



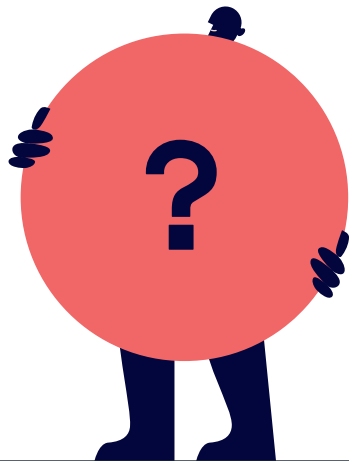
# DILEMMA

Eirik er ansatt i forskningsavdelingen ved Utmarka høgskole. I forbindelse med forskning han har gjort tilknyttet en nasjonal forskningsgruppe har Eirik intervjuet innsatte på høysikkerhetsavdelingen ved Utmarka fengsel.

Forskningsgruppen er ledet av en professor ved Hovedstatsuniversitetet. Prosjektet har en referansegruppe, som består av eksterne og interne ledere. Et av medlemmene i referansegruppa er leder ved Utmarka fengsel.

En dag får Eirik en telefon fra forskningsleder ved Hovedstatsuniversitetet. Lederen spør om Eirik kan presentere intervjuene sine for forskerne og referansegruppa i prosjektet. Eirik er veldig i tvil om hvordan han skal presentere intervjuene og hvordan han kan anonymisere informantene sine. Forskningslederen sier at alle involverte i prosjektet har taushetsplikt. Han foreslår at Eirik i e-posten med manus for innlegget også sender noen av intervjuene i heltekst, slik at forskergruppen kan gi gode kvalifiserte innspill og råd. «På dette stadiet i forskningen er det ikke viktig at materialet er anonymisert», sier han.

Eirik er usikker på om dette ivaretar informasjonssikkerheten.



## Spørsmål – og innspill til deltagere

- Om bruk av e-post – alle sider av informasjonssikkerhet (KIT) må vurderes
- Taushetsplikt – gjelder for hvem?
- Samtykke?
- Er det viktig at informasjonen ikke kommer på avveie
- Er det viktig at informasjonen ikke kan endres?
- Er det viktig at informasjonen er riktig når den sendes?
- Er det greit å dele disse opplysningene på andre måter – ved bruk av snegle-post?
- Hvor «sikkert» er e-post?

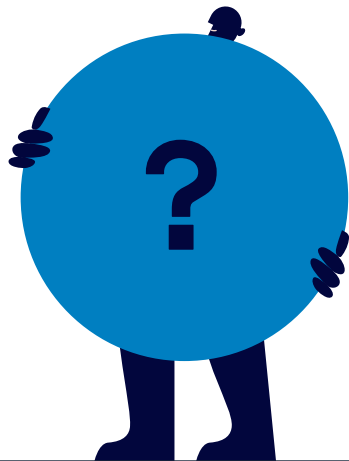


# DILEMMA

Synne reiser til Hovedstatsuniversitetet for å holde et innlegg på en konferanse.

Hun har tatt backup av slides til foredraget og lagt det i en skytjeneste som telefonen og nettbrettet hennes bruker. Hun bruker samme skytjeneste til backup av eget forskningsmateriale. Skytjenesten skal være sikker. Synne er redd for at datamaterialet skal bli borte eller komme på avveie. Hun har derfor også tatt ekstra kopier på minnepinner som hun alltid har med i veska. I tillegg sender hun alltid siste utkast av materialet til gmailen sin og hotmailen sin.

Synne er usikker på om dette ivaretar informasjonssikkerheten.



## Spørsmål – og innspill til deltagere

- Hva slags informasjon? – utfør riskikovurdering – er dette personopplysninger, er dette sensitive opplysninger?
- Om bruk av e-post – alle sider av informasjonssikkerhet (KIT) må vurderes?
- Om bruk av minnepinne – alle sider av informasjonssikkerhet (KIT) må vurderes?
- Om bruk av skytjenester – alle sider av informasjonssikkerhet (KIT) må vurderes?
- Hva er skytjenester?
- Er det viktig at informasjonen ikke kommer på avveie?
- Er det viktig at informasjonen ikke kan endres?
- Hvor viktig er det at en alltid har tilgang til informasjonen?
- Hvor «sikkert» er e-post, minnepinne, skytjenester?



# DILEMMA

Ola er ansatt i HR-avdelingen. Han har ansvar for oppfølging av langtidssykemeldte. En ansatt i IKT-avdelingen har vært sykmeldt etter en bilulykke. Hun skal nå begynne på fysisk opptreningsprogram hos Frisktrening AS tre dager i uken.

En dag får Ola en telefon fra daglig leder for aktivitetssenteret på Frisktrening. Hun har flere spørsmål om den ansattes situasjon, blant annet helsetilstanden. Hun skulle gjerne ha fått tilsendt opplysningene på e-post, slik at hun kan vurdere om den ansatte kan delta på de ulike aktivitetene som tilbys.

Den ansatte har tidligere samtykket til at Frisktrening kan få denne informasjonen. Ola har allikevel ikke lyst til å sende dette på e-post. Frisktrening-lederen mener at deler av informasjonen må kunne sendes på e-post. Eventuelt kan han sende alt hvis han bare ikke oppgir navn. Ola er usikker. Hvordan kan han egentlig bruke e-post i sin arbeidshverdag og samtidig ivareta informasjonssikkerheten?

Ola rådfører seg med sine kolleger i en pause om hva han bør gjøre.



# DILEMMA

Eva jobber i en avdeling der de ikke har fokus på formelle prosedyrer og øvelser.

De har en beredskapsplan med prosedyrer for å håndtere hendelser, men det er flere år siden denne ble oppdatert. De har heller aldri øvd på hva de skal gjøre hvis en større informasjonssikkerhetshendelse skulle inntreffe. Det har de siste årene vært noen mindre hendelser. Disse har blitt håndtert helt fint av de som var på jobb, uten å kalle inn ekstra hjelp, og uten å forholde seg til beredskapsplanen.

DSS' ledelse har besluttet at alle avdelinger skal utforme beredskapsplaner, deriblant rutiner for håndtering av informasjonssikkerhetshendelser, både hendelige uhell og planlagt sabotasje. De skal øve på hvordan de håndterer slike hendelser, og planene skal også oppdateres jevnlig.

Verken ledelsen eller de ansatte i avdelingen ser behovet for å øve på sikkerhetshendelser eller å holde beredskapsplanen oppdatert. Det er få hendelser i året, og det oppleves at disse håndteres greit uten beredskapsplan og skriftlige prosedyrer.

Dere møter Eva i kantina, og hun er usikker på om det virkelig er nødvendig å bruke ressurser på øvelser fremfor produksjon?



# DILEMMA

Samir jobber i din avdeling. Etaten har nettopp startet et nytt prosjekt rundt automatisert saksbehandling som skal vare et års tid.

Ansatte fra flere avdelinger skal være med i prosjektet, deriblant Samir. De får nye kontorplasser i et prosjektrom (åpent landskap). Dette ligger i en egen sone med adgang kun for de som er med i prosjektet.

Samtidig som de flytter inn i landskapet får de utdelt nye PC-er. På disse er det et klistremerke med budskapet «Lås PC-en når du går fra den!». Samir husker at informasjonssikkerhetsleder snakket om dette på nyansattkurset han deltok på for lenge siden, men har egentlig aldri forstått hvorfor han skal låse PC-en. Alle i landskapet jobber på det samme prosjektet og har de samme tilganger. Hvorfor skal de låse PC-ene sine?

På et besøk til den gamle avdelingen sin nevner han dette for dere og ønsker diskusjon om dette bare er nok et eksempel på regler som kun er til for regelens skyld.



# DILEMMA

Julia jobber med renhold for etaten deres. Hun har flere ganger oppdaget at det slurves med dokumentetsikkerheten.

Særlig er det én avdeling der hun stadig finner dokumenter med rødt stempel «BEGRENSET» liggende på pulten. Dette gjelder først og fremst når de ansatte forlater kontoret midlertidig, for å hente kaffe, for å hente papirer på skriveren, eller bare for at Julia skal kunne gjøre jobben sin.

Hun synes det er vanskelig å ta dette opp med den enkelte ansatte. Når hun kommer inn til din avdeling for å gjøre rent så spør hun dere om råd for hvordan man bør håndtere slike situasjoner.





# DILEMMA

Assisterende fylkeslege Fredrik Frisk er en travel fyr. Han reiser fylket på kryss og tvers for å møte helseinstitusjoner og andre samarbeidspartnere. Samtidig har han alltid en mengde saker på vent. Det er mye elendighet og mange skjebner for tiden.

For å spare tid og for å slippe køkjøring, tar Fredrik toget til jobben. Det gjør de fleste i distriktet, toget er nesten alltid fullt. Nå kan NSB tilby trådløst nett på togturen. Det passer Fredrik utmerket. Det betyr at han via sin hendige bærbare PC, kan utnytte tiden på toget til å få unna noen saker.

Dette er da ikke noe problem, eller?



# DILEMMA

Agnes arbeider hos Fylkesmannen i Helse- og Sosialavdelingen med førerkortsaker.

En dag ringer Trine. Hun ønsker å få vite om hennes mann, Kåre, får beholde førerkortet sitt eller ei. Hun sier de skal i bryllup om ikke så lenge og er helt avhengige av at Kåre kan kjøre. Det er deres datter som skal gifte seg, og de er nødt til å kjøre i to biler, siden flere av barnebarna skal være med, samt at de skal ha med seg mange gaver og utstyr. Hvis ikke Kåre kan få kjøre, så må de kanskje avlyse hele turen og datteren blir så ulykkelig som ikke får sin far med i bryllupet. Hun må få vite dette nå, så de eventuelt kan forberede seg og finne en annen sjåfør.

Agnes ser i systemet sitt at kona til Kåre heter Trine. Der er ingen informasjon utover det.

Agnes blir usikker på om hun kan svare på dette per telefon. På den ene siden vil hun gjerne hjelpe familien, men hva om de har inne en separasjonssøknad? Og er det egentlig så farlig om feil person får denne informasjonen?



# DILEMMA

Andreas jobbar i Helse- og sosialavdelinga. Han er veldig glad for å få jobbe med det nye satsingsområdet «Eldre i unge miljø» dei neste to åra.

Han må byte kontor plass, fordi alle som arbeider med prosjektet skal vere samla i landskap i same etasje. Alle får nye PC-ar. Det er klistrelapp på dei med beskjeden: «Lås PC-en når du går frå den!»

Andreas hugsar at det vart sagt noko om dette på eit introduksjonskurs, men han har aldri forstått kvifor han skal låse PC-en sin. Alle i landskapet jobbar på det same prosjektet. Dørene inn til landskapet er låste.

Kvifor skal dei eigentleg låse PC-en sin? Andreas har også tilgang til andre fagsystem, men det er vel dei same tilgangane alle har?



# DILEMMA

Trude har ansvaret for postmottaket. Ho går gjennom e-postane og journalfører dei.

Så ser ho ein e-post frå ein advokat med eit vedlegg som heilt tydeleg inneheld sensitive opplysningar. E-posten er stila til ei anna verksemd, så den er nok feilsendt.

Dette inneber at sensitive opplysningar har kome på avvege.

Kva skal Trude gjere? Opne vedlegget? Slette e-posten og late som ingenting? Nei, kanskje heller vidaresende e-posten til sjefen sin og informere om at sensitive opplysningar har kome på avvege?



# DILEMMA

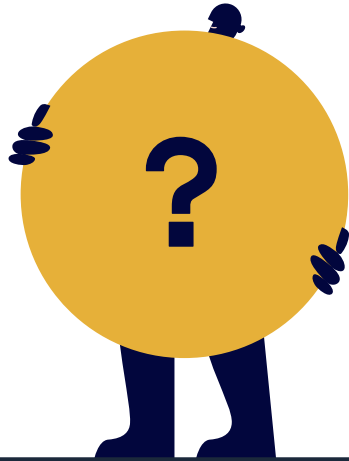
Direktoratet for eksempler leverer samfunnsviktige tjenester og må derfor ha evne til å opprettholde virksomhetskontinuitet i ekstraordinære situasjoner.

Direktoratet har derfor årlige utgifter til beredskapsmateriell. Mye av dette beredskapsmateriellet er lite eller aldri brukt når det kasseres. Det er en utfordrende oppgave å estimere hvor mye beredskapsmateriell som er nødvendig for å opprettholde en tilfredsstillende beredskap.

Riksrevisjonen har varslet formålsrevisjon av direktoratets styring av virksomhetskontinuitet og forvaltning av beredskapsmateriell. Et av spørsmålene som skal besvares er hvilket beslutningsgrunnlag som ligger til grunn for hvor mye beredskapsmateriell som anskaffes og utgiftene for vedlikehold av dette materiellet fram til det kasseres.

Godt arbeid med forebyggende sikkerhet kan bidra til å begrense hvor ofte et sikkerhetstiltak forhindrer en uønsket hendelse eller er nødvendig for å begrense konsekvensen av hendelsen.

Hvordan kan direktoratet dokumentere rett nivå på utgifter til sikkerhetstiltak?



## Spørsmål – og innspill til deltagere

### DILEMMA: Fylkeslege Fredrik Frisk

- Tyvtitting, personen i setet ved siden av kan se dokumentene på PC-en
- Teknisk, er forbindelsen sikker nok?

### DILEMMA: Agnes på førerkort

- Hva er konsekvensen dersom andre enn Kåre får denne informasjonen?  
Hvordan kan innringer identifisere seg? Kan bakgrunnen for å få denne informasjonen være en annen? (Tilsvarende skoledilemmaet fra grunnpakken)

### DILEMMA: Trude på postmottak

- Når skal man varsle? Hvordan varsler man i virksomheten?

### DILEMMA: Andreas Lås PC

- (Tilsvarende Lås-PC dilemmaet fra grunnpakken)



# DILEMMA

Ali er ansatt i kommunen. Han har ansvar for utbetaling av økonomisk støtte til brukere med ulik grad av uførhet. En av brukerne han er ansvarlig for, deltar på flere aktiviteter på et aktivitetssenter i regi av organisasjonen Hvite Due.

En dag får Ali en telefon fra Kari, som er daglig leder på aktivitetssenteret. Hun har flere spørsmål om brukerens situasjon, blant annet helsetilstanden. Kari skulle gjerne ha fått tilsendt opplysningene på e-post, slik at hun kan vurdere om brukeren kan delta på de ulike aktivitetene Hvite Due tilbyr.

Brukeren har tidligere samtykket til at Hvite Due kan få denne informasjonen. Ali har allikevel ikke lyst til å sende dette på e-post. Kari mener at deler av informasjonen må kunne sendes på e-post. Eventuelt kan han sende alt hvis han bare ikke oppgir navnet på brukeren. Ali er usikker.

Hvordan kan han egentlig bruke e-post i sin arbeidshverdag og samtidig ivareta informasjonssikkerheten?

A



# DILEMMA

Ali er ansatt i kommunen. Han er ansvarlig for utbetaling av økonomisk støtte til vanskeligstilte.

En dag får han en telefon fra en av brukerne sine. Hun vil gjerne sende ham en e-post med dokumentasjonen han har bedt om. Det er snakk om opplysninger om helse, økonomiske forhold og familieforhold.

Ali er i tvil. Dette er tross alt brukerens opplysninger — men hvordan kan han vite at det kommer fra riktig person? Kan han motta all dokumentasjonen på e-post? Er det forskjell på de ulike typene opplysninger? Hvordan kan han bruke e-post i sin arbeidshverdag og samtidig ivareta informasjonssikkerheten?

**B**





# DILEMMA

Trine jobber i administrasjonen i Storskolen, en barne- og ungdomsskole med 1500 elever.

En dag ringer Amanda. Hun ønsker å få informasjon om hvorvidt elevpermisjonen til Andy i andre klasse er innvilget. Det er ikke lenge til permisjonen skal starte, og Amanda sier hun har behov for informasjonen for å bestille flybilletter. Hun høres veldig overbevisende ut, og sier at siden det er få plasser igjen på flyet må hun ha informasjonen så fort som mulig.

Trine ser i systemet sitt at navnet innringeren oppgir stemmer med det som er registrert som barnets mor i skolens systemer. Det er imidlertid faren som har søkt om permisjon. Ifølge informasjonen i skolens systemer bor foreldrene på ulike adresser.

Trine blir usikker på om hun kan svare på dette per telefon. Kan hun være sikker på at det er riktig person som ringer? Og er det egentlig så farlig om feil person får denne informasjonen?

C



# DILEMMA

I plan- og bygningsavdelingen i Lillevik kommune har de ikke fokus på formelle prosedyrer og øvelser. De har en beredskapsplan med prosedyrer for å håndtere hendelser, men det er flere år siden denne ble oppdatert.

De har heller aldri øvd på hva de skal gjøre når informasjonssikkerhets-hendelser inntreffer. Det har de siste årene vært noen mindre hendelser. Disse har blitt håndtert av de som var på jobb, uten å kalle inn ekstra hjelp, og uten å forholde seg til beredskapsplanen.

Kommunens ledelse har besluttet at alle enheter skal utforme beredskapsplaner med prosedyrer for håndtering av informasjonssikkerhetshendelser. Dette gjelder både hendelige uhell og planlagt sabotasje. De skal øve på hvordan de håndterer slike hendelser, og planene skal også oppdateres jevnlig.

Ledelsen og de ansatte i plan- og bygningsavdelingen forstår ikke hvorfor det er viktig å øve på sikkerhetshendelser, og holde beredskapsplanen oppdatert. De har veldig få hendelser i løpet av et år, og dagens ansatte har ikke opplevd store hendelser. De mindre hendelsene de har opplevd har de greid å håndtere uten beredskapsplan og skriftlige prosedyrer.

## D

Hvorfor er det nødvendig å gjennomføre øvelser?



# DILEMMA

Festivaldirektoratet bevilger pengestøtte til festivaler. Nylig var det et tilfelle av feil overføring av midler. Det viste seg at en ansatt hadde fått tilgang til systemet for festivalmiddelfordeling, til tross for at han ikke hadde behov for det. Dette lot seg gjøre fordi virksomheten ikke hadde kontroll på hvem som skulle ha tilgang til systemet.

Etter dette innførte direktoratet strenge regler for godkjenning av tilganger. Ingen får tilgang til festivalmiddelfordelingssystemet uten godkjenning fra både linjeleder og systemeier. I tillegg har de innført bruk av personlige kodebrikker i kombinasjon med passord for å logge inn.

Det er sommerferie, og få ansatte på jobb. Etter et par uker i jobb får ferievikaren Frida i oppdrag å overføre midler til to festivaler. Hun ber om å få tilgang til systemet for å overføre midlene, men får beskjed av sin leder at det ikke er nødvendig. Den som har hovedansvaret for bevilgningene lar kodebrikken sin og en lapp med passordet ligge igjen på jobben når han tar ferie. Det tar så lang tid å få godkjent og ordnet slik tilgang, så de har funnet ut at dette er enklere. Dermed kan Frida bruke hans kodebrikke og passord. Frida synes det er rart å omgå reglene på denne måten. Samtidig er det tungvint å følge dem.

Hvordan kan reglene utformes for å ivareta informasjonssikkerheten best mulig, samtidig som de ansatte får gjort jobben sin på en effektiv og god måte?

E



# DILEMMA

Elisabeths jobb i Målstyringsdirektoratet krever ofte at hun kan gi raske tilbakemeldinger på faglige spørsmål.

Det kommer e-poster utenom vanlig arbeidstid både fra sjefen og andre kolleger. Dette er ikke et stort problem for Elisabeth siden hun bruker sin private telefon til å svare på e-post. Hun har også et nettbrett som hun ofte bruker til å notere ned jobbrelevante ting hun kommer på utenfor arbeidstid.

Per kjøper en brukt mobiltelefon. Han oppdager at det ligger interne notater fra HR-avdelingen i Målstyringsdirektoratet lagret på telefonen. Per ser sitt snitt til å tjene noen raske kroner og ringer avisen Dagens Gang, som neste dag har første-sideoppslaget «Målstyringsdirektoratet bryr seg ikke om sine ansattes personvern».

Direktoratet innfører umiddelbart retningslinjer for bruk av privat utstyr i jobbsammenheng. De ansatte får beskjed om at det ikke er lov å bruke egne data-maskiner, telefoner eller nettbrett i jobbsammenheng. Retningslinjene sier også at det ikke er tillatt å bruke jobbutstyr til private formål.

Elisabeth leser nyheten på intranett og klør seg i hodet. Hun forstår at det ikke er bra at interne dokumenter kommer på avveie på denne måten. Samtidig tenker hun at de nye retningslinjene vil gjøre arbeidshverdagen hennes mer tungvint. Men det må kanskje til for å sikre at ikke slike ting skjer igjen?

Hva kan Målstyringsdirektoratet gjøre for å ivareta informasjonssikkerheten, samtidig som de ansatte ikke opplever at det blir vanskelig å få gjort jobben sin?

F



# DILEMMA

Ole har akkurat begynt i ny jobb i arkivet i Bygningstilsynet. Han har blant annet ansvar for at papirdokumenter digitaliseres.

Etter en bombetrussel har det blitt besluttet at alle ansatte må bruke adgangskort med kode for å komme inn i bygningen. I tillegg må man bruke kortet og tilhørende kode for å komme inn i hver enkelt etasje og avdeling.

Papirarkivet har blitt vurdert til å være en egen sikkerhetssone i bygget. Dette innebærer at Ole må bruke kort og kode enda en gang for å komme inn i papirarkivet. Inne i arkivet er det et eget rom der den konfidensielle informasjonen oppbevares. For å komme inn i denne delen må han igjen trekke kort og taste kode. Totalt må han altså trekke kort og taste kode fem ganger for å komme inn dit. Adgangskontrollen virker på samme måte både i og utenfor arbeidstiden.

Ole oppdager raskt at det er fast praksis blant de ansatte i arkivet å la dørene i papirarkivet stå på gløtt. Da han nevner dette for en av kollegaene, får han beskjed om at de er så lei av å måtte trekke kort og taste kode hele tiden. De må inn i arkivet flere ganger i løpet av dagen, så de synes det tar for lang tid å trekke kort og taste kode hver gang. Ole synes kravene er strenge, men at det er rart at dørene står åpne.

G

Kan Bygningstilsynet utforme adgangskontrollen sin annerledes for å ivareta informasjonssikkerheten og de ansattes hverdag på en bedre måte?



# DILEMMA

Ole har akkurat begynt i ny jobb i Bygningstilsynet. De deler et stort bygg i sentrum av Lillevik med to private virksomheter. Tilsynet holder til i tre etasjer i bygget.

Allerede den første dagen i ny jobb reagerer Ole på at det er lite kontroll på hvem som kommer inn i bygget. Det er ikke betjent resepsjon, og alle kan gå rett inn hoveddøren mellom klokken 8.00 og 16.00. Det er i samme periode heller ikke nødvendig å bruke kort, taste kode eller lignende for å komme inn i de enkelte etasjene. Mellom klokken 16.00 og 08.00 må man bruke adgangskortet sitt for å komme inn i bygget.

I sitt arbeid behandler Ole personopplysninger og bedriftshemmeligheter både elektronisk og på papir. Dette er opplysninger om tilsynets egne ansatte (personalinformasjon) og informasjon fra tilsynsvirksomheten. Han synes derfor det er rart at hvem som helst i teorien kan komme inn på kontoret hans i arbeidstiden. Han tar opp spørsmålet med sin leder, som aldri har tenkt over manglende adgangskontroll. Han synes det er ganske praktisk at det er enkelt å komme seg inn i bygget og mellom de ulike avdelingene.

Blir informasjonssikkerheten godt nok ivaretatt med dagens adgangskontroll?

H



# DILEMMA

Jim jobber i innenriksdepartementet. Han er veldig fornøyd med å få jobbe med deres nye satsningsområde, automatisert saksbehandling, de neste to årene. Han har fått beskjed om å bytte kontor plass fordi alle som jobber i prosjektet skal sitte samlet i et åpent landskap i øverste etasje.

Samtidig som de flytter inn i landskapet får de utdelt nye PC-er. På disse er det et klistremerke med budskapet «Lås PC-en når du går fra den!». Jim husker at informasjonssikkerhetsansvarlig snakket om dette på nyansattkurset han deltok på for lenge siden, men har egentlig aldri forstått hvorfor han skal låse PC-en sin. Alle i landskapet jobber på det samme prosjektet.

Hvorfor skal de egentlig låse PC-en sin?