Oslo

# Informasjons-sikkerhet og personvernforum

26.05.2020

# Program

- 09:00 Velkommen.
  En rask introduksjon om programmet og hvordan man tegner seg/stiller spørsmål.
- 09:10 Status etter rapportering på ledelsens gjennomgang (LG) og virksomhetsleders egenerklæring (VE) for 2019 ved Jeanne Hammer Espedalen , seksjon for informasjonssikkerhet og IKT, Byrådsavdeling for finans
- 09:55 Arbeid med overordnet styringssystem informasjonssikkerhet ved Tommy Nysveen, seksjon for informasjonssikkerhet og IKT, Byrådsavdeling for finans
- 10:20 Informasjon om brev til virksomhetene om fellesføringene og oppnevning av personvern- og informasjonssikkerhetskooridnatorer ved Atle Halvorsen Hjelkerud, seksjon for informasjonssikkerhet og IKT, Byrådsavdeling for finans
- 10:30 Personvernombudets årsrapport ved Morten Haug Frøyen, Personvernombudet i Oslo Kommune
- 10:55 Avslutning og introduksjon av programgruppa til personvern- og informasjonssikkerhetsforum.

Oslo

# Status for arbeid med informasjonssikkerhet og personvern 2019

Jeanne H. Espedalen

Forum for personvern og informasjonssikkerhet
26.05.2020

# Hva skal jeg presentere?

- Status for arbeid med informasjonssikkerhet og personvern
- Basert på
  - Oppsummeringer fra byrådsavdelingene på sektornivå
    - Basert på rapportering fra virksomhetene, LG/VE, og styringsdialog
  - Sammenstilling av data på kommunenivå, fra spørsmål i Virksomhetenes egenerklæring (nytt fra 2019)
  - Dialog som FIN/ISI har hatt med virksomheter og byrådsavdelinger
    - Opplæringsaktiviteter og kompetansetiltak
    - Workplace
  - Andre kilder
    - Kommunerevisjonen
    - Meldinger til Datatilsynet

  Vurderingene som er gjort er basert på faktagrunnlag, men i stor grad «synsing»

# Er «Virksomhetsleders egenerklæring» mottatt fra alle underliggende virksomheter?

| År | BLK | FIN | NOE | BYU | MOS | KIF | OVK | EHA |
|---|---|---|---|---|---|---|---|---|
| 2019 | 3 av 3 | 2 av 3 | 6 av 6 | 3 av 3 | 7* av 7 | 4** av 4 | 2 av 2 | 17 av 18 |
| 2018 | 3 av 3 | 2 av 2 | 6 av 6 | 3 av 3 | 7 av 7 | 4 av 4 | 2 av 2 | 18 av 18 |
| 2017 | 3 av 3 | 2 av 2 | 6 av 6 | 3 av 3 | 5 av 7 | 3 av 3 | 1 av 1 | Ja |
| 2016 | 3 av 3 | 2 av 2 | Ja | 2 av 3 | 5 av 5 | 3 av 3 | 1 av 1 | 12 av 19 |

*Behandlingen for en er virksomhetene er ikke sluttført
**Dokumentene er mottatt, men byrådsavdelingen mener at utfyllingen kan gjøres mer omfattende

# Anses status for som tilfredstillende?

| År | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 |
|---|---|---|---|---|---|---|---|---|
| 2019 | | | | | | | | |
| 2018 | | | | | | | | |
| 2017 | | | | | | | | |
| 2016 | | | | | | | | |

# Har virksomhetene et fungerende internkontrollsystem?

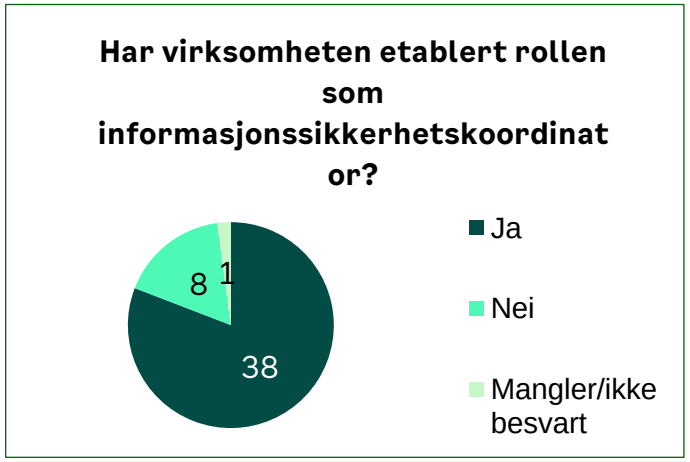
| År | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 |
|---|---|---|---|---|---|---|---|---|
| 2019 | Overordnet beskrivelse | Ja | Ja | Alle har forbedrings-potensiale | Ja | Ikke besvart? | 3(4?) av 7 har | Ja |
| 2018 | Ja, i hvert fall overordnet | Ja | Ja | Ja, men i varierende grad | Ja | Ja | 3 av 7 har | 1 ja<br>1 delvis |
| 2017 | Ja | Ja | Kjenner ikke detaljene | Er i prosess | 1 ja<br>2 delvis | Ja | 3 av 7 har | 1 ja<br>1 delvis |
| 2016 | Ja | Ikke besvart | Ja | Nei, noen delvis | 1 ja<br>2 under etablering | Ja | 2 ja<br>1 delvis<br>2 vet ikke | 1 ja<br>1 delvis |

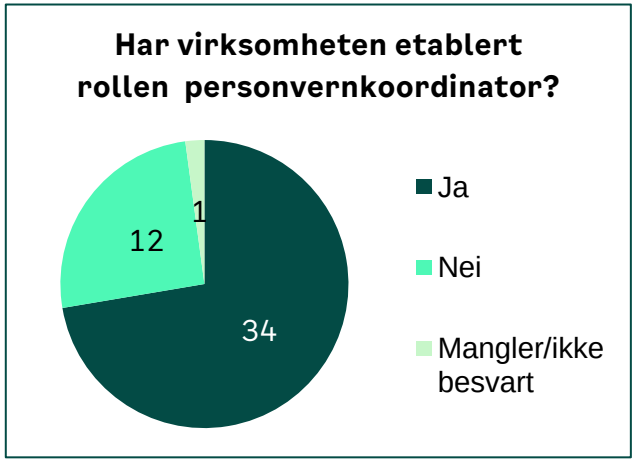
# Roller og ansvar innenfor informasjonssikkerhet og personvern

Definerte roller i byrådsavdelingen?

| BLK | FIN | NOE | BYU | MOS | KIF | OVK | EHA |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

Roller i virksomhetene




**214** personer i virksomhetene med dedikerte roller

**45** årsverk totalt

**16** oppgir at dette er samme person

# Risikostyring og risikovurderinger

## Gjennomføres det systematiske risikovurderinger?

| År | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 |
|---|---|---|---|---|---|---|---|---|
| 2019 | Det fremstår som om det gjøres | Alle har gjennomført | Ja | Ulikt nivå, nesten alle har forbedrings-potensiale | Gjøres i alle, men behov for økt kompetanse | I ulik grad | 1 etat overordnet ROS, ellers ja | Ja |
| 2018 | Ja – med et visst forbehold | Ja | Ja | I fremgang – stadig en del utestående | 2 av 3 foretar systematisk e risikov. | Nei, ikke systematis k | Bra i noen virksomh. | Ja |
| 2017 | For noen systemer. | Ja, i stor grad. Er også i prosess og i planlegging | Flere systemer. Flere er under planlegging | Viktige systemer tatt ut – flere i 2018 | Foretatt på enkelte prosedyrer / hendelser. | Usikkert om det er for det enkelte system | Bra i noen virksomh. | Variabelt – fra bra til i liten grad |
| 2016 | Ja | Ja i stor grad | Ja | Ikke fullstendig kartlagt. | Ikke komplett | Ja | VarierendeV et det finnes mangler | I noen grad |

# Risikostyring og risikovurderinger

Er det besluttet akseptabelt risikonivå?

| År | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 |
|---|---|---|---|---|---|---|---|---|
| 2019 | Arbeid igangsatt, må jobbes videre med | Ja | Er i prosess med å ferdigstille | Ja | Ja | Nei, avventer arbeid i BLK | Foreløpig ikke gjort | Virks. etablerer nivå basert på egen vurdering |
| 2018 | Arbeid igangsatt | Har startet, trenger bistand | Ønsker bistand fra FIN | Ja | Pågår, ferdigstilles 2019 | Nei, bistand nødvendig | Nei, avventer virksom-hetenes vurdering | Prosesser pågår |

# Risikostyring og risikovurderinger

## Kartlegging og verdivurdering av informasjon

| År | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 |
|---|---|---|---|---|---|---|---|---|
| 2019 | Ja | Ja, mener det | Noe er gjort, ikke tilstrekkelig | De fleste har gjort, men mange avvik | Pågår, vil sluttføres 2019 | Vurderer at det er gjort – på forskjellige måter | Helt eller delvis | Ja |
| 2018 | Ja | Ja, viser til internkont rollsystem | I god prosess | Ja, men enkelte avvik | Delvis | Alle er i gang | Delvis | Noe arbeid gjenstår |

Har virksomheten et metodeverk for å klassifisere og verdivurdere informasjon?

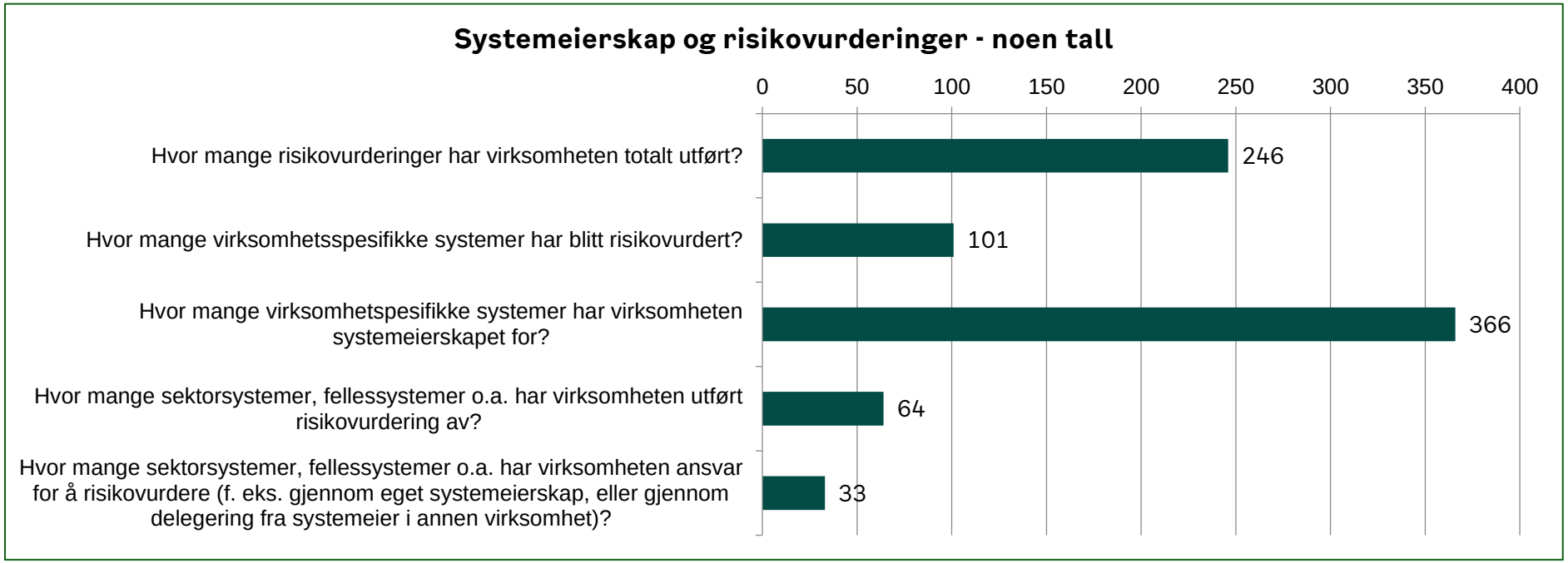
**28** virksomheter sier ja
**9** virksomheter har ikke
**10** virksomheter har enten ikke svart eller svaret er uklart.

# Risikostyring og risikovurderinger

## Personvernkonsekvensvurdering (DPIA)

- Totalt oppgis det å ha blitt gjennomført 220 personvernkonsekvensvurderinger (DPIAer).
- Tallene er svært usikre. (Av det totale antallet står én bydel for 200 av vurderingene).
- 11 virksomheter oppgir å ha gjennomført de resterende 20
- Det er vanskelig vurdere status for hver enkelt sektor. Lave antall i alle sektorer og virksomheter bortsett fra 1 bydel
- Antas at manglende kompetanse på området er bakgrunnen, for både det lave antallet og for de usikre tallene

# Risikovurderinger – noen tall



# Sikkerhet i anskaffelsesprosesser - noen tall


Bekrefter funn i Kommunerevisjonens rapport 01/2019

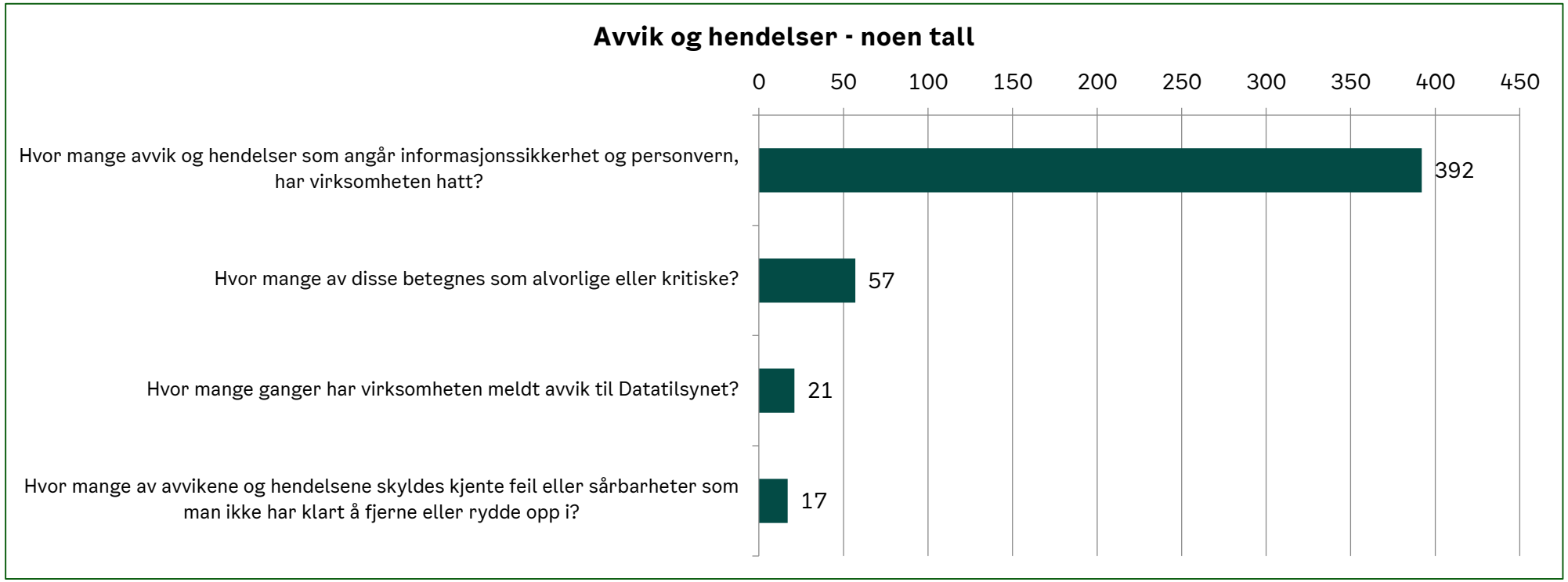
# Tilstrekkelig opplæring innen informasjonssikkerhet?

| År | B5 | B8 | B1 | B2 | B7 | B6 | B3 | B4 |
|---|---|---|---|---|---|---|---|---|
| 2019 | Ja | Ikke rapportert ? | Ja, men fortsatt potensiale for forbedring | Ja, henviser til internkontr ollsystem | Ja, alle rapportere å ha rutiner | Tja, i varierende grad | Ja | Tja, har fokus, men evnen til å gjennomfør e varierer |
| 2018 | Opplæring fortsetter – behov finnes | Uklart besvart fra virksomh. | Ja, men vi er ikke helt i mål. | Ja, alle virksomhet er har. | Ja, alle virksomhet er har. | Opplæring i varierende grad | Ja, kontinuerli g og systematis k | Har fokus, men kan også forbedres. |
| 2017 | Opplæring av ansatte | Har dels definerte krav | Har økt kompetans e | Opplæring av ansatte | Ikke besvart | Opplæring av ansatte | Opplæring av ansatte | Opplæring av ulike roller |
| 2016 | Ikke besvart | Utfordrend e | Tilstrekkeli g | Tilstrekkeli g | Identifisert mangler | Tilstrekkeli g | God kompetans e | Mangler |

# Kompetanse og opplæring, fra VE

- Oppgitt at ca. 5 % av kommunens ansatte har gjennomført opplæring på mer enn en halv dag.
- Stor usikkerhet rundt svarene i VE. Både relatert til hvor god oversikt virksomhetene har over kompetansetiltak, og når det gjelder systematikk innen området.
- Flere virksomheter oppgir e-læring i sikkerhetsmåneden som opplæringstiltak.
  - 15 prosent deltagelse, ned 1 prosent fra i fjor

# Avvik og hendelser – noen tall



# Meldinger til Datatilsynet

- Basert på virksomhetenes rapporteringer er det meldt 21 avvik til Datatilsynet.
- Datatilsynet selv oppgir at de har mottatt flere avvik enn dette.
- FINs vurdering er at det er underrapportering i kommunen, men det er vanskelig å slå fast i hvor stor grad.

# Status på personvernområdet

- Reviderte behandlingsoversikter
  - **29** har revidert
  - **10** har ikke revidert
  - **8** uklare svar eller ikke besvart
- Databehandleravtaler
  - **25** virksomheter har totalt **56** systemer med ekstern leverandør hvor det mangler databehandleravtaler
  - **36** systemer med databehandleravtaler som ikke har vært revidert i forhold til ny personopplysningslov
- Tilstrekkelig fokus?
  - Gjenstår mye arbeid før det er tilstrekkelig fokus i de ulike sektorene og i kommunen som helhet.
  - Positivt at flere virksomheter anerkjenner behovet for økt fokus på området.

# Oppsummering

## Utviklingen i kommunen går i riktig retning:

- Økt bevissthet og fokus generelt i kommunen (også i samfunnet)
  - Stor etterspørsel etter kompetanse og bistand (spesielt på personvern)
  - (Fortsatt) godt oppmøte på forum/møter
  - Workplace er tatt i bruk – digitalt samhandlingsverktøy med muligheter
  - Sikkerhetsmåneden 2019 – god oppslutning
- Godt i gang med etablering av roller som informasjonssikkerhetskoordinator og personvernkoordinater i virksomhetene
- Mange jobber godt med informasjonssikkerhet og personvern (men det er store forskjeller!)
- Kartoteket – kommunens løsning for en samlet system- og behandlingsoversikt, er tatt i bruk av mange
  - Potensiale for økt nytteverdi

# Utfordringer

***Høye forventninger til digitale tjenester - stor endringstakt - stor og kompleks organisasjon - trusselbilde i stadig endring.***

- Risikostyring og risikovurderinger – generelt økt kompetansebehov
  - Akseptabelt risikonivå
    - Kun 3 av 8 sektorer sier at det er etablert kriterier for akseptabelt risikonivå for sektoren
  - Personvernkonsekvensvurderinger (DPIA)
- Kompetanse/opplæring
  - Total vurdering er at behov for opplæring ikke er oppfylt
  - Mangelfull kompetanse og bevissthet på alle nivåer
- Sikkerhet i anskaffelser
  - Stort potensiale for forbedringer og bevisstgjøring om behov for risikovurderinger og sikkerhetstesting i anskaffelsesprosesser

# Utfordringer

- Hendelser og avvik – identifisering, varsling, håndtering og rapportering , eskaleringskriterier.
  - Kan se ut som mange har  mangelfull systematikk og oversikt. Varsles/rapporteres det som er relevant, eskaleres til rett nivå og raskt nok?
- Kontinuitetsplanlegging og beredskap (spesielt ved cyberhendelser)
  - Aktualisert ved Corona-situasjonen
- Oppdaterte behandlingsoversikter og databehandleravtaler
- En utfordring å få god nok oversikt innenfor sektorer og for fagmiljøet
  - Potensiale for forbedret rapportering
  - Måling av status og valg av riktige/gode indikatorer for dette
  - Måling av effekten av tiltak

# Viktige områder å jobbe videre med:

- Roller i alle virksomheter: **Personvernkoordinator(PKO) og informasjonssikkerhetskoordinator (ISK)**
- FIN fortsetter arbeid med **kompetanseprogram**
- Etablere rammeverk for å **måle modenhet**
- Ta i bruk **Kartoteket** som obligatorisk verktøy for bedre oversikt over systemer og behandlingsoversikter i kommunen
- Økt fokus på **kontinuitets- og beredskapsplanlegging** og **øving**

Sentralt verktøy for dette:

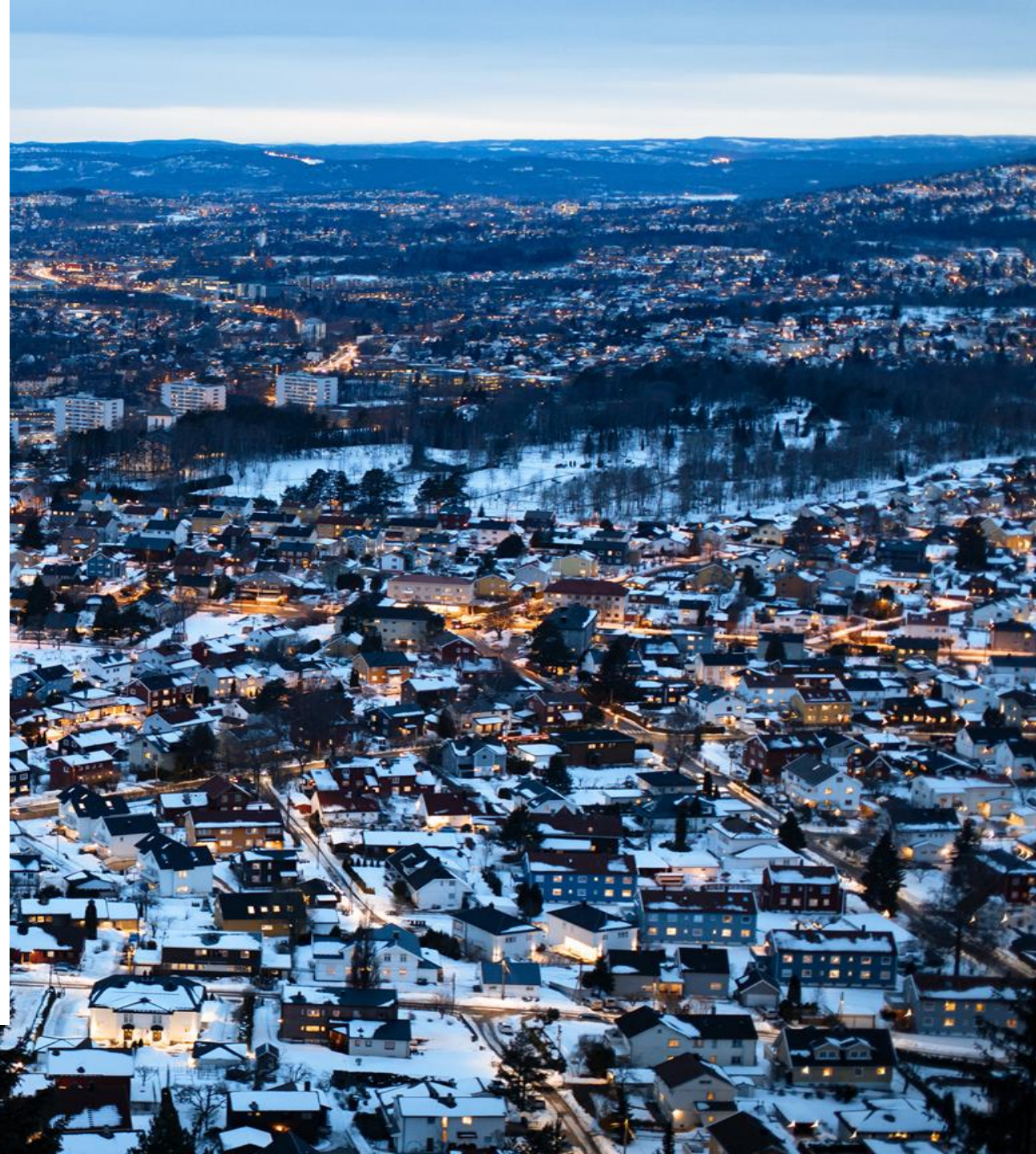
- **Styringssystem** (internkontrollsystem) i alle virksomheter - FIN jobber videre med overordnet styringssystem

Oslo

# Overordnet styringssystem for informasjonssikkerhet

Forum for personvern og informasjonssikkerhet

Mai 2020



# Hensikten med dagens presentasjon

- Informere om arbeidet med det overordnede styringssystemet i Oslo Kommune

# Bidra til enklere operasjonalisering av krav i styrende dokumenter

- Virksomhetene og sentrale fagressurser uttrykker at det er stor avstand mellom overordnede reglement og operasjonaliseringen i den enkelt virksomhet
- Tydeliggjøring av fellesføringer vil bidra til enklere operasjonalisering av informasjonssikkerhet i virksomhetene
- Bidra til bedre forutsigbarhet for virksomhetsledere og fagpersoner
- Sikre at sentrale risikoområder ivaretas i alle sektorer

# Rammebetingelser for arbeidet

- Styrende dokumentene for informasjonssikkerhet
- Lover og regler
- Se hen til erfaringer fra andre fagområder, som f.eks anskaffelser
- 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 rolle, 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)

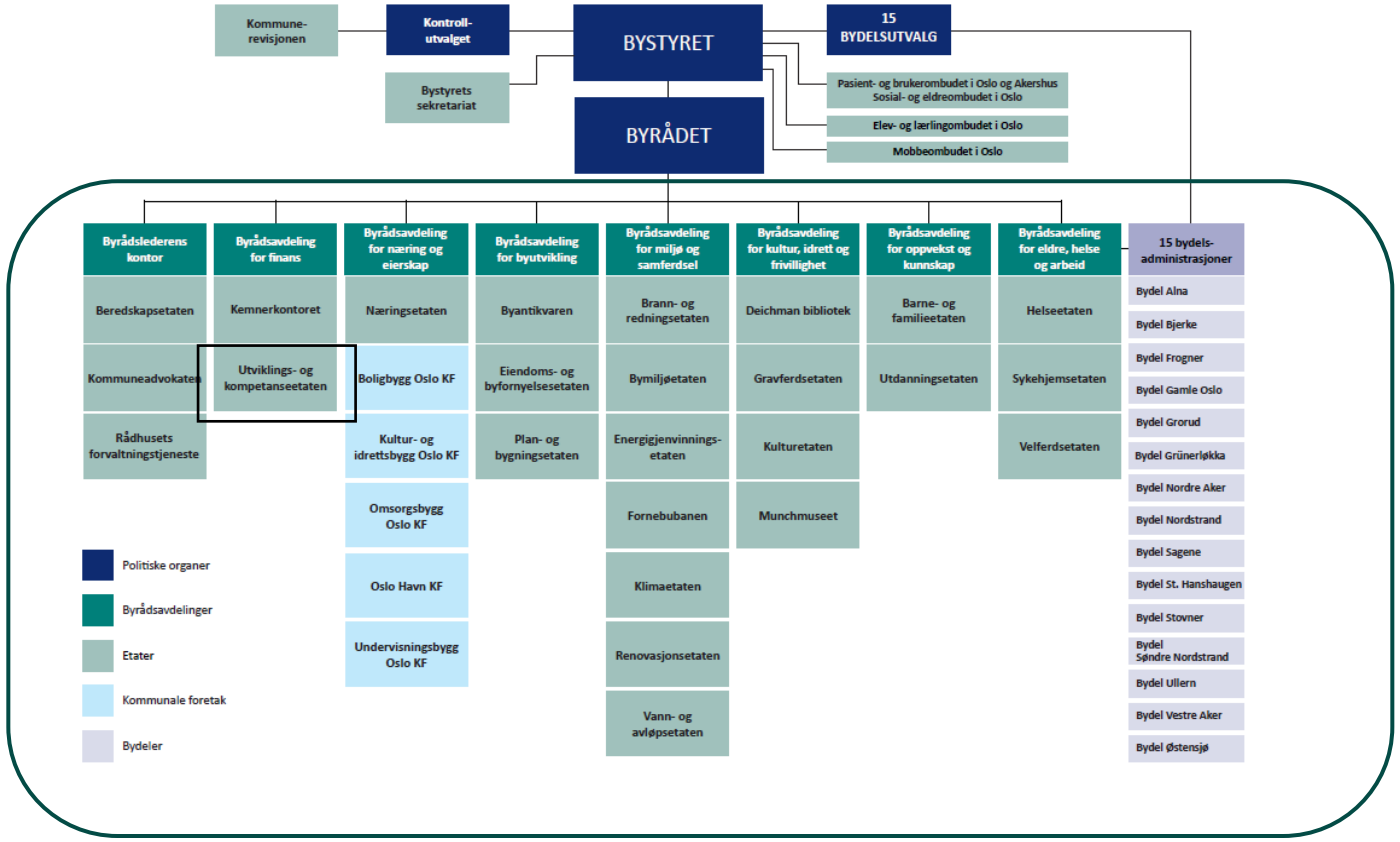
**Instruks for virksomhetsstyring**

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 |

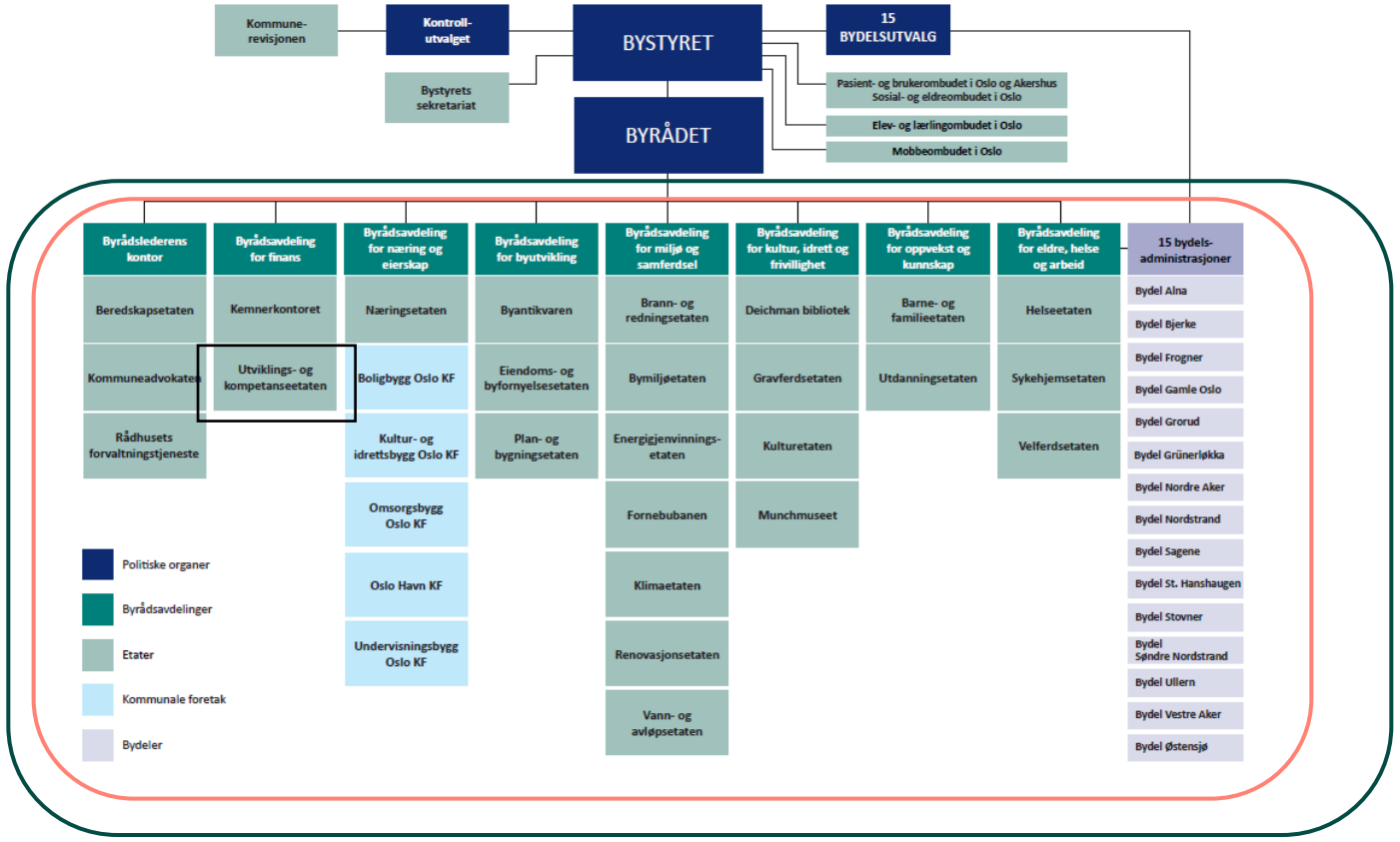
# Det overordnede styringssystemet omfatter hele kommunen, hvor de styrende dokumentene inngår.




Instrukser og reglement på informasjonssikkerhetsområdet (politisk nivå)

Virksomhetene beslutter egen operasjonalisering.

# Det overordnede styringssystemet omfatter hele kommunen, hvor de styrende dokumentene inngår.




Instrukser og reglement på informasjonssikkerhetsområdet (politisk nivå)

Informasjonssikkerhets-standarder (administrativt nivå)

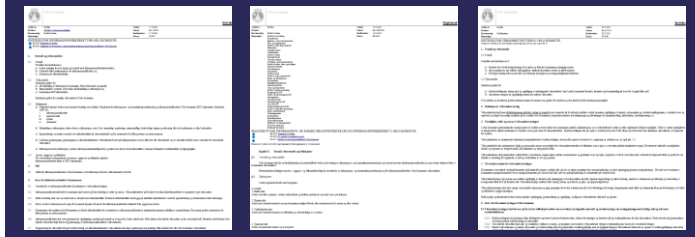
Utgjør det overordnede styringssystemet

Virksomhetene beslutter egen operasjonalisering.

# Risikoområder som dekkes i et styringssystem

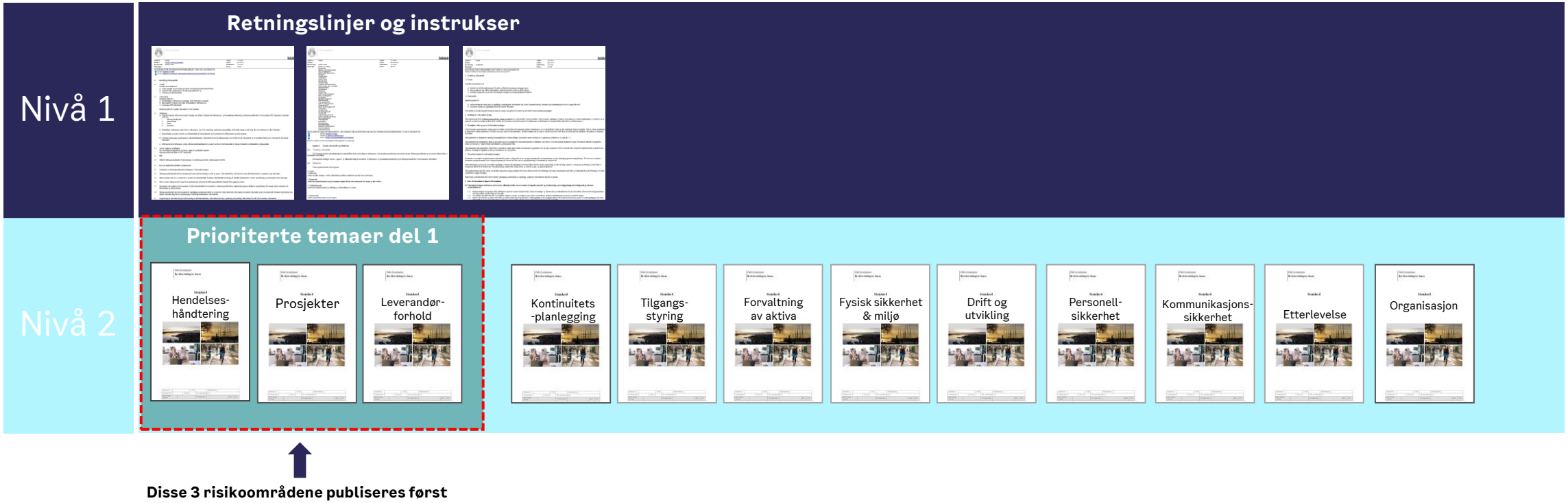
Nivå 1

**Retningslinjer og instrukser**



Nivå 2

# Risikoområder som dekkes i et styringssystem



# 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.

Krav til **opplæring** av alle medarbeidere slik at de er i stand til å identifisere situasjoner som kan innebære en informasjonssikkerhetshendelse.

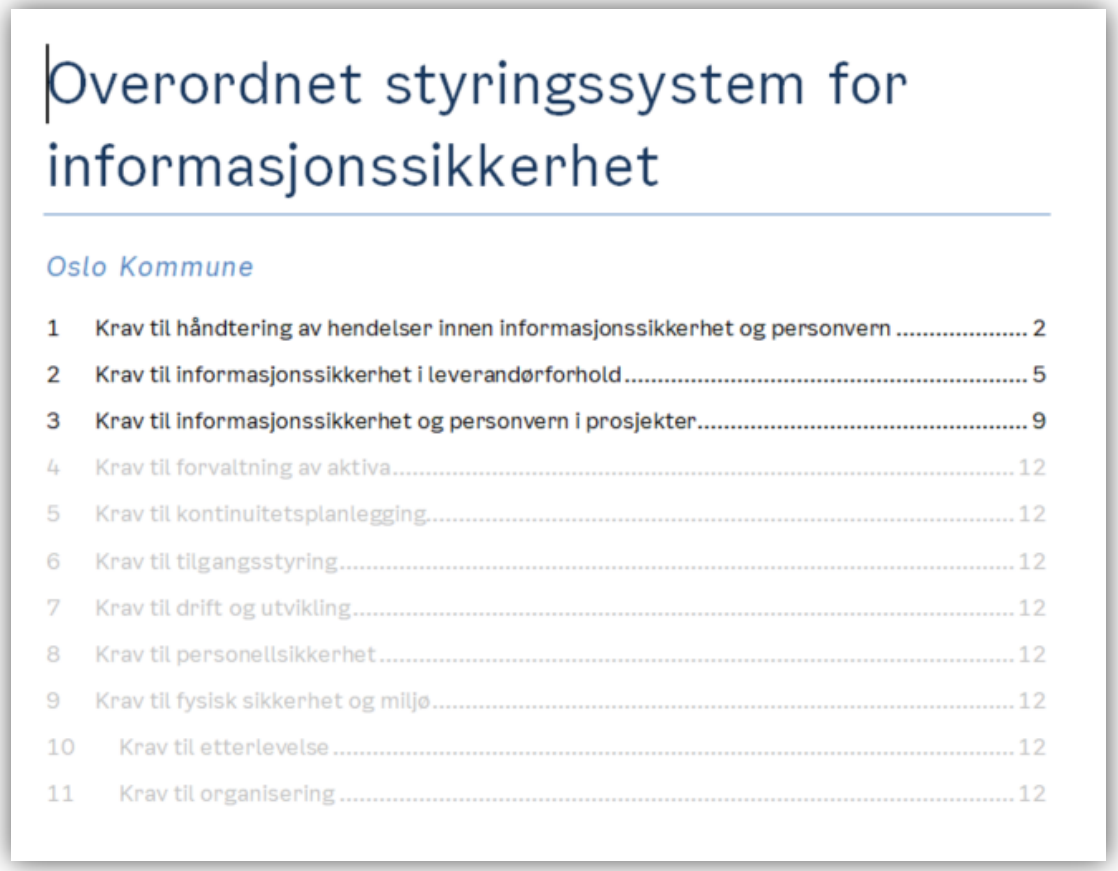
Krav til at virksomhetene identifiserer **et eller flere varslingspunkt** hvor hendelser skal innrapporteres.

Virksomhetene skal i samråd med overordnet byrådsavdeling varsle **Datatilsynet** innen 72 timer dersom det har skjedd et brudd på personopplysnings-sikkerheten. Ombudet skal kontaktes.

Krav til en **rapport** som oppsummer:
- Hendelsesforløpet
- Iverksette tiltak
- Vurdering av årsak
- Eventuelle ytterligere tiltak

# 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 informasjonssikkerhet

*Oslo Kommune*

# Kvalitetssikring av arbeidet

- Kvalitetssikring av fremgangsmåte og innholdet standardene opp mot:

✓Standard of good practice (Information security forum)

✓ISO 27001/2 standarden

✓Digitaliseringsdirektoratets anbefalinger for informasjonssikkerhetsarbeid i offentlig ektor

✓Erfaringer innhentet fra Bærum og Trondheim kommune

# Veien videre

- Formalisere og publisere overordnet styringssystem - del 1
  - Høste erfaringer
  - Kontinuerlig forbedring
- Fortsette arbeidet med del 2 og 3 for formalisering og publisering

# Personvern- og informasjonssikkerhets-koordinator

Forum for personvern og informasjonssikkerhet
26.05.2020

Oslo

# Fellesføring i 2020

- *Virksomhetenes arbeid med å etterleve krav til informasjonssikkerhet og personvern må fortsette. Alle virksomhetene skal ha utpekt personvern- og informasjonssikkerhetskoordinatorer innen utgangen av året.*

- FIN vil innen kort tid sende ut informasjon til alle virksomheter om formålet med koordinatorrollene, vanlige oppgaver og utpeking av koordinatorer.

# Formål

- Øke virksomhetenes kompetanse innen personvern og informasjonssikkerhet.
- Bedre grunnlaget for samhandling på tvers i kommunen.
- Fagressurs for virksomhetene – sentral rolle.

# Status

- Basert på rapporteringene fra i fjor har de fleste allerede utpekt personer, spesielt som informasjonssikkerhetskoordinator.
- Noe usikkert om alle som er utpekt har fått tilstrekkelig tid til å ivareta oppgavene og tilstrekkelig opplæring.
- Behov for å tydeliggjøre hva rollene innebærer, både for ledere, koordinatorene selv og virksomhetene for øvrig.

Oslo

# Årsrapporten til Personvernombudet 2019

Personvernombudet