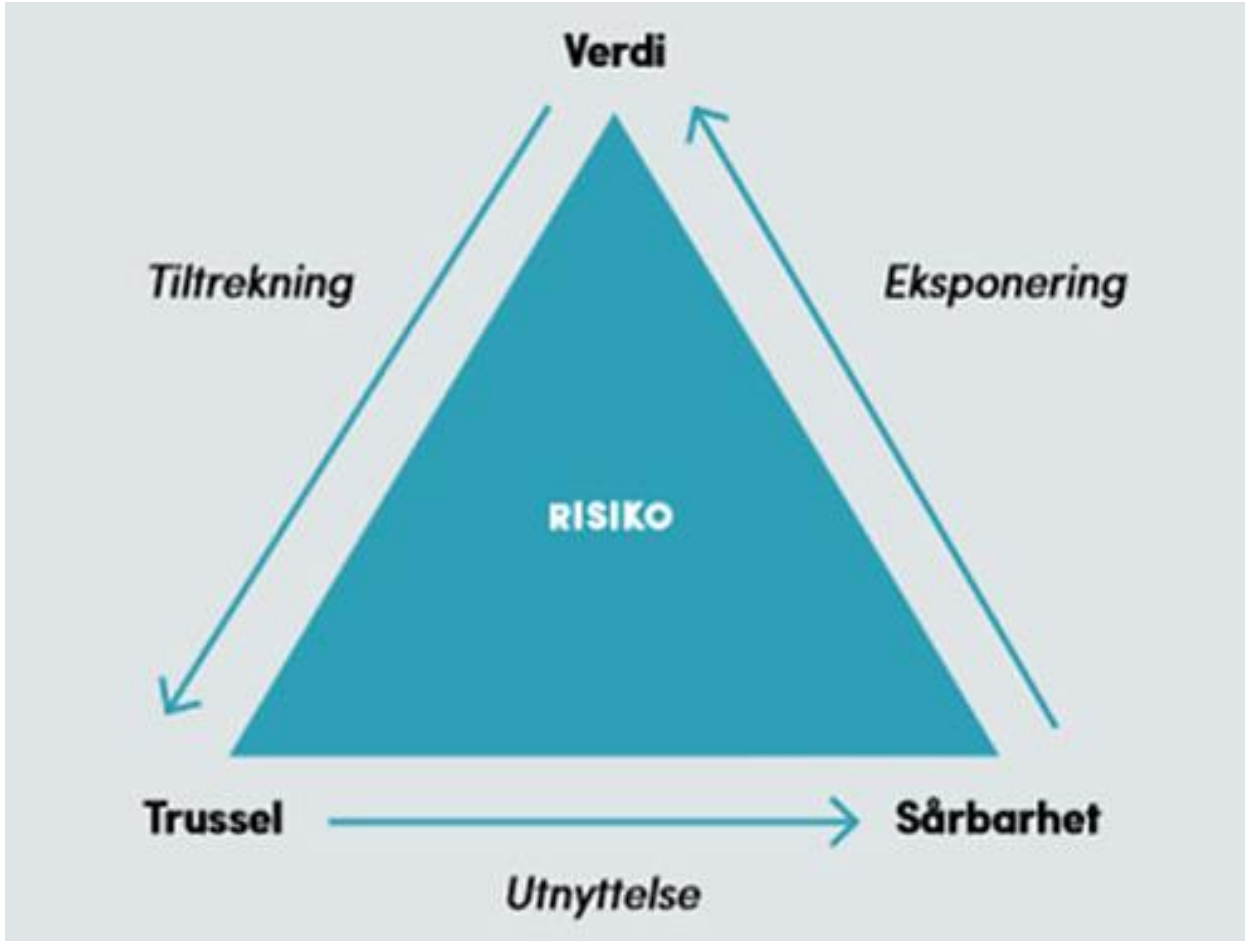
Danske CFCS viser til at kriminelle aktører kan gå etter forskningsdata eller patenter i helsektoren for å videreselge informasjonen [29], [46]. Finansiell informasjon

Forskning, utvikling og innovasjon

Forskningsinformasjon kan være spesielt attraktiv for videresalg, men kan også brukes i digital utpressing (informasjonslekkasje) [46], [29]. Sikkerhetsselskapet Mandiant trekker frem forskningsinformasjon som en sentral driver for trusselaktørers aktivitet mot helsesektoren globalt [42].

Det vurderes som **meget sannsynlig** at helseopplysninger og personopplysninger er de mest attraktive informasjonsmålene til digitale utpressingsaktører (informasjonslekkasje). Det vurderes som **sannsynlig** at forskning og innovasjon, påloggingsopplysninger

Trussel i et risikoperspektiv



Trusselvurdering 2023 - Trusselaktører

Organiserte kriminelle aktører

Statlige aktører

Hacktivister

Selvmotiverte innsidere

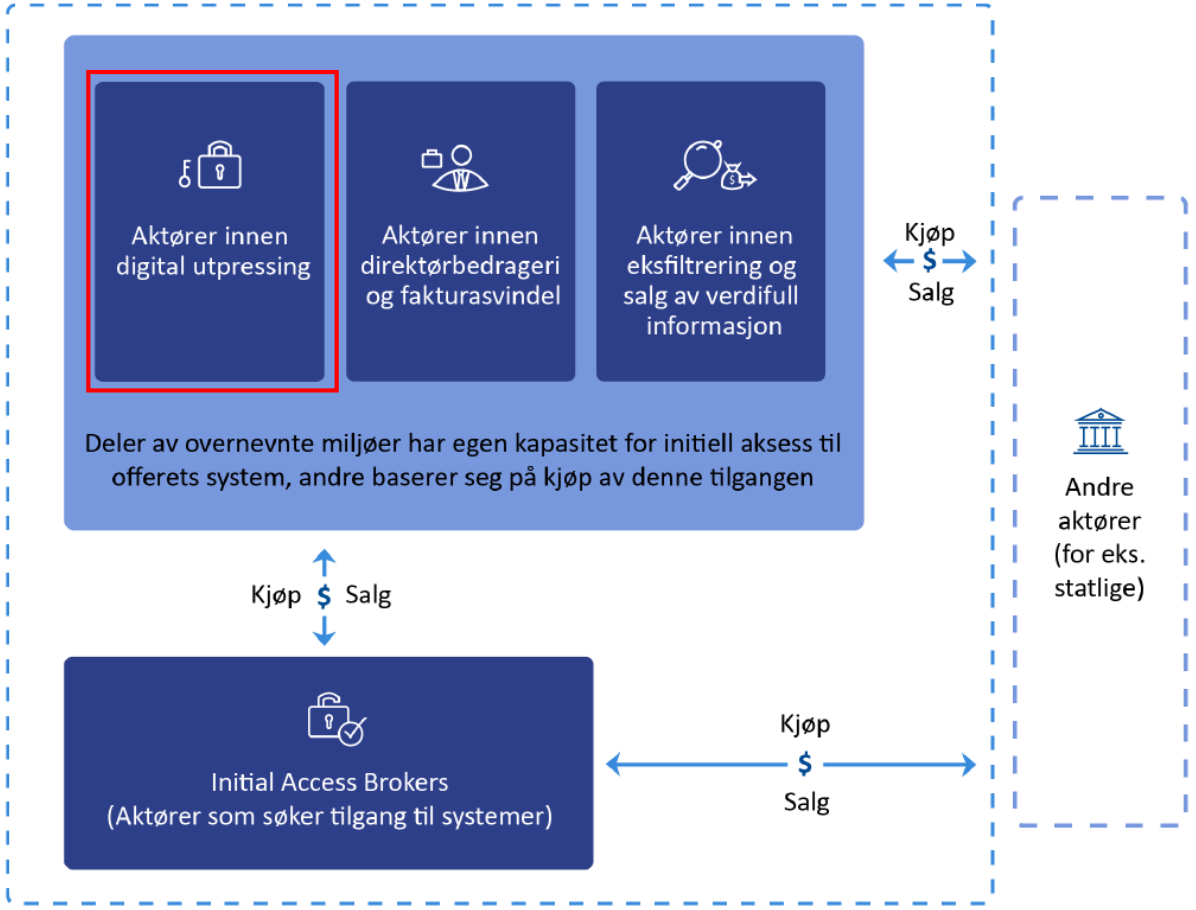
Trusselvurdering 2023 - Hovedtrussel

Den mest alvorlige trusselen identifisert er fra organiserte kriminelle aktører som driver digital utpressing. De har både vilje og evne til å angripe spesialisthelsetjenesten og krever løsepenger[1] for å låse opp systemer og unngå offentliggjøring av sensitiv informasjon.

[1]Gjennomsnittskostnaden i 2022 for et digitalt utpressingsangrep mot helse globalt, var ca. 100 millioner kroner

Aktører som driver med digital utpressing	Vilje	Evne	Skadepotensiale
	Meget høy	Høy	Meget høyt

Trusselvurdering 2023 – Aktører innen digital utpressing

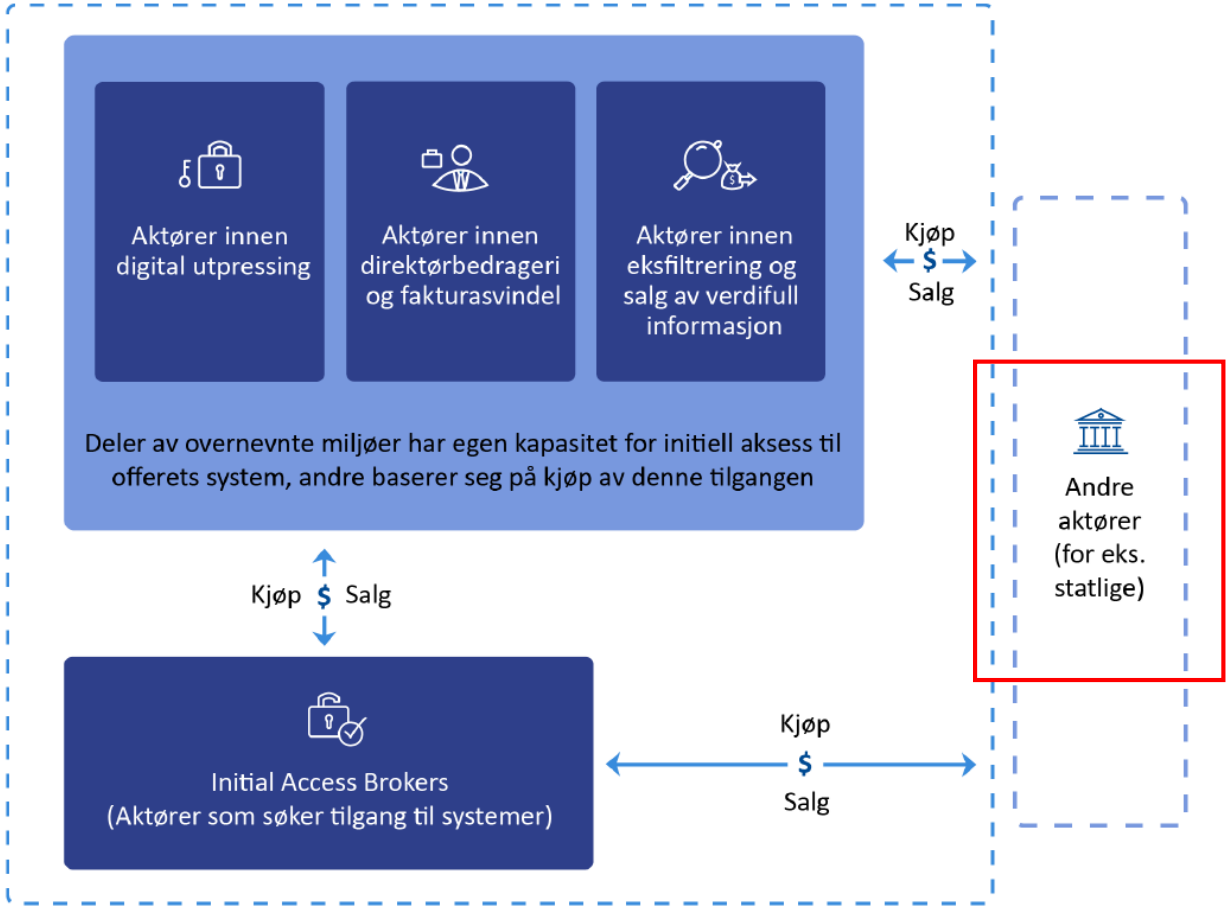


Eksempel organiserte kriminelle aktører - Conti

Figure 8: Conti's organization chart concluded from the leaks

Source: Cyberint

Trusselvurdering 2023 – Aktører innen digital utpressing



Trusselvurdering 2023 – Statlige aktører

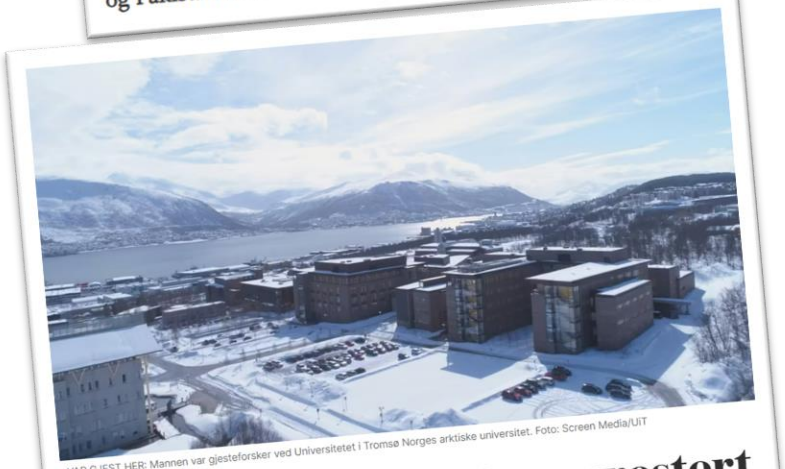
PST: Norske forsknings- og utdanningsinstitusjoner utnyttes til ulovlig kunnskapsoverføring

Av Julia Loge
Publisert 17. februar 2023 kl. 09:30

I trusselvurderingen for 2023 trekker PST fram Russland, Kina, Iran og Pakistan som utfordringer for forskningsmiljøene.

Stillinger
Se alle stillinger

Kilde: forskerforum.no, 17.02.2023



VAR GJEST HER: Mannen var gjesteforsker ved Universitetet i Tromsø Norges arktiske universitet. Foto: Screen Media/UiT

Mistenkt russisk spion arrestert i Tromsø

Justisdepartementet mener at mannen er en trussel mot norske interesser og varslet om utvisning av ham allerede 20. oktober.

Kilde: vg.no, 25.10.2022

SIKKERHET

USA anklager Kina for hacking av vaksineforskning

Kina avviser anklagene som grunnløse.

Kilde: digi.no, 12.05.2020

SIKKERHET

PST: – Alle som har informasjon, må regne med å bli utsatt for russisk etterretningsaktivitet

Politiets sikkerhetstjeneste (PST) tar over etterforskningen av dronesakene. Nå varsler de endret kurs fra russisk etterretning i Norge.

Kilde: digi.no, 19.10.2022

Trusselvurdering 2023 – Selvmotiverte innsidere

Selvmotiverte innsidere - Overordnet vurdering mot spesialisthelsetjenesten: (Viljenivået er gitt i begrepet selvmotiverte, derfor vurderer vi sannsynlighet i stedet for vilje)		
Sannsynlighet	Evne	Skadepotensiale
Meget lite sannsynlig	Personell med evne og mulighet til å påføre spesialisthelsetjenesten meget høy skade	Meget høyt
Meget sannsynlig	Personell med evne og mulighet til å påføre spesialisthelsetjenesten medium skade	Medium

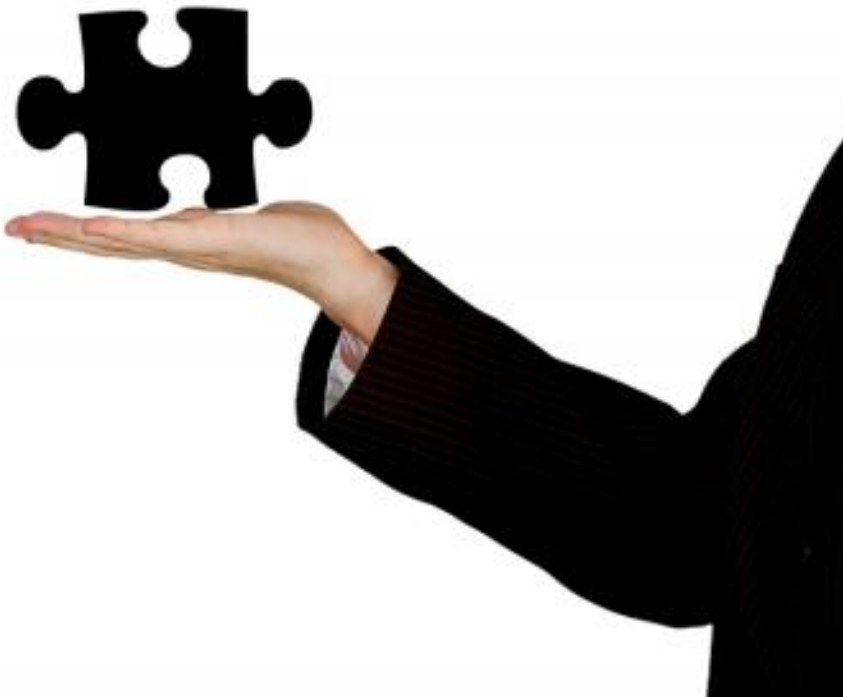
«Et forsøk på å rekruttere en norsk forsker kan for vedkommende fremstå som tilforlatelig og legitimt. Klassisk kinesisk fremgangsmåte er å invitere aktuelle personer til Kina. Det kan gjerne begynne med at forskeren blir spurt om å skrive en artikkel for en kinesisk tenketank, mot god betaling.

Deretter blir vedkommende invitert til konferanser i Kina, med alle utgifter dekket. Videre fortsetter relasjonsbyggingen i ulike sosiale sammenhenger. I realiteten er målet å få vedkommende til å dele sensitiv informasjon», skriver PST.

Kilde: forskerforum.no, 17.02.2023

Sikkerhetskultur

Kontinuerlig arbeide med å øke ansatte bevissthet, motivasjon og forståelse, og heve kompetansen innen sikkerhet på alle nivåer i virksomheten.



Sikkerhetskultur

«**Å lede arbeidet med sikkerhetskulturutvikling er en lederoppgave.** Det er av stor betydning at toppledelsen er involvert og har forståelse for behovet for å bygge en sikkerhetskultur mot dataangrep.»

- Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer

Mennesket – «Det viktigste sikkerhetstiltaket»

NSM anbefaler at virksomheter som er underlagt sikkerhetsloven gjør følgende for alle ansatte:

- Ha god dialog med alle ansatte. Sikre at alle ansatte har tilstrekkelig risiko- og sikkerhetsforståelse i en ny sikkerhetspolitisk situasjon, gjennom for eksempel felles orienteringer/oppdateringer om sikkerhet.
- Praktiser en god sikkerhetskultur med sikkerhetsbevisst personell som viser årvåkenhet, bærer ID-kort, påpeker når andre glemmer det, følger besøk, fanger opp besøk på vandring, varsler om irregulære e-poster, og viser varsomhet ved åpning av vedlegg.
- Sikre at alle ansatte forstår viktigheten av å si fra dersom de opplever press, trusler eller annen tilnærming fra personer som kan ha interesser inn mot virksomheten. Alle skal vite hvem i virksomheten de skal kontakte ved slike tilfeller.
- Tilby samtaler til personell som ønsker å snakke om egne potensielle sårbarheter.

Kilde: Nasjonal sikkerhetsmyndighet (https://nsm.no/aktuelt/sikkerhetskompetansen-hos-ansatte-ma-styrkes)

Sikkerhetskompetansen hos ansatte må styrkes

Publisert: 18.03.2022

PST vurderer at etterretningstrusselen fra Russland er høyere nå enn før krigen i Ukraina. Norske virksomheter som har tilknytning eller samarbeid med Russland eller Ukraina må derfor forvente at de er relevante mål for russisk etterretning eller påvirkning.

«... det som oftest er grunnleggende svakheter i sikkerhetstilstanden som muliggjør vellykkede angrep. »

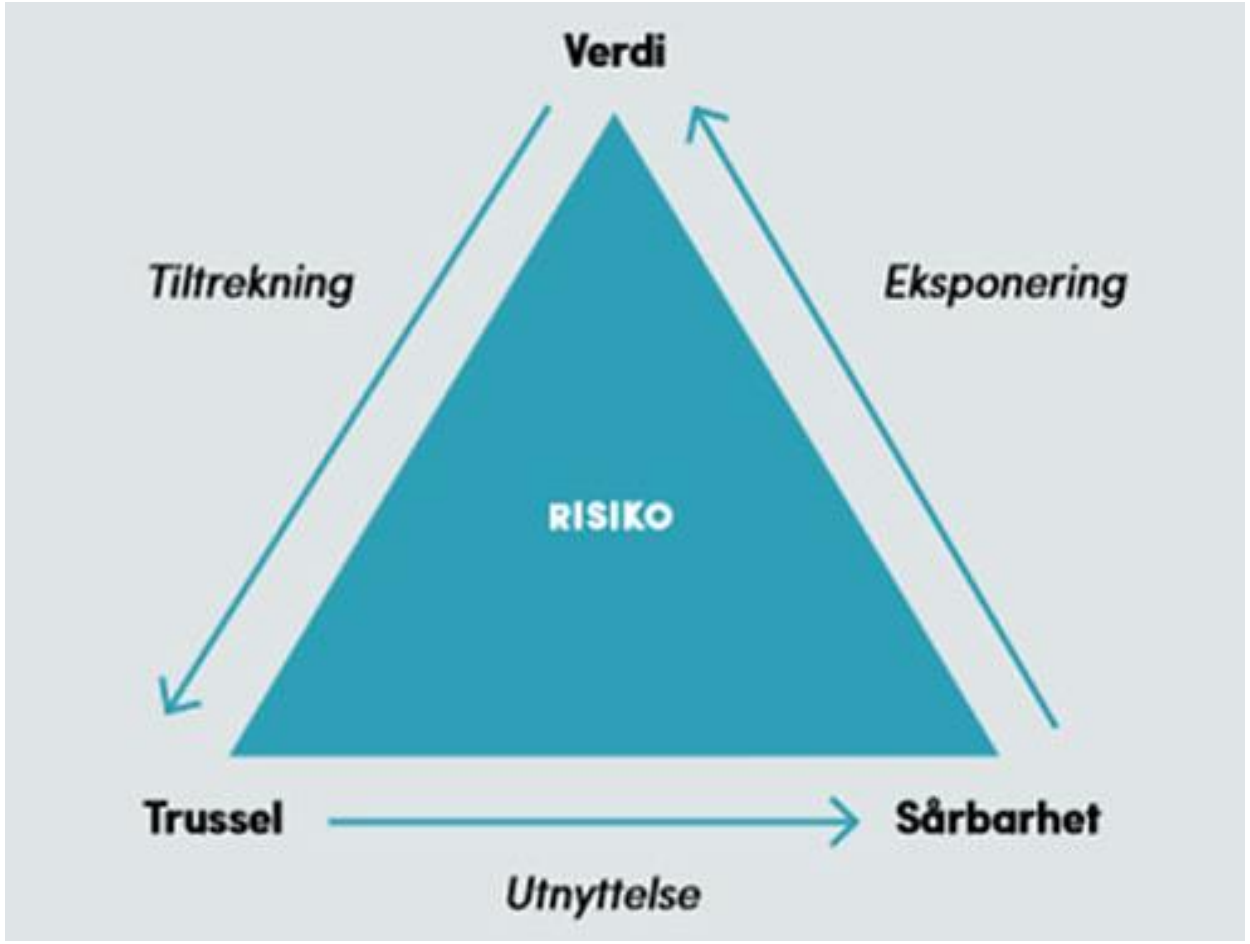
https://www.sykehuspartner.no/nyheter/trusselvurdering-2023--det-digitale-trusselbildet-mot-spesialisthelsetjenesten/

Grunnleggende tiltak

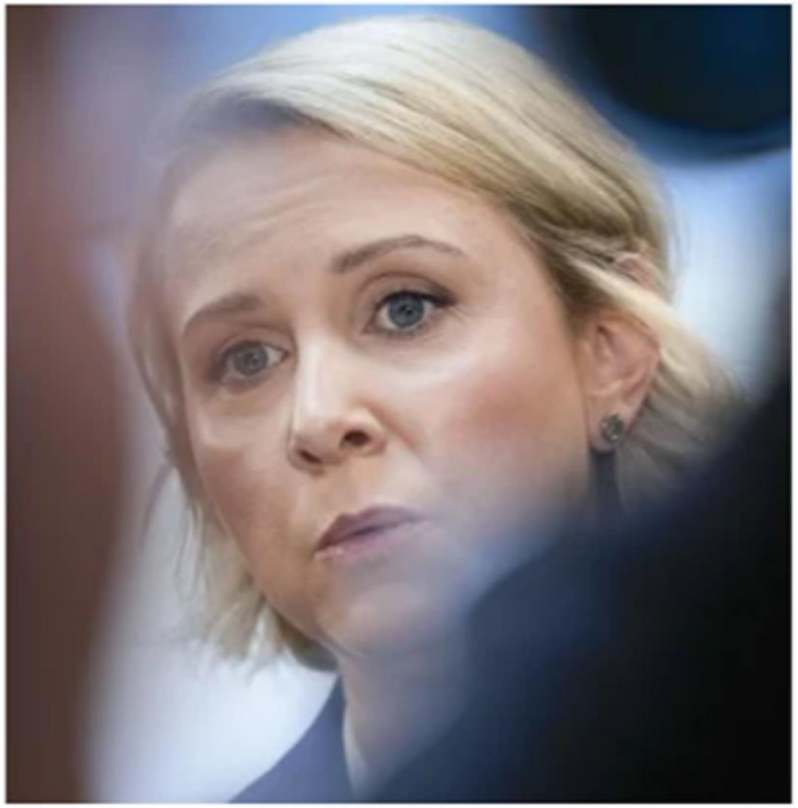
Phishing
assord
atching

+ bruk av minnepenner

Sårbarheter



Sårbarheter



SISTE: Nytt alvorlig cyberangrep mot Norge

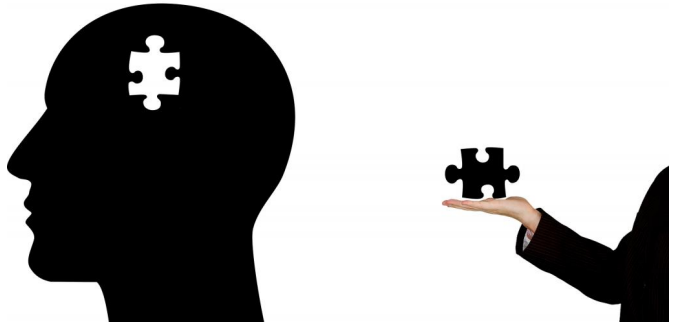
https://www.vg.no/, 23.10.2023

14. Januar 2020

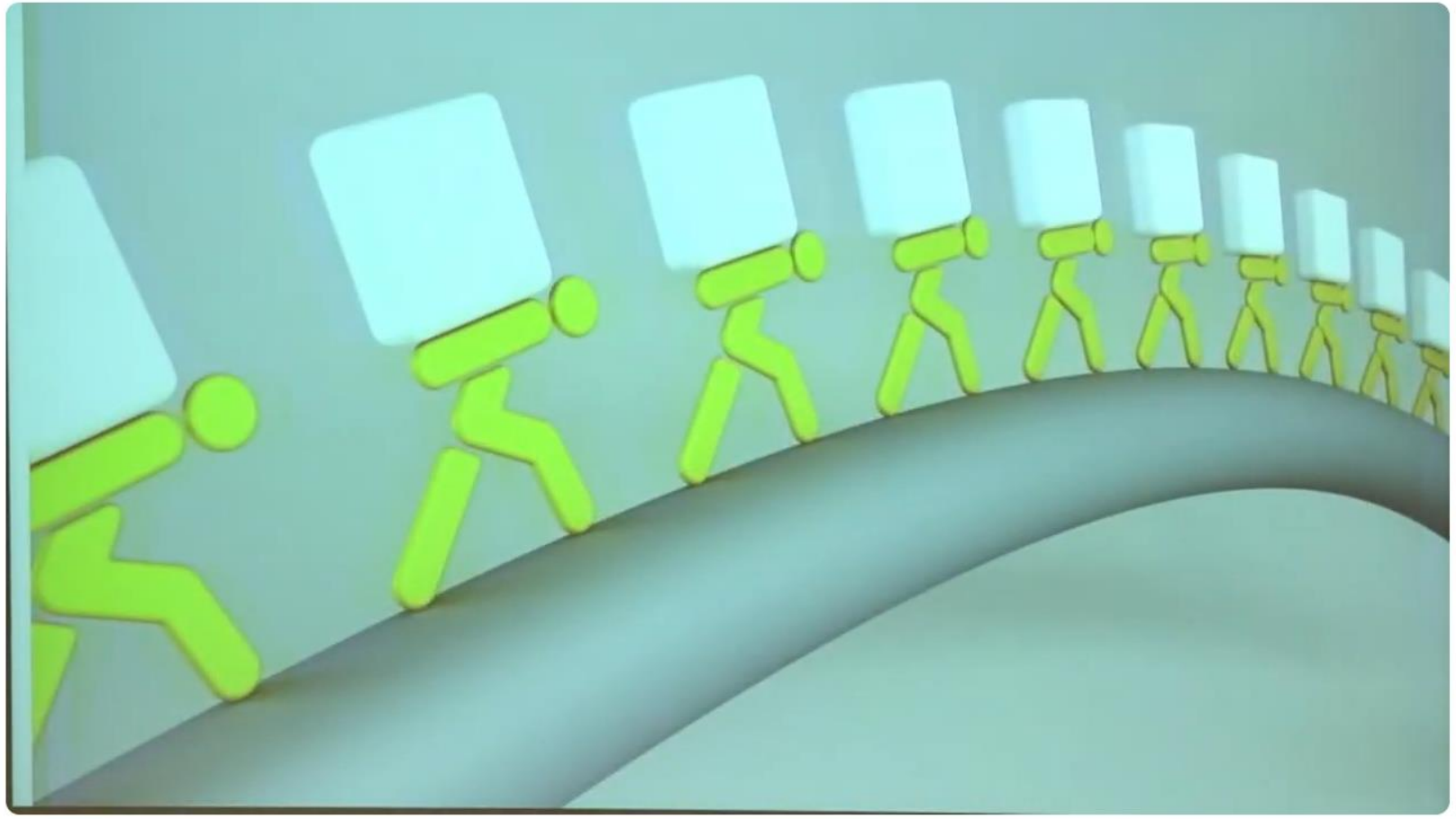
Sårbarheter

If you continue to use Windows 7 now that support has ended, your PC will still work, but it will be more vulnerable to security risks and viruses. Your PC will continue to start and run, but will no longer receive software updates, including security updates, from Microsoft.

Eksempler



Verdikjeder



Fagdag om samfunnssikkerhet og beredskap 28. september 2023

Kilde: https://youtu.be/w1khZzUoVYA?t=4840

«Vi har altså, med å introdusere internett som en funksjonsbærer, gjort oss avhengig av en ekstremt lang, fullstendig uoversiktlig, og utrolig kompleks avhengighetskjede/leverandørkjede.»

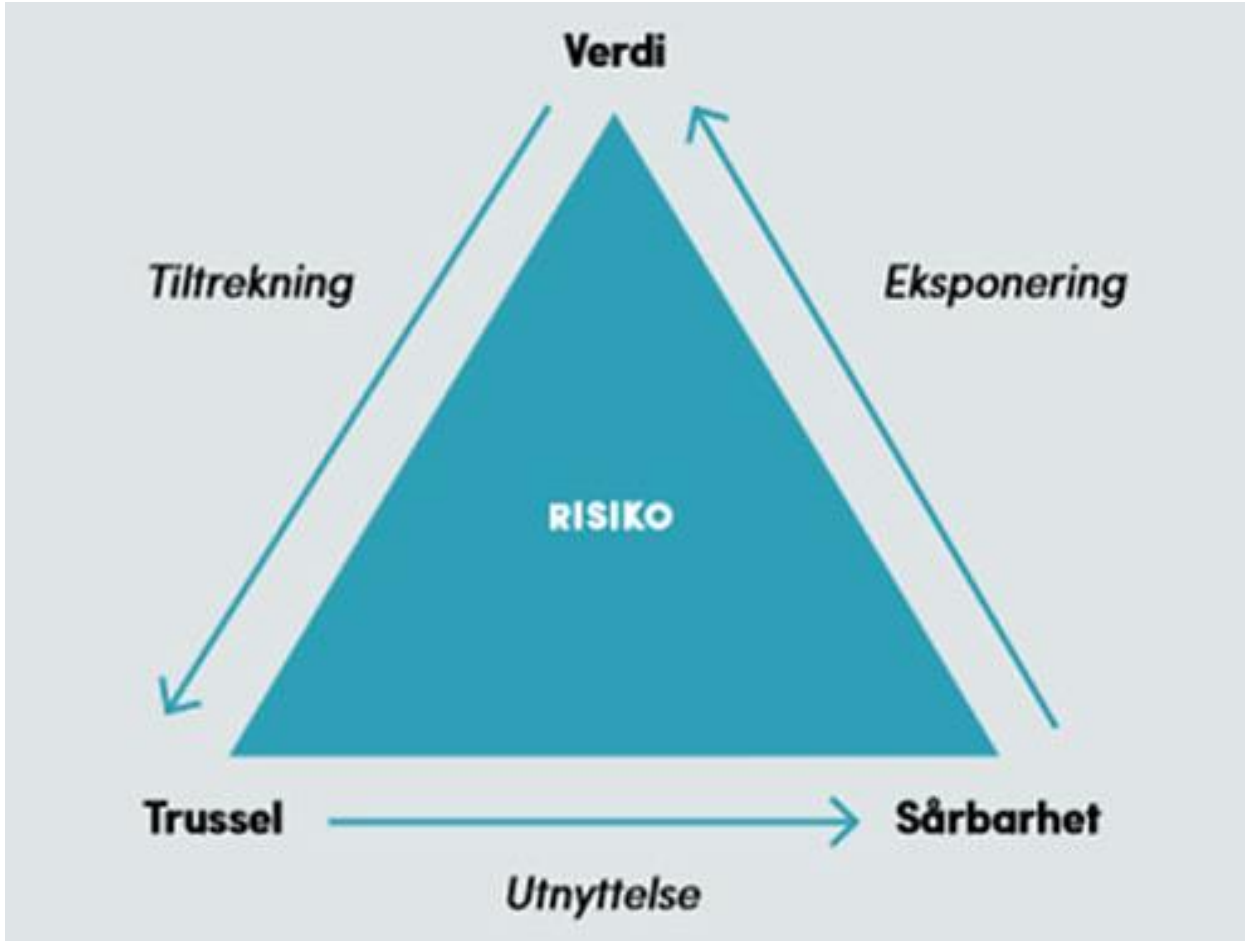
Sitat: Jørgen Dyrhaug, Nasjonal Sikkerhetsmyndighet

Verdikjeder – eksempel databehandleravtale

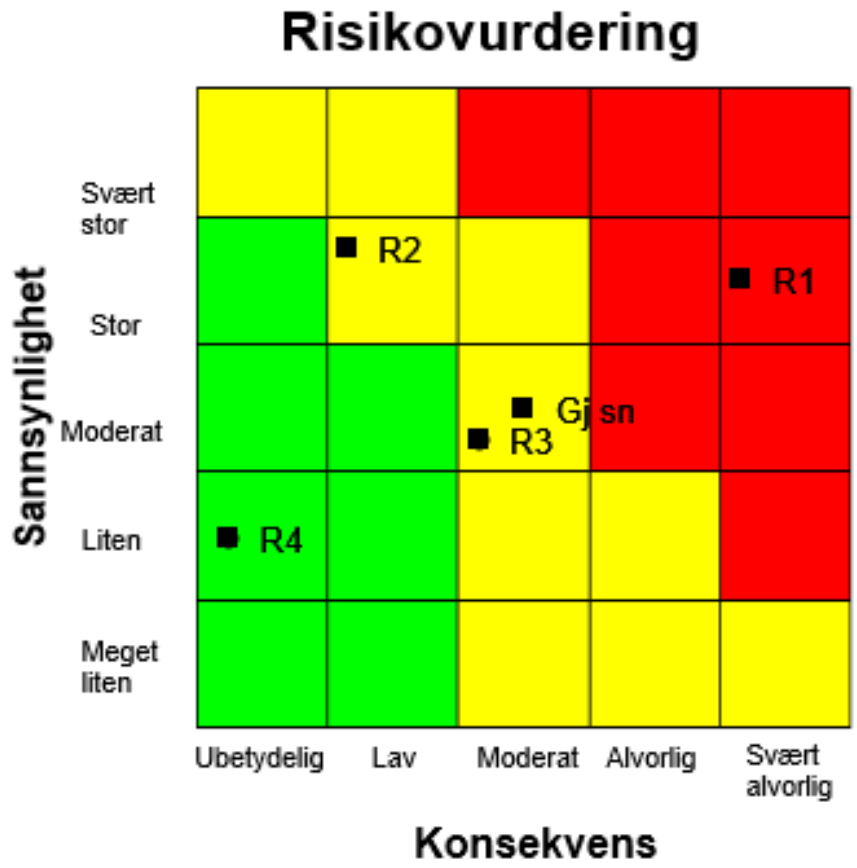
Databehandler benytter følgende underleverandører:
Se vedlegg til databehandleravtalen

Navn	Org.nr	Adresse	Leveransetype (behandling)	Behandlingssted
IDS (Informatique de Sécurité)		2 avenue des Puits, BP 70022, 71301 MONTCEAU LES MINES, France	Data hosting	Frankrike
Cheops Technology France		3 Route de Lyon, 69530 Brignais, France	Teknisk støtte system	Frankrike
Amazon Web Services EMEA SARL		O38 Avenue John. F Kennedy, L-1855 Luxembourg	Data hosting	Tyskland & Frankrike
Vodafone		Vodafone HQ, The Connection Newbury, Berkshire, RG14 2FN, United Kingdom	Telekommunikasjon leverandør	Storbritannia
Okta		2 Waters Park Drive, San Mateo, California 94403	Flerfaktorautentiserings system	Tyskland

Vurder risiko – og iverksett tiltak



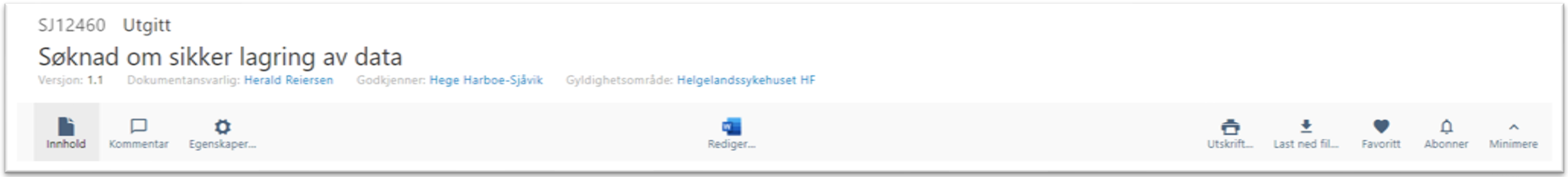

MEDIUM
HIGH
LOW
RISK


Risikovurdering
Svært stor
Stor
Moderat
Liten
Meget liten
Sannsynlighet
R2
R1
Gj sn
R3
R4
Ubetydelig
Lav
Moderat
Alvorlig
Svært alvorlig
Konsekvens

SJ12460 Utgitt

Søknad om sikker lagring av data

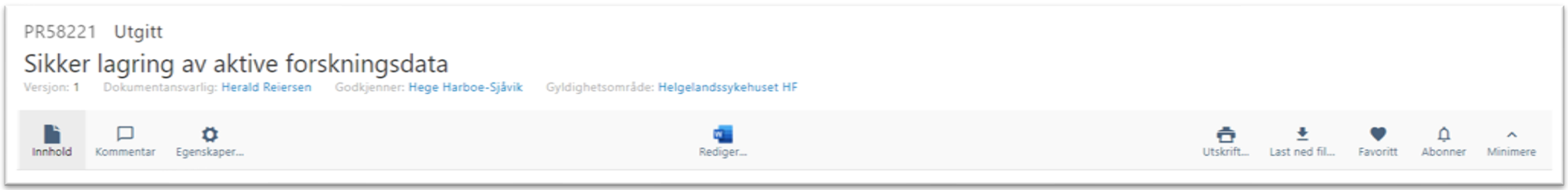
Versjon: 1.1 Dokumentansvarlig: Herald Reiersen Godkjenner: Hege Harboe-Sjåvik Gyldighetsområde: Helgelandssykehuset HF



PR58221 Utgitt

Sikker lagring av aktive forskningsdata

Versjon: 1 Dokumentansvarlig: Herald Reiersen Godkjenner: Hege Harboe-Sjåvik Gyldighetsområde: Helgelandssykehuset HF



SJ12460

PROSJEKTINFORMASJON	
Prosjekttittel:	
Klassifisering av prosjekt: *(Forsknings-/kvalitets-/student/ evt. usikker)*	
Oppstarts- og avslutningsdato for prosjektet:	
Prosjektleder ved HSYK:	
Eventuell ekstern prosjektleder:	
Enhet/område/avd.:	
Kort beskrivelse av type data som skal lagres:	
Tidspunkt for sletting av forskningsdata:	
Rettslig grunnlag for prosjektet (REK, Datatilsynet eller andre):	
Særskilte krav stilt av godkjenningsinstans (REK, Datatilsynet eller andre):	
Annen informasjon om prosjektet:	
TILGANGSINFORMASJON	
Ansatte ved HSYK med tilgang til data (navn og HSYK brukernavn oppgis):	
Eventuelle andre som skal ha tilgang:	
Ansatte ved HSYK med tilgang til key-mappe (koblingsnøkkel) (navn og HSYK brukernavn oppgis):	

Viktig å oppdatere underveis – ikke bare ved bestilling!

PR58221

4.4 *Koblingsnøkkel*

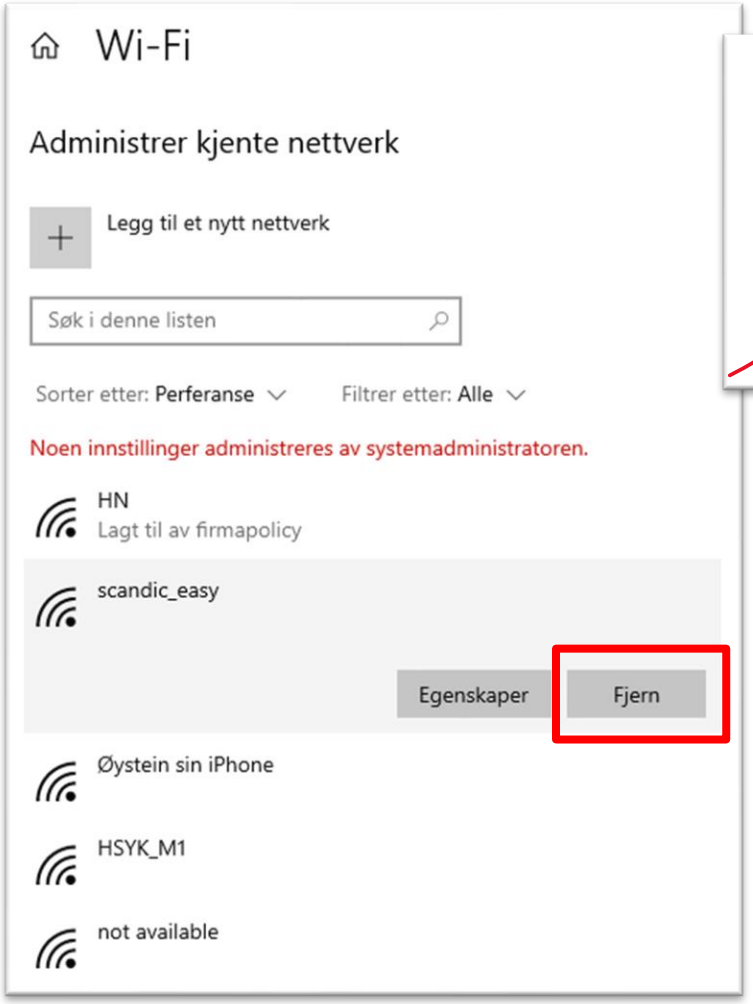
- Hovedregelen er at helseforskningsdata skal oppbevares avidentifisert, det vil si at forskningsdata og identifiserende elementer (koblingsnøkkel) skal lagres hver for seg.
- Lagres både data og koblingsnøkkel elektronisk, er det krav om at disse lagres på adskilte områder, og koblingsnøkkelen må være spesielt sikret.
- Tilgangen til koblingsnøkkelen skal sterkt begrenses etter at datainnsamling og kvalitetssikring er fullført. Ved Helgelandssykehuset er et eget serverområde opprettet for å ivareta dette. Kun et begrenset antall ansatte med rettigheter vil ha tilgang til denne delen.

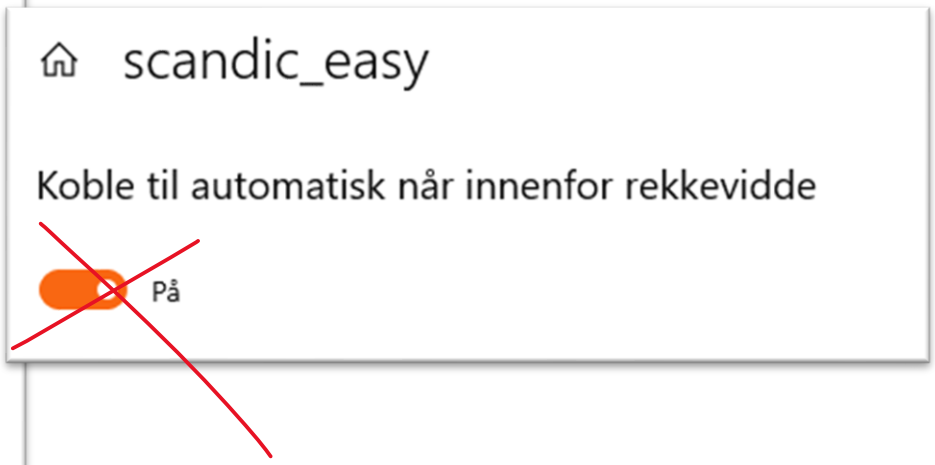
4.5 *Fysisk lagring*

- Ved lagring av fysiske dokumenter/persondata som ikke er anonymiserte, skal dokumentene oppbevares nedlåst. Kun en definert brukergruppe skal ha tilgang. Rommet som benyttes til lagring av fysiske data skal låses når man forlater det.

+ + +

Wifi





7. Foretrekk 4G fremfor tredjeparts Wi-Fi

Unngå generelt bruk av Wi-Fi som ikke krever et passord for tilkobling, og benytt kun kjente Wi-Fi-nettverk. Unngå bruk av offentlige, gratis Wi-Fi på for eksempel på hoteller, caféer og flyplasser, og på konferanser. Bruk heller din telefon til internett-deling (4G mobildata).

Spørsmål