

Forum for informasjonssikkerhet og personvern

0900 – 0905	Velkommen til forum Informasjon om dagens program
0905 – 0920	Informasjon om KINS og medlemsfordeler Daglig leder i KINS Harald Torbjørnsen
0920 – 0935	Presentasjon av de nye ansatte fagsjefene i seksjon for informasjonssikkerhet og IKT
	Informasjonssikkerhet: Åsmund Skomedal
	Personvern: Maryke Silalahi Nuth
	IKT: Geir Faremo
0935 – 1000	Informasjon om planer for årets Sikkerhetsmåned Wenche Hagan
1000 – 1010	Pause
1010 – 1050	Avvikshåndtering Tommy Nysveen og Linda Mari Knutsen gir deg en innføring hva et avvik er (innenfor områdene personvern og informasjonssikkerhet), hvordan vurdere når et avvik skal meldes og hvilke rutiner må virksomheten ha.
1050 – 1100	Avslutning og eventuelle spørsmål



Aktiviteter og fordeler

Oslo 8. september 2020

Hva er KiNS?

Foreningen kommunal informasjonssikkerhet

- ▶ Medlemsorganisasjon
- ▶ Startet i 2003
- ▶ Status 2020
 - 294 kommuner og fylkeskommuner
 - 49 bedriftsmedlemmer
- ▶ Daglig leder fra 1.mars 2019
- ▶ Hovedmålgruppe
 - Ansatte i kommuner, fylkeskommuner og kommunale foretak
- ▶ Aktiviteter møteplasser og verktøy
 - Kurs, e-læring, konferanser, seminarer, webinarer
 - Verktøykasse med maler, veiledninger og ressurser.



Hva er KiNS?

Foreningen kommunal informasjonssikkerhet

Våre partnere

Digitaliseringsdirektoratet
Norwegian Digitalisation Agency



Oslo

Strategi 2020 -2023 - prioriteringer



Norm/ code of conduct i grunnopplæringen



Kommunalt samarbeid om kompetanse og forvaltning for
LSIS/ISMS



E-læringskurs

Kompetanseprogram for personvern
og informasjonssikkerhet

Hva skjer?



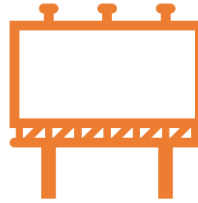
Konferanser

Nord-Norge konferansen

13. Oktober (digital)

Kins-tech

16.-17. November



Kurs

Fysiske og digitale ut over
høsten 2020



Arrangementer

Webinarer for
erfaringsutveksling mellom
kommunale medlemmer

Webinarer for å synliggjøre
våre bedriftsmedlemmer



Oslo

Høstens aktiviteter

ARRANGEMENTER I OKTOBER

KURS 09 OKTOBER	Grunnkurs i informasjonssikkerhet og personvern - nr 2 (- NETTBASERT)	
13 OKTOBER	KiNS Nord Norge konferansen 2020 (- NETTBASERT)	
23 OKTOBER	Sammen om en sikker digital offentlig sektor – dag 1	
29 OKTOBER	Sammen om en sikker digital offentlig sektor – dag 2	
KURS 29 OKTOBER	Sikkerhetshendelser og håndtering av digitale bevis (- NETTBASERT)	

ARRANGEMENTER I NOVEMBER

16 NOVEMBER	KiNS tech 2020 (- NETTBASERT)	
KURS 26 NOVEMBER	Sikkerhet i trådløse nettverk	

ARRANGEMENTER I DESEMBER

KURS 03 DESEMBER	Grunnkurs i informasjonssikkerhet og personvern - nr 3 (- NETTBASERT)	
KURS 04 DESEMBER	Introduksjon styringssystemer for informasjonssikkerhet og personvern – (- NETTBASERT)	



Oslo

Hva kan KiNS tilby i dag?

- Kurs og konferanser til medlemspris
- Kompetansepakker for ansatte (KS Læring)
- Verktøykasse
- Samarbeid om kursbehov, seminarer ol
- Bredt nettverk – kommunalt og i bransjen



Takk for oppmerksomheten

Harald Torbjørnsen
harald@kins.no



Oslo



Sikkerhetsmåned 2020

Nettverkssamling 8.09.2020
Wenche Hagan



Sikkerhetsmåned 2020

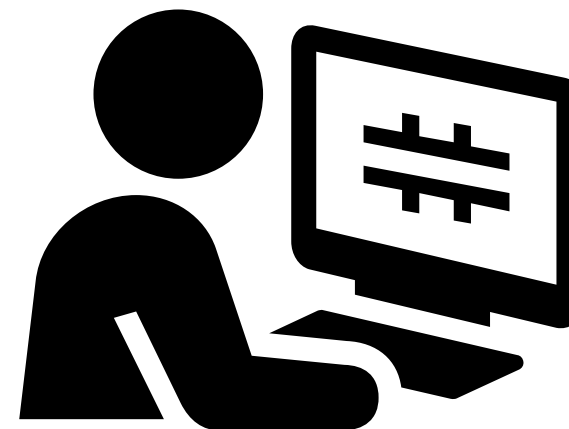
- ▶ Legger kun opp til digital deltakelse under årets sikkerhetsmåned

Innhold:

- E-læringer
- Digitale arrangementer
- Seminar og foredrag
- Materiell/verktøy
- Bruk av Workplace
- Historien om Tim – en sikker digital hverdag
- Kort forklart
- Månedspan – hva skjer når

E-læringer/nanolæringer

- Sendes på epost til alle ansatte
- 5 e-læringer á 2-5 minutter ukentlig i oktober.
 - Aktuelle temaer:
 1. Velkommen til sikkerhetsmåned (sendes 22. september)
 2. 5 enkle tips som hjelper deg å avsløre en svindel
 3. Personvernmyter
 4. Beskytt de viktigste brukerkontoene dine
 5. «Hurra, det er gratis Wi-Fi her!»
- Målet er å fortsette med e-læringer en gang i måneden etter oktober



Digitale arrangementer

Alle seminarer streames til Workplace

▶ **Åpning av Sikkerhetsmåned**

Tema:

- Informasjonssikkerhet og personvern i et fremtidsperspektiv
- Lansering av Tim-film:
Historien om Tim – en sikker digital hverdag

▶ **Samarbeid med Oslo Origo om to Tim-talks**

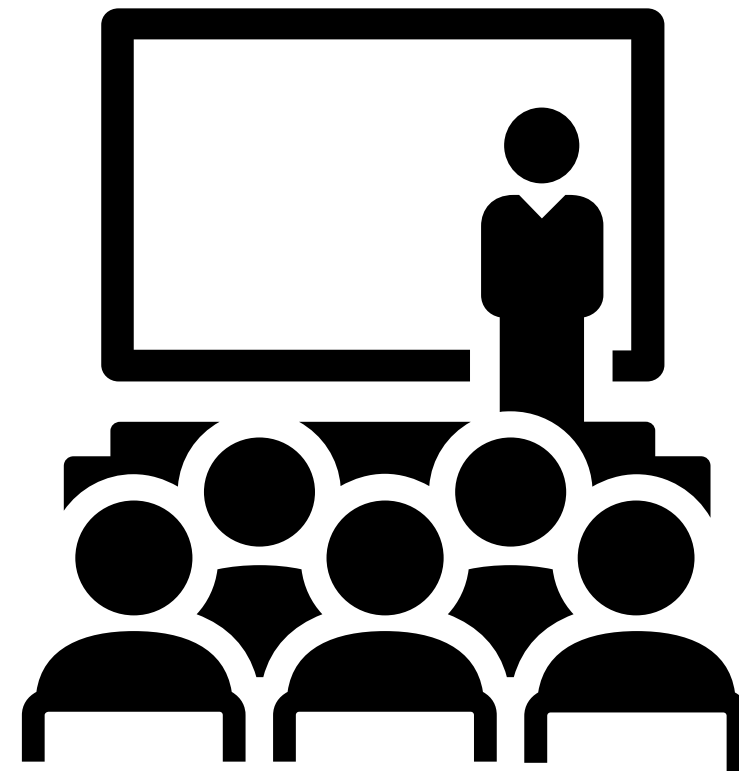
Tema:

- Hvor proaktive *kan* og *vil* vi være
- Sikkerhet fra start – en ansvarsreise

▶ **Avslutning av Sikkerhetsmåned**

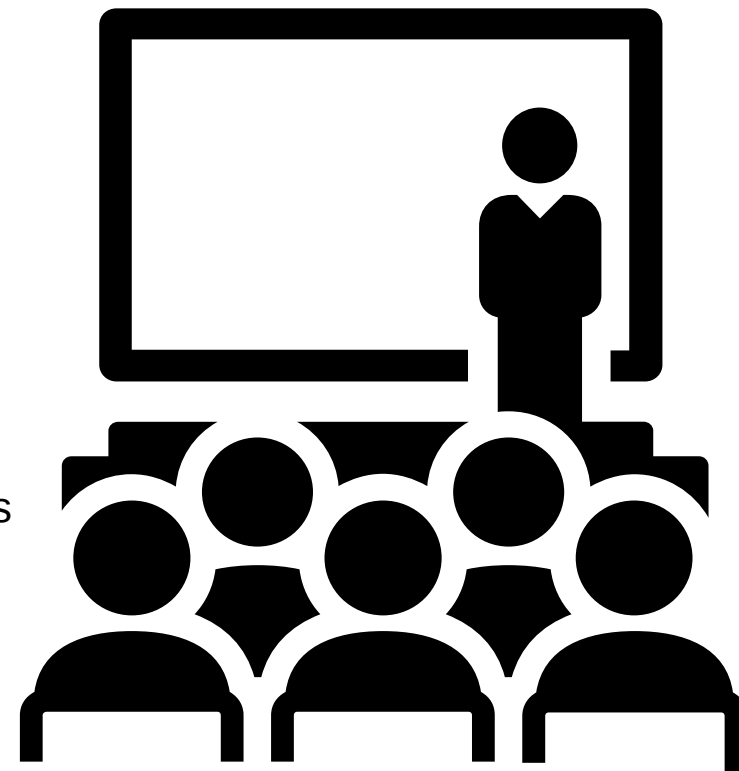
Tema:

- Organisasjon, kultur og den menneskelige faktor



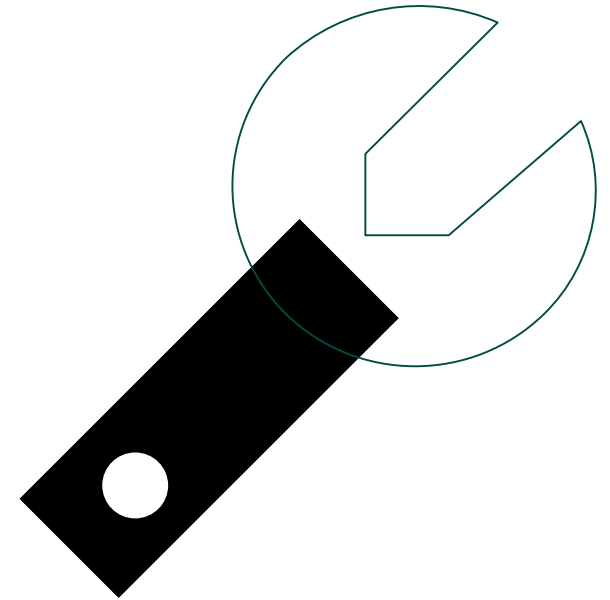
Seminar og foredrag på Teams

- ▶ Lederforedrag som virksomhetene kan bestille fra oss
 - Fortrinnsvis avholdes på Teams
 - Tema og innhold ikke avklart, men mulige aktuelle temaer:
 - Hvorfor drive kompetansebygging i informasjonssikkerhet og personvern hos dine ansatte og i din virksomhet
 - Hvordan beslutte risiko på informasjonssikkerhet og personvern - et praktisk foredrag for deg som leder.
- ▶ Innføring i personvern (med åpen påmelding)
 - Målgruppe alle ansatte.
- ▶ Innføring i informasjonssikkerhet (med åpen påmelding)
 - Målgruppe alle ansatte



Materiell/ verktøy til virksomhetene

- ▶ Virksomhetene kan bestille materielle som vi allerede har på lager (plakater, sikkerhetstips, bordkort etc.)
- ▶ Endre alle låseskjermer på Oslo felles i oktober



Workplace

- ▶ Bruke fellesgruppene **Oslo/alle** i Oslo kommune og **Oslo/Nyheter** i Oslo kommune
- ▶ Bruke våre egne grupper Oslo/personvern og Oslo/informasjonsikkerhet og IKT
- ▶ Innhold
 - Tim-film
 - *Kort forklart*
 - Videoer fra politiskledelse
 - Konkurranser med premie



Historien om Tim – en sikker digital hverdag

▶ Hva:

- En film med utgangspunkt ulike case/problemstillinger (4-5 minutter)
- Bygger på de eksisterende Tim-filmene og belyser informasjonssikkerhet og personvernsaspekter i ulike digitale fremtidsvisjoner

▶ Bakgrunn:

- Ønsker å bruke en etablert «karakter» (Tim) til å underbygge vårt budskap
- Historiefortelling er et godt virkemiddel for å levendegjøre og nå frem med budskap
- Tim skal vise til målbilder for digitalisering og vil gi en positiv vinkling på vårt budskap

▶ Når:

- Lanseres på åpningsseminaret av Sikkerhetsmåneden 7. oktober

▶ Kompetansehevende tiltak:

- Utvikle materiell utover filmen (små filmsnutter med refleksjoner, skjem bakgrunner) som kan brukes utover Sikkerhetsmåneden



Kort forklart

▶ Hva:

- Korte små videoer på 40 sekunder til 2 ½ minutt med forklaringer av ord og aktuelle temaer innen våre fagområder (informasjonssikkerhet, personvern og IKT)
- Et lett gjenkjennelig konsept med lik oppbygging av hver film
- Videoene har alle ansatte som målgruppe og det er viktig at «kort forklart» formidler til den enkelte ansatte

▶ Mål:

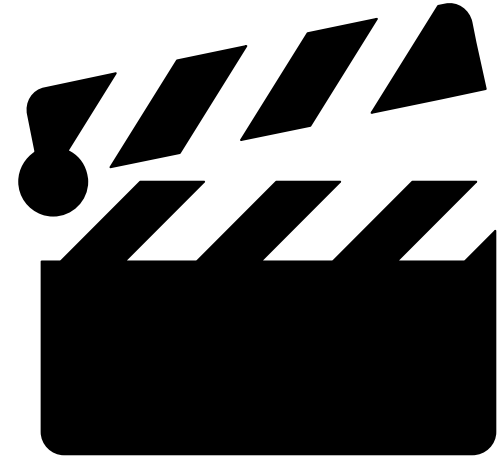
- å formidle budskapene våre kort og smart (tenk gjerne filmer på sosiale medier og reklamefilm)
- å inspirere til læring og nysgjerrighet - ikke belæring og pekefinger

▶ Når:

- Konseptet lanseres for første gang på Sikkerhetsmåneden

▶ Kompetansehevende tiltak:

- Målet er at disse skal være lette å lage og leve utenom Sikkerhetsmåneden



Foreløpig plan for aktiviteter i Sikkerhetsmåned

Mandag

Tirsdag

Onsdag

Torsdag

Fredag

41	5	07:00 08:00 Låseskjerm 08:00 08:30 Åpningsvideo Oslo/alle eller Oslo/Nyheter	6	08:00 08:30 E-læring Sikkerhetsmåned 08:00 08:30 Kort forklart	7	08:00 08:30 Tim-film på Oslo/alle eller Oslo/nyheter 09:00 11:00 Åpning av Sikkerhetsmåned?	8	08:00 08:30 Påminnelser om e-læring + lenke til e-læring 09:00 11:00 Innføring i grunnleggende personvern; Te	9	08:00 08:30 Kort forklart
	12	07:00 08:00 Låseskjerm 08:00 08:30 Kort forklart	13	08:00 08:30 E-læring Sikkerhetsmåned 08:00 08:30 Konkurrans	14	09:00 10:00 Sikkerhetsmåned - Tim talk	15	08:00 08:30 Påminnelser om e-læring + lenke til e-læring	16	08:00 08:30 Trekke vinner konkurranse
42	19	07:00 08:00 Låseskjerm 08:00 08:30 Kort forklart	20	08:00 08:30 E-læring Sikkerhetsmåned 08:00 08:30 Konkurrans	21	09:00 10:00 Sikkerhetsmåned - Tim talk	22	08:00 08:30 Påminnelser om e-læring + lenke til e-læring 09:00 11:00 Innføring i grunnleggende informasjonssil	23	08:00 08:30 Trekke vinner konkurranse
	26	07:00 08:00 Låseskjerm 08:00 08:30 Kort forklart	27	08:00 08:30 E-læring Sikkerhetsmåned	28	09:00 11:00 Avslutning Sikkerhetsmåned	29	08:00 08:30 Påminnelser om e-læring + lenke til e-læring	30	08:00 08:30 Avslutningsvideo Oslo/alle eller Oslo/Nyhe
44										



Oslo



Overordnet styringssystem for personvern og informasjonssikkerhet

Hendelseshåndtering

08.09.2020

Tommy Nysveen



Hensikten med dagens presentasjon

- ▶ Informere kort om overordnede styringssystemet for personvern og informasjonssikkerhet i Oslo kommune
- ▶ Informere om overordnede krav for risikoområdet hendelseshåndtering
 - (Ikke publisert dd.)
- ▶ Linda informerer videre om veileder for avvikshåndtering og melding til datatilsynet

Bidra til enklere operasjonalisering av krav i styrende dokumenter

- ▶ Virksomhetene og sentrale fagressurser uttrykker at det er stor avstand mellom føringer og krav i kommunens styrende dokumenter og operasjonaliseringen den enkelt virksomhet må gjøre for å få internkontrollen på plass
- ▶ Tydeliggjøring av føringene vil bidra til enklere operasjonalisering av informasjonssikkerhet i virksomhetene
- ▶ Bidra til bedre forutsigbarhet for virksomhetsledere og fagpersoner
- ▶ Bidra til at sentrale risikoområder ivaretas i alle sektorer

Rammebetingelser for arbeidet

- ▶ Styrende dokumentene for informasjonssikkerhet
- ▶ Lover og regler
- ▶ Prinsippet om tillitsbasert ledelse
- ▶ Tett involvering av byrådsavdelingene og virksomhetene

Informasjonssikkerhet

Det er vedtatt flere styrende dokumenter for informasjonssikkerhet i Oslo kommune. Disse gjelder for alle virksomhetene. Dokumentene angir rollefordeling i kommunen, ansvar for ulike roller, krav til sikkerhetsarbeidet i kommunen, omtale av hendelseshåndtering mv.

IKT-reglement for Oslo kommune

IKT-reglement for Oslo kommune (byrådssak 1099/10)

Instruks for informasjonssikkerhet



Instruks for informasjonssikkerhet for Oslo kommune (byrådssak 1105/13)

Instruks for virksomhetsstyring

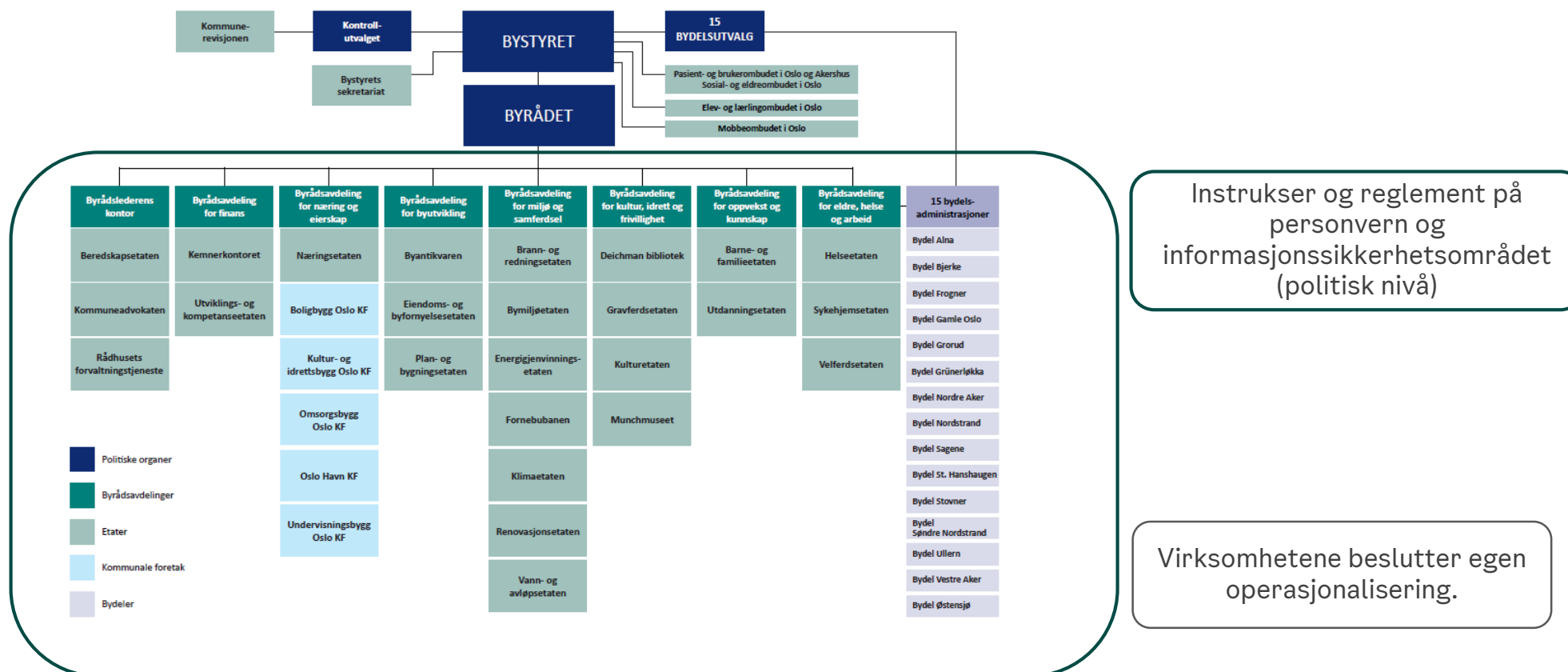
Instruks for virksomhetsstyring i Oslo kommune (byrådssak 1070/15, endret i sak 1107/16, sist i sak 1104/17)

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

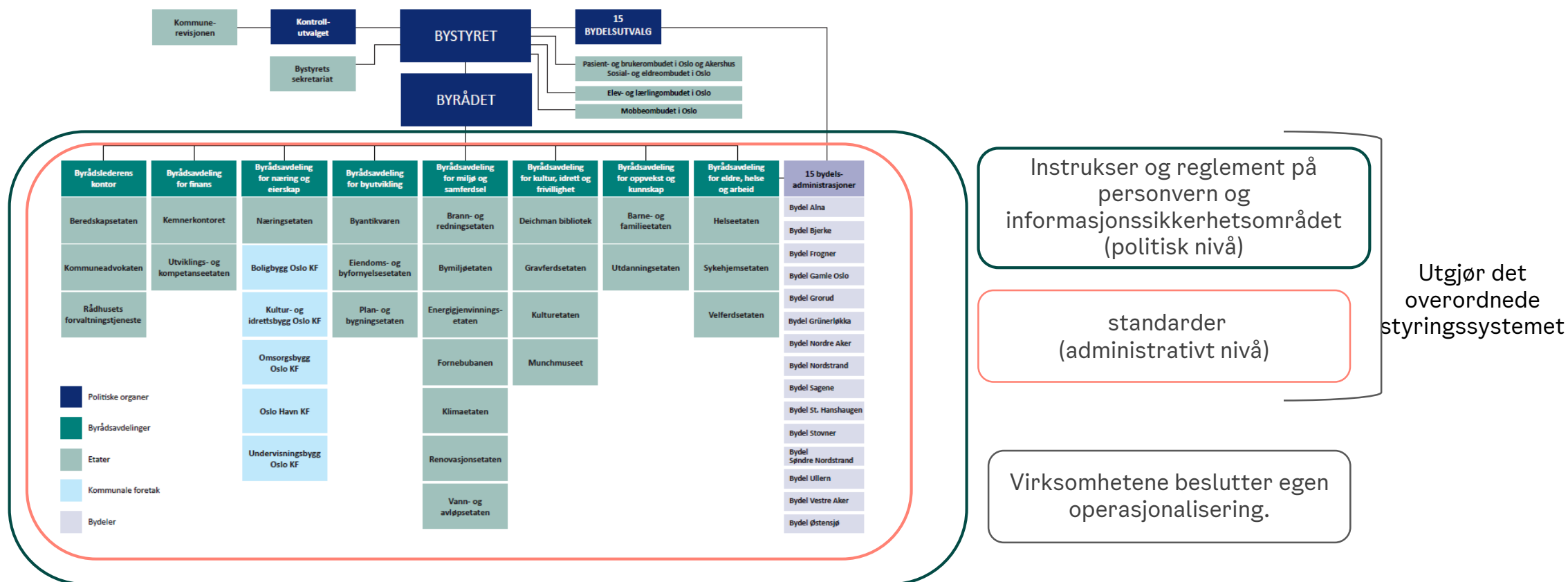
Dato	FOR-2004-06-25-988
Departement	Kommunal- og moderniseringsdepartementet
Publisert	I 2004 hefte 10
Ikrafttredelse	01.07.2004
Sist endret	FOR-2014-02-07-102 fra 01.07.2014
Gjelder for	Norge
Hjemmel	LOV-1967-02-10-§15a, LOV-2001-06-15-81-§5, LOV-1992-12-04-126-§12, jf LOV-2018-06-15-44-§10
Kunngjort	29.06.2004
Rettet	05.08.2014 (§ 3 annet ledd)
Korttittel	eForvaltningsforskriften



Det overordnede styringssystemet for personvern og informasjonssikkerhet omfatter hele kommunen



Det overordnede styringssystemet for personvern og informasjonssikkerhet omfatter hele kommunen



Et dokument som dekker alle risikoområdene

- Formål
- Omfang
- Målgruppe
- Ansvar
- Krav til [gjeldende risikoområde]
- Krav til internkontroll
 - Kobler dokumentet opp mot Ledelsens gjennomgang og Virksomhetsleders egenerklæring

Overordnet styringssystem for personvern og informasjonssikkerhet

Oslo kommune

1	Krav til håndtering av hendelser innen informasjonssikkerhet og personvern.....	2
2	Krav til informasjonssikkerhet i leverandørforhold	5
3	Krav til informasjonssikkerhet og personvern i prosjekter	9
4	Krav til forvaltning av aktiva	12
5	Krav til kontinuitetsplanlegging.....	12
6	Krav til tilgangsstyring.....	12
7	Krav til drift og utvikling.....	12
8	Krav til personellsikkerhet.....	12
9	Krav til fysisk sikkerhet og miljø	12
10	Krav til etterlevelse	12
11	Krav til organisering.....	12

Oslo Kommune sitt overordnede styringssystem for informasjonssikkerhet har tre sentrale styringsdokumenter innen informasjonssikkerhet:

- Instruks for virksomhetsstyring i Oslo kommune (IN-0089)
- Instruks for informasjonssikkerhet for Oslo kommune (IN-0077)
- IKT-reglement for Oslo kommune (RE-0018)

Fra Instruks for virksomhetsstyring i Oslo kommune kap. 4 fremkommer følgende:

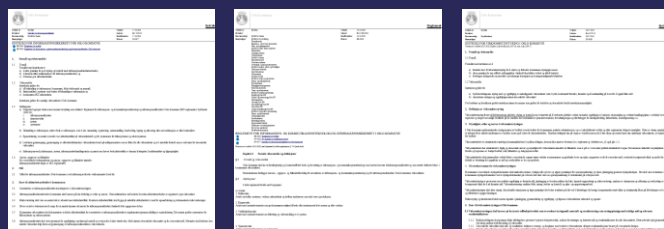
Kommunens overordnede styringsdokumenter skal inneholde rammer, tydelige mål og krav og utgjøre grunnlaget for operasjonisering og videre planlegging gjennom styringsdialogen. Det skal være konsistens i kommunens styringsdokumenter ved at styringsdokumenter på et lavere nivå skal være en operasjonisering av dokumenter på et høyere nivå.

Foreliggende dokument beskriver krav til de forskjellige risikoområder innenfor informasjonssikkerhet som er definert av Oslo kommune og skal bidra til operasjonisering av kommunens styringsdokumenter, herunder instruks for informasjonssikkerhet.

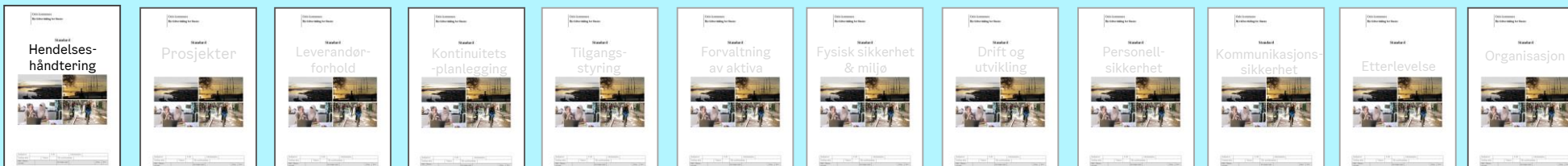
Risikoområder som dekkes i et styringssystem for personvern og informasjonssikkerhet

Nivå 1

Retningslinjer og instruksjer



Nivå 2



Eksempel – tydeliggjøring av krav til hendelseshåndtering

Instruks for informasjonssikkerhet for Oslo kommune

5.6 Hendelseshåndtering

- a) Varsling og håndtering av hendelser (avvik, feilsituasjoner eller fare for slike) skal skje så nær hendelsen som mulig, og i henhold til dokumenterte rutiner for varsling og håndtering.
- b) Det skal være enhetlige rutiner for etterfølgende rapportering av hendelser.
- c) Rutiner for varsling og håndtering av hendelser knyttet til forvaltning eller drift av systemer må foreligge fra systemeier for så vidt gjelder fellessystemer, sektorsystemer og tverrsektorielle systemer.

Instrukser og reglement på informasjonssikkerhetsområdet
(politisk nivå)

Informasjonssikkerhets-
standards
(administrativt nivå)

Utdypes mer gjennom følgende temaer innenfor hendelseshåndtering (med noen eksempler):

Hva kreves innenfor:

- Opplæring
- Varsling
- Håndtering
- Rapportering
- Evaluering
- Læring
- Internkontroll

Virksomhetene beslutter egen operasjonalisering

- ▶ Hvordan virksomhetene operasjonaliserer kravene i form av egne prosedyrer, veiledere osv. er avhengig av bl.a:
 - egen risikoprofil
 - størrelse
 - egenart
 - kompetanse
 - osv...
- ▶ Noen områder kan det også være fornuftig å bidra mer konkret sentralt til operasjonalisering
 - Veileder for avvikshåndtering og melding til datatilsynet



Veileder for avvikshåndtering og melding til Datatilsynet

Forum for personvern og
informasjonssikkerhet
08.09.2020

Linda Mari Knutsen



Foto: Thomas Ekström

Formål og målgruppe til veilederen

- ▶ **Formål:** bidra til en lik håndtering av brudd på personopplysningssikkerheten for kommunens virksomheter, herunder etablere gode prosesser og vurderinger ved håndtering av denne typen avvik, lukke disse, etablere tiltak og vurdere hvorvidt disse skal meldes til Datatilsynet, samt informere den berørte registrerte
- ▶ **Målgruppen:** alle ansatte som behandler personopplysninger i sin virksomhet.
- ▶ Veilederen vil særlig være relevant for virksomhetens ledelse, personvern- og informasjonssikkerhetskoordinatorer, IKT-ansvarlig, databehandlere, prosjektledere, informasjonssikkerhetsledere og personvernombud.



Hva er et avvik etter
GDPR?



Hvordan vurdere risiko
for de registrertes
rettigheter og friheter?



Meldeplikt til
Datatilsynet og
informasjon til de
registrerte



Virksomhetens plikter

Hva er et avvik etter personvernforordningen (GDPR)

- ▶ «Brudd på personopplysningssikkerheten:

et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet»



Hvordan vurdere risiko for de registrertes rettigheter og friheter

- ▶ Hva betyr dette?
- ▶ Det omfatter en vurdering av den enkelte registrertes **personopplysningsvern og personvern**, og også **andre grunnleggende rettigheter** som
 - retten til ytringsfrihet, tankefrihet, samvittighet, religionsfrihet, bevegelsesfrihet, og
 - forbud mot diskriminering etter den Europeiske menneskerettighetskonvensjonen.

Kriterier ved vurdering av risiko

- ▶ Vurdering av de konkrete omstendighetene rundt avviket
- ▶ Kriteriene må vurderes mot hverandre og husk at dette skal være skriftlig!
- ▶ Kriterier:
 - Type brudd
 - Type personopplysninger
 - Antall berørte enkeltpersoner
 - Enkelt å identifisere enkeltpersoner?
 - Alvorlighetsgrad av konsekvenser for enkeltpersoner
 - Spesielle egenskaper ved enkeltpersoner
 - Også kode 6 eller 7
 - Spesielle egenskaper ved behandlingsansvarlig (maktforhold og skjevheter)



Nærmere om høy risiko ved avvik

- ▶ Høy risiko innebærer en vurdering av om konsekvensen og sannsynligheten av avviket er høy for den enkelte registrertes rettigheter og friheter.
- ▶ Eksempler på høy risiko :
 - Diskriminering eller forskjellsbehandling av den registrerte, for eksempel ved vedtak om ytelser eller liknende.
 - Feilsendte personopplysninger som oppleves som sensitiv/er sensitiv for den registrerte (fødselsnummer, helseopplysninger, fortrolig informasjon, økonomiske opplysninger etc).
 - Bedrageri eller svindel, ID-tyveri
 - Økonomisk tap for den registrerte
 - Tap av omdømme eller sosiale konsekvenser for den enkelte registrerte
 - Forringelse av andre tjenester den registrerte har rett til.
 - Tap av liv eller helse

Hva skjer videre når risikoen er vurdert?

- ▶ Ingen eller lav risiko for den registrerte, ikke behov for å melde fra til Datatilsynet eller varsle den registrerte.
- ▶ Middels risiko for den registrerte, skal virksomheten melde fra til Datatilsynet.
- ▶ Høy risiko for den registrerte, skal virksomheten sende melding til Datatilsynet og varsle den berørte registrerte.
- ▶ Personvernombudet i Oslo kommune skal informeres om avvik i virksomheten, også de som ikke meldes til Datatilsynet.

Melding til Datatilsynet og informasjon til de registrerte

- ▶ Avvik skal meldes til Datatilsynet så raskt som mulig («uten ugrunnet opphold») og senest 72 timer etter at man har en rimelig grad av visshet om at det kan ha skjedd et brudd på sikkerheten som har ført til at personopplysninger er på avveie eller tilgjengelig for uvedkommende mv.
 - Skjema via Altinn
 - Viktig at også journalføres i arkivsystemet
 - Krav til innhold i meldingen – se www.datatilsynet.no
- ▶ Foreligger høy risiko er det en plikt å informere de berørte registrerte
 - Minimumskrav til innhold
 - Ulike kanaler kan benyttes

Virksomhetens plikter

- ▶ Etablere gode avviksrutiner
 - Plassering av ansvar, tildeling av roller i for eksempel Altinn
 - Dokumentere årsak, korrigerende tiltak og rapportering
 - Tilrettelegge for nødvendig verktøy/digitale løsninger
 - Opplæring og praktisering av «lav terskel»



Hvorfor er det viktig å melde avvik?

- ▶ Hindre misbruk eller skade!
- ▶ Tillit og omdømme!
- ▶ 72 timers frist!
- ▶ Bidrar til å forbedre virksomheten (vi lærer av feil!)
- ▶ Det er positivt å si ifra om avvik



Spørsmål?

Du finner veilederen på Intranett -> informasjonssikkerhet og personvern

