Oslo

Byrådsavdeling for finans

Veiledning

Ledelsens gjennomgang

Oversikt og status for siste periode på informasjonssikkerhets- og personvernområdet, og føringer for videre aktiviteter og prioriteringer.

Foto: Thomas Ekström

Ledelsens gjennomgang

Innhold

Godkjent av:			U.off:		Saksbehandler:		
Godkjent dato:		Versjon:		Sak- og dokumentnr:			
Mal – denne versjonen:	Ledelsens gjennomgang (2021)			Erstatter mal:	Ledelsens gjennomgang (2020)	Eier:	FIN

1 Om Ledelsens gjennomgang

A - Ledelsens gjennomgang

Følgende innledende tekst fra malens kapittel 1.1 kan gjerne beholdes når virksomheten fyller ut Ledelsens gjennomgang:

Ledelsens gjennomgang skal sikre at ledelsen får en helhetlig oversikt over personvern- og informasjonssikkerhetsarbeidet i virksomheten, og er en aktivitet for å følge opp, forbedre og effektivisere styringen av dette arbeidet.

Formålet med Ledelsens gjennomgang er å:

- orientere og bevisstgjøre ledelsen i virksomheten
- sikre en helhetlig oversikt over styrings- og kontrollaktiviteter i foregående periode
- sørge for at ledelsen har grunnlag for å gi føringer for prioriteringer for kommende periode
- fremskaffe nødvendig grunnlag for Virksomhetsleders egenerklæring

Ledelsens gjennomgang av informasjonssikkerhet er forankret i Instruks for informasjonssikkerhet punkt 3.6 for Oslo kommune (byrådssak 1105/13) og gjennomføres årlig.

> *«Informasjonssikkerhet skal være gjenstand for oppfølgning, regelmessig kontroll og revisjon for å sikre etterlevelse, både internt i den enkelte virksomhet og fra overordnet nivå. Herunder skal ledelsen i den enkelte virksomhet årlig foreta en gjennomgang av informasjonssikkerheten i virksomheten.»*

Ledelsens gjennomgang er i tillegg krav i Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) for de virksomheter som er knyttet til Norsk helsenett. Krav i Normen er av den grunn ivaretatt i ny revidert mal for Ledelsens gjennomgang.

Rapportering gjennom Ledelsens gjennomgang er en rapportering av all behandling av informasjon i virksomheten, dette inkluderer all behandling av personopplysninger.

B - Målgruppe for rapporteringen

Målgruppen for Ledelsens gjennomgang er virksomhetens egen ledergruppe.

Byrådsavdeling for finans eller egen byrådsavdeling kan bestemme at Ledelsens gjennomgang skal sendes inn til byrådsavdelingen sammen med Virksomhetsleders egenerklæring.

C - Om beskrivelse av funn og tiltak

Rapportene fra Ledelsens gjennomgang vil være unntatt offentlighet. For dette året må vi anta at rapportene blir liggende i Acos WebSak, slik at det vil være ganske bred tilgang for kommunens «innsidere».

En utdypning av detaljer i funn og tiltak vil kunne avsløre detaljer om virksomhetens sårbarheter og risiko. Utdypning av tiltak avslører sikkerhetstiltakene som implementeres og øker behovet for ytterligere beskyttelse av dokumentet. Det er derfor ønskelig å holde beskrivelsene på et slikt nivå at det er tydelig og forståelig hva det gjelder, men å ikke gi detaljert informasjon som kan utnyttes til å angripe virksomheten eller misbruke systemer og informasjon. Dette gjentas i veilederen for de mest aktuelle enkeltområdene.

D - Om veilederen

Veilederen skal bidra til at en virksomhet innhenter, strukturerer og presenterer relevant informasjon til Ledelsens gjennomgang med bruk av mal utarbeidet av Byrådsavdeling for finans (FIN). I veilederen finnes det beskrivelse av hvordan de forskjellige feltene og tabellene i Ledelsens gjennomgang skal brukes.

Dette dokumentet inneholder også eksempeltekst som viser hvordan Ledelsens gjennomgang er fylt ut for en fiktiv virksomhet. Dette kan være nyttig å se på når Ledelsens gjennomgang skal fylles ut for din virksomhet.

2 Om malen

Malen brukes i gjennomføring av Ledelsens gjennomgang av informasjonssikkerhet.

A - Slik fyller du ut forsiden i malen

Rapporteringsperioden er satt til 01.09.2020 – 31.8.2021. Avvik fra dette må avtales med egen byrådsavdeling.

- **Fyll inn rapporteringsperiode og navn på virksomheten i boksen på forsiden av rapporten.**
- **Erstatt <Virksomhet> med navn på virksomheten i toppteksten.**

B - Slik fyller du ut «1.2 Om rapporten» i malen

Det må fremgå hvem som har utarbeidet rapporten og hvem som har bidratt med informasjon i form av navn og rolle. Videre bør det spesifiseres hvilke datakilder og datagrunnlag som er brukt for innsamling til Ledelsens gjennomgang. Dette spesifiseres i *«1.2 Om rapporten»* i malen, se eksempel.

Sett inn rapporteringsperiode, dersom denne avviker fra 01.09.2020 – 31.8.2021:

Involverte som har bidratt med informasjon til, og utfylling av, rapport:

- Samuel Sag, saksbehandler og ansvarlig for innhenting av informasjon som danner grunnlag for Ledelsens gjennomgang for informasjonssikkerhet
- Asta Angrer, personvernkoordinator (PKO)
- Stein Skrekk, informasjonssikkerhetskoordinator (ISK)
- Nils Nerd, IKT-leder
- Kari Kontroll, revisjonsleder. Har bidratt med datagrunnlag om gjennomførte interne og eksterne revisjoner, tilsyn, mv.
- Avdelingsledere har bidratt med informasjon om tiltak utført i egne avdelinger i perioden. Det gjelder både risikovurderinger og oppfølging av avtaler og leverandører der avdelingsleder også er systemeier.
- Frode From, kvalitetsleder og systemeier for avviks- og hendelseshåndteringssystemet
- Arne Areal, eiendomsforvalter

Rapporten er gjennomlest og godkjent av Dina Direktør, virksomhetens daglige leder.

Datakilder og datagrunnlag:

- Ledelsens gjennomgang og Virksomhetsleders egenerklæring for foregående år
- Etablering av sikkerhetsorganisasjon, saksnummer: 18-389
- Gjennomførte risikovurderinger i etaten i perioden
- Meldte avvik og hendelser med høy alvorlighetsgrad rapportert i avviks- og hendelsessystemet i perioden
- Interne og eksterne revisjoner gjennomført i perioden
    - Saksnummer
        - 18-885
        - 18-974
        - 19-176

C – Slik fyller du ut «2 Oversikt – Ledelsens gjennomgang» i malen

I kapittel 2 i malen skal virksomhetene fylle ut tabellene. Nederst i flere av tabellene er det en tekstboks for kommentar og utfyllende svar. **Eksempler på svar er fylt inn i tabellene.**

Slik fyller du ut «2.1 Ansvar og organisering»

Virksomheten skal kortfattet beskrive sin organisering av arbeidet med informasjonssikkerhet og personvern. Det er også mulig å sette inn sette inn en link til en beskrivelse dersom dette er åpen informasjon. De skal også angi om valgt informasjonssikkerhetsorganisering fungerer etter hensikten. Dersom det er opprettet nye roller eller nye ansvarsområder i løpet av rapporteringsperioden, bør dette beskrives.

Gi en kortfattet og overordnet beskrivelse av hvordan arbeidet med informasjonssikkerhet og personvern er organisert i virksomheten.
Rollene som personvernkoordinator og informasjonssikkerhetskoordinator er tildelt to personer i ulike seksjoner. Koordinatorene er operative og veileder i spørsmål/saker knyttet til informasjonssikkerhet og personvern. De støtter seg til en styringsgruppe for ivaretagelse av spørsmål og utfordringer relatert til informasjonssikkerhet. Gruppen består av avdelingsdirektør for Administrasjon, seksjonsleder HR, seksjonsleder Tjenester og seksjonsleder IKT. Delene av rollekortet som handler om personellsikkerhet, fysisk sikring, beredskap og hendelser og avvik (HMS), ligger i linja i henholdsvis Seksjon for eiendom og i Seksjon HR.
Beskriv eventuelle endringer i organisering av arbeidet med personvern og informasjonssikkerhet som er gjort i rapporteringsperioden.
Det er opprettet mandater for personverns- og informasjonssikkerhetskoordinatorene basert på rollekortene. Vi har gått fra en duplisering av rollen som personverns- og informasjonssikkerhetskoordinator til at de samme to ansatte rendyrker hver sin rolle.

Gi en kort vurdering av om valgt personvern- og informasjonssikkerhetsorganisering fungerer etter hensikten.
Virksomheten oppfatter sin egen organisering som hensiktsmessig. Sentrale roller for å koordinere informasjonssikkerhet og personvern er tildelt navngitte personer som har dette som en stor del av sine arbeidsoppgaver. Ledelsen godkjenner alle styrende dokumenter.
Gi en kort vurdering av om virksomheten har tilstrekkelige ressurser til personvern- og informasjonssikkerhetsarbeidet.
Virksomheten vil også gå gjennom de rutinene som blir brukt for systemeierskap og systemforvaltning og få verifisert at de er i samsvar med kommunens styrende dokumenter. Dette skal også sees i sammenheng med ressursbruk.

Slik fyller du ut «2.2 Risikovurderinger» i malen

Beskriv risikovurderinger innen informasjonssikkerhetsområdet som er gjennomført i perioden.

Risikovurderinger som det er relevant å informere om, er der risiko og sårbarheter kan påvirke målene til virksomheten gjennom brudd på konfidensialitet, tilgjengelighet og integritet.

Begrepene her er:

- Konfidensialitet: At kun de med tjenstlig behov får innsyn i informasjonen.
- Integritet: At informasjonen er korrekt og pålitelig.
- Tilgjengelighet: At informasjonen er tilgjengelig ved behov.

Ved vurdering av alvorlighet er det den høyeste alvorlighetsgraden for en uønsket hendelse, ved tidspunktet for utført risikovurdering som skal beskrives i tabellen.

Som en del av styringen av informasjonssikkerhet er det viktig å ha et innblikk i systematikken i risikovurderinger og forstå hvilke risikovurderinger som prioriteres. Det er derfor ønskelig at virksomhetene beskriver dette og gjerne også sier noe om hvilke risikovurderinger som tenkes prioritert for neste rapporteringsperiode.

Dersom det kommer flere viktige tiltak ut av en gjennomført risikovurdering, kan det brukes en linje per tiltak, slik at det blir mange linjer per risikovurdering.

For å melde grønt på en risikovurdering må det som minimum finnes konkrete planer for å lukke alle viktige funn.

Når funn og tiltak skal beskrives, må beskrivelsen være på et slikt nivå at det ikke blir gitt detaljert informasjon som kan utnyttes til å angripe virksomheten eller misbruke systemer. Det advares derfor mot å være altfor eksplisitt om sårbarheter som ikke er lukket.

For utfylling av status for planlagte tiltak kan *utført, i arbeid, ikke påbegynt* brukes.

Se eksempel på utfylling i tabellen nedenfor.

2.2 Risikovurderinger

Risikovurderinger innen informasjonssikkerhetsområdet som er gjennomført i perioden.

Nr.	Beskrivelse av risiko-vurderinger	Risiko-vurderingens avgrensning	Beskrivelse av funn (mulig uønsket hendelse)	Vurdering alvorlighet	Planlagte tiltak	Status / restrisiko	Ansvarlig
1	Tilganger til regnskaps-systemet	Vurdert brukertilganger og tilgang til informasjon (tjenstlig behov)	Utdaterte brukertilganger			Går ned til grønt.	
					1.1 Fjerne tilganger for personer som ikke lenger er ansatt, eller har andre oppgaver	Utført	Økonomi-leder
					1.2 Lage ny rutine for å gå gjennom tilganger månedlig	I arbeid	Økonomi-leder
2	Fysisk sikring Hoved-kontoret i Dilemmaveien 12	Er det god nok fysisk sikring av kontorer der informasjon om ansatte behandles?	Manglende muligheter for å låse kontorer eller låse ned personopplysninger			Går ned til gult	
					2.1 Ansatte på kontorer med muligheter for å låse med nøkkel skal få utdelt nøkler. Ansatte	I arbeid	Eiendoms-forvalter

Nr.	Beskrivelse av risiko-vurderinger	Risiko-vurderingens avgrensning	Beskrivelse av funn (mulig uønsket hendelse)	Vurdering alvorlighet	Planlagte tiltak	Status / restrisiko	Ansvarlig
					på kontorer uten låse-mulighet skal få utdelt safe.		
	Kommentar: Vi ser på alle systemer som vår virksomhet har eierskap til og vurderer om det er behov for en fullstendig risikovurdering. Hvis det ikke har vært større endringer i systemet, rammebetingelsene eller omgivelsene, foretas kun en kort gjennomgang for å verifisere at bilde av sårbarheter og trusler ikke har forandret seg nevneverdig. Andre typer risikovurderinger blir utført etter behov. Vi vet at det mangler noe systematikk i hvordan avvik og forslag til tiltak fra risikovurderingene blir fulgt opp.						

Slik fyller du ut «2.3 Personvernkonsekvensvurderinger (DPIA)»

Det skal fylles ut informasjon om hvilke personvernkonsekvensvurderinger (DPIA) som er gjennomført i perioden. Det vil her være snakk om de behandlingene som medfører en høy risiko for den registrertes rettigheter og friheter, og som utløser en plikt for virksomheten etter personvernforordningen art 35 til å gjennomføre en personvernkonsekvensvurdering (DPIA).

En DPIA vil være en del av virksomhetens internkontrolldokumentasjon. Det er derfor ønskelig at virksomheten beskriver hvilke personvernkonsekvensvurderinger som er gjennomført og hvilke funn som ble gjort i vurderingen. Virksomheten skal beskrive hvilke tiltak som iverksettes for å ta ned risikoen til et akseptabelt nivå. Det skal også beskrives hvem som er ansvarlig leder (godkjenner DPIA). Dersom risikoen ikke kan tas ned (forblir høy) er virksomheten pliktig til å sende DPIA'en til en forhåndsdrøftelse med Datatilsynet før behandlingen starter, dette skal virksomhetene også svare på i tabellen.

Sett inn teksten over tabellene i malen: Personvernkonsekvensvurderinger (DPIA) etter personopplysningsloven art 35 som er gjennomført i perioden. Aktuelle personvernkonsekvensvurderinger er der risikoen for den registrertes rettigheter og friheter anses som høy.

2.3 Personvernkonsekvensvurderinger (DPIA)

Personvernkonsekvensvurderinger (DPIA) etter GDPR art 35 som er gjennomført i perioden. DPIA er påkrevd når risikoen for den registrertes rettigheter og friheter anses som høy.

Nr.	Beskrivelse av DPIA: kort om bakgrunn og hvilken løsning/systemer som er vurdert	DPIAs omfang og avgrensning	Vurdering alvorlighet
1	Vurdering av digital kommunikasjonsverktøy med pasienter	Avgrenses mot intern digital kommunikasjon mellom ansatte innad i kommunen	

Nr.	Beskrivelse av funn	Beskrivelse av tiltak	Status/restrisiko	Forhåndsdrøftelse med Datatilsynet (Ja/Nei)	Ansvarlig
1	Løsningen tilbyr funksjonalitet som utfordrer prinsippene om dataminimering, lagringsbegrensning, konfidensialitet og integritet, samt retten til privatliv.	Informasjon til de registre Tilgangsstyring Stenge av funksjonalitet som gjør at kun nødvendig informasjon behandles, det vil ikke kunne lagres helseopplysninger, slik at bruken kun blir videooverføring. Sletteintervaller i logger utføres automatisk	Ingen restrisiko	Nei, risikoen anses som Middels forutsatt at skisserte tiltak gjennomføres	Seksjonsleder/ avdelingsleder

Slik fyller du ut «2.4 Avvik og hendelser»

Beskriv hvilke avvik og hendelser som er registrert i perioden. Dette kan være helt eller delvis bortfall av kritiske tjenester, fare for liv og helse, og personopplysninger på avveie slik at uautoriserte har fått eller kan få tilgang. Avvik omfatter også brudd på personopplysningssikkerhet etter GDPR.

Et avvik er at manglende oppfyllelse av ett eller flere krav oppdages. En uønsket hendelse er en hendelse som kan føre til tap av konfidensialitet, integritet eller tilgjengelighet for en verdi (f. eks. en informasjonsverdi), eller brudd på lovverk eller andre styrende krav. Alvorlighetsgraden for avvikene og hendelser kan kategoriseres ut fra konsekvensnivå i akseptkriterier for risiko. Alle hendelser som, enten enkeltstående eller aggregert, har en alvorlighetsgrad som er høyere enn «Moderat», skal rapporteres.

Hendelsene kan være rapportert direkte fra ansatte eller gjennom andre rapporteringskanaler. Medarbeidere har plikt til å informere ledelsen om avvik eller hendelser med høy alvorlighetsgrad, f.eks. delvis eller helt bortfall av kritiske tjenester, fare for liv og helse, og utilsiktet eller ulovlig endring av personopplysninger eller personopplysninger på avveie slik at uautoriserte har fått eller kan få tilgang.

Brudd på personopplysningssikkerheten skal meldes til Datatilsynet etter GDPR art. 33. Alle brudd på personopplysningssikkerheten skal meldes til personvernombud, Byrådsavdeling for finans ved Seksjon for informasjonssikkerhet og IKT, egen overordnet byrådsavdeling, og alltid rapporteres i Ledelsens gjennomgang. Informasjon til de berørte registrerte skal gis dersom risikoen for de registrerte er høy.

Når alvorlighetsgrad blir fastslått, må det tas hensyn til både enkelthendelser og hendelser som ikke er så alvorlige i seg selv, men som ut fra hyppighet og omfang kan innebære alvorlige konsekvenser for de registrerte eller for virksomheten.

Når avvik, hendelser og tiltak skal beskrives, må beskrivelsen være på et slikt nivå at det ikke blir gitt detaljert informasjon som kan utnyttes til å angripe virksomheten eller misbruke systemer, eller medføre konsekvenser for den berørte registrerte. Det advares derfor mot å være altfor eksplisitt i denne rapporteringen om avvik som ikke er lukket.

Det er også viktig for virksomheten å kartlegge om de har viktige kjente sårbarheter og ikke-realiserte trusler hos seg. Dette bør nevnes i kommentarfeltet, men igjen advares det mot å være altfor eksplisitt i det en beskriver.

For utfylling av status for planlagte tiltak kan ***utført, i arbeid, ikke påbegynt*** brukes.

Se eksempel på utfylling i tabellen nedenfor.

2.4 Avvik og hendelser som er registrert i perioden

Nr.	Beskrivelse av avvik/hendelse	Beskrivelse av årsak	Vurdering alvorlighet	Planlagte tiltak?	Status	Meldt til Data-tilsynet (Ja/Nei)	Informasjon gitt til de berørte registrerte?	Ansvarlig
						(Gjelder ved brudd på personopplysningssikkerhet)		
1	Anarkistgruppe hacket nettside for innrapportering av sviktende moral, tok ned siden og offentliggjorde innholdet.	Feil konfigurasjon av brannmur		Nytt oppsett av brannmur Inntrengingstest	Utført			Driftssjef
2	Ansatt mistet PostIt-lapp med passord til etikksystem	Ingen hadde lært de ansatte rutiner for å oppbevare passord		Passord ble byttet. Rutiner vil bli gjennomgått	I arbeid			Linjeleder

Kommentar: *Inntrengingstest i brannmur indikerte at det fremdeles er noen utestående sårbarheter i oppsettet. Arbeid for å lukke disse pågår. Situasjonen er under kontroll, og vi vil ikke offentliggjøre mer detaljer her*

Slik fyller du ut «2.5 Revisjon, tilsyn, mv.»

Beskriv hvilke enkeltstående og/eller systematiske tiltak som er gjennomført i perioden for å kontrollere om virksomheten etterlever gjeldende krav innenfor informasjonssikkerhets- og personvernområdet. Her skal revisjoner fra Kommunerevisjonen, tilsyn fra

kontrollmyndigheter eller egne vurderinger for å påse at krav i en lov/forskrift etterleves, tas med. Revisjoner eller gjennomganger som er initiert, bestilt og betalt av overordnet instans i Oslo kommune skal også listes opp i denne tabellen.

Beskriv funn og tiltak på et slikt nivå at det ikke blir gitt detaljert informasjon som kan utnyttes til å angripe virksomheten, misbruke systemer eller medføre konsekvenser for den berørte registrerte

2.5 Revisjon, tilsyn, mv.

Nr.	Beskrivelse av revisjon, tilsyn, mv.	Aktivitetens omfang/formål/ fokus	Hovedfunn	Vurdering alvorlighet	Planlagte tiltak	Status	Ansvarlig
1	Intern revisjon av behandling av personopplysninger i personalsystemet.	Behandles person-opplysninger og sensitive personopplysninger iht. personopplysningsloven?	Personalsystemet er ikke i henhold til krav i personopplysningslov og *-forskrift*.		1.1 Gå gjennom systemet ut fra krav til innebygget personvern	I arbeid	HR-sjef
2	Kommunerevisjonen – Forvaltningsrevisjon av informasjonssikkerhet.	Virksomhetens etterlevelse av instruks for informasjons-sikkerhet.	Informasjonssikkerhet er ikke godt nok integrert i virksomhetsstyringen		2.1 Ta info.sikkerhet inn i virksomhetens styrende dokumenter	Planlagt	Direktør
					2.2 Få på plass roller for å ivareta ansvar for informasjonssikkerhet og få disse forankret	I arbeid	Direktør
3	E-post med phishing-test.	E-post med forsøk på phishing er sendt til ansatte for å måle hvor mange som klikker på lenken.	Ingen av de ansatte klikket på lenken		Unødvendig	--	--

Kommentar:

Slik fyller du ut «2.6 Oppfølging av avtaler og leverandører»

Oppsummer oppfølging og kontroll av avtaler som virksomheten har inngått. Dette inkluderer databehandleravtaler med eksterne leverandører som behandler personopplysninger på vegne av virksomheten, og oppfølging/kontroll av leverandørers etterlevelse av personvern- og informasjonssikkerhetskrav. Avtaler/ordninger om felles behandlingsansvar som Oslo kommune har inngått med andre virksomheter må også tas med i oppsummeringen. Felles behandlingsansvar betyr at to eller flere virksomheter sammen fastsetter formålet med og midlene for behandling av personopplysninger.

For utfylling av status for planlagte tiltak kan ***utført, i arbeid, ikke påbegynt*** brukes.

2.6 Oppfølging av avtaler og leverandører

Nr.	Avtale/leverandør	Vurdering / endringsbehov for avtale	Leverandørs etterlevelse av PV-og ISkrav	Vurdering alvorlighet	Planlagte tiltak	Status	Ansvarlig
1	Avtale med HighClouds – innkjøp av skytjeneste	Ansvar og roller for info.sikkerhet hos leverandør er uklare	Ansvar og roller for info.sikkerhet hos leverandør er uklare		Ansvar og roller for ivaretakelse av informasjonssikkerhet må defineres hos leverandør	I arbeid	System-forvalter

2	Databehandleravtale med AS Norsk Etikkdata	Kontroll viser at alle nødvendige punkter er på plass, og blir etterlevet	Kontroll viser at alle nødvendige punkter er på plass, og blir etterlevet		Unødvendig	--	--
Kommentar: *Virksomheten har sett over alle databehandleravtaler som kan være relevante for personopplysninger. Alle disse er gjennomgått i løpet av de seneste 1 ½ år. Andre avtaler om utkontraktering og utsetting av tjenester er ikke gjennomgått på samme måte.*							

Slik fyller du ut «2.7 Norsk helsenett»

Avsnittet er kun relevant for virksomheter som er tilknyttet Norsk helsenett. I kap 2.5. i Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren skal virksomhetene foreta en gjennomgang der følgende punkter bør inngå:

- endringer i behandlinger av helse- og personopplysninger (protokoll)
- endringer i organiseringen av arbeidet
- resultat fra risikovurderinger og personvernkonsekvensvurderinger
- resultat av avviksbehandling
- oppfølging av leverandører og databehandleravtaler
- endring i nivået for akseptabel risiko mv.

Hvis virksomheter har gjennomført kontrollaktiviteter for disse punktene som ikke fremgår av informasjon tidligere i Ledelsens gjennomgang, skal disse listes opp her. Dersom gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt, skal det vedtas tiltaksplaner for å rette opp dette, med tidsfrister og plassering av ansvar. For utfylling av status for planlagte tiltak kan utført, i arbeid, ikke påbegynt brukes

2.7 Norsk helsenett

Nr.	Utført kontrollaktivitet	Eventuelle behov for endringer eller nye tiltak	Vurdering alvorlighet	Planlagte tiltak	Status	Ansvarlig

Kommentar: *Avsnittet er kun relevant for virksomheter som er tilknyttet Norsk helsenett, og vi har ikke fylt ut det.*

D – Slik fyller du ut «Prioriteringer og konklusjon» i malen

I kapittel 3 skal det gjøres rede for status på tiltak som ledelsen har prioritert å gjennomføre for å forbedre informasjonssikkerhet og personvern i virksomheten.

Slik fyller du ut «3.1 Status for prioriteringer forrige periode»

Her gis en status for aktiviteter besluttet prioritert i forrige Ledelsens gjennomgang i virksomheten. For utfylling av status kan ***utført, i arbeid, ikke påbegynt*** brukes.

3.1 Status for prioriteringer forrige periode

Beskriv oppdatert status for de aktivitetene som ble besluttet å følge opp i forrige Ledelsens gjennomgang.

Nr.	Forrige periodes prioriteringsområde	Status	Ansvarlig
1	Definere oppgaver og utpeke info.sikkerhetskoordinator	Utført	Direktør
2	Inntrengingstest i etikksystemet	Ikke påbegynt	IKT-sjef
3	Verdivurdering av all informasjon i systemet	I arbeid	ISK

Slik fyller du ut «3.2 Prioriteringer neste periode»

I dette avsnittet gjøres det rede for hvilke områder ledelsen i virksomheten ønsker å prioritere neste periode. Valgene skal baseres på en helhetlig vurdering av status for personvern og informasjonssikkerhet og behovene som er avdekket underveis i gjennomgangen. Prioriteringsområdene gir føringer for hvilke tiltak virksomheten skal iverksette innenfor bl.a. internkontroll, risikovurdering eller opplæring av og informasjon til ansatte.

3.2 Prioriteringer neste periode

Fyll inn aktiviteter ledelsen ønsker å prioritere for neste periode.

Nr.	Prioriteringsområde	Begrunnelse	Ansvarlig
1	Mulighet til å låse kontorer og plassere ut låsbare skaper der kontorplassene ikke kan låses	Risikovurdering viser at fysisk tilgang til data er en risiko	Bygn.sjef
2	Rutiner for passord	Hendelse siste år viste at etaten var sårbar	IKT-sjef
3	Inntrengingstester	Mangelfullt brannmuroppsett	IKT-sjef

Slik fyller du ut «3.3 Ledelsens konklusjon»

Her skal ledelsens oppsummere med sin konklusjon etter gjennomført Ledelsens gjennomgang. Konklusjonen skal gi føringer for videre arbeid med personvern og informasjonssikkerhet i virksomheten og supplere listen over prioriterte tiltak.

3.3 Ledelsens konklusjon

<Oppsummering fra virksomhetens leder>