FELLES - Instruks for IKT, informasjonssikkerhet og personvern - Instruks

Kommentar til versjon

Siste endring: Større revisjon av innhold, oppdaterte lenker og ansvar. Godkjent etter høringsrunde.

Formål

Denne instruksen skal sikre at kommunen opptrer og handle i tråd med gjeldende lovverk for informasjonssikkerhet og personvern. Instruksen etablerer et felles sett med sikkerhetsregler for alle som bruker kommunens IKT-systemer

Omfang/Virkeområde

Instruksen gjelder for alle ansatte i Lørenskog kommune, eksterne konsulenter, folkevalgte og andre som gis tilgang til kommunens IKT- utstyr og systemer, i eller utenfor kommunens lokaler. Dersom ikke mobiltelefon og nettbrett er nevnt eksplisitt gjelder instruksen for utlevert PC-utstyr.

Ansvar

Den som gir tilgang til kommunens IKT- utstyr og systemer, skal sørge for at den som får tilgang er kjent med instruksen. Den som får tilgang plikter å følge instruksen. Se IKT-tilgangsstyring, nettverks-bruker til LK nettverket og Tilgangsstyring- Rutine.

Aktivitet/beskrivelse

Innholdsfortegnelse (klikk for å følge lenken)

Informasjonssikkerhet og personvern/GDPR

- Hva er personvern, og hva er GDPR
- Sentrale prinsipper i GDPR er
- Personvern i IKT

- Taushetsplikt

Datasikkerhet

- Sikkerhetskopiering
- Data som brukeren selv har ansvar for
- Lagring og deling av personopplysninger i Microsoft 365
- Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger
- Utlevering av sensitive personopplysninger
- Sikring mot ondsinnet programvare og "hacking"

Bruk av elektronik postsystem (e-post)

Internett, samhandling, sosiale medier

- Internett
- Samhandling
- Retningslinjer for bruk av sosiale medier i kommunen

Tilgang til bruk av IKT-system og nettverk

- Brukernavn og passord
- Krav om to-faktors pålogging
- Oppsett og konfigurasjon av kommunens datamaskiner
- Bruk av bærbart utstyr
- Egen-eid utstyr (Bring Your Own Device)
- Reparasjon, service og vedlikehold
- Kassering av lagringsmedier
- AV-utstyr
- Eksplisitte forbudte aktiviteter
- Sikker print, kopiering og makulering
- Telefaks

Logging, sanksjoner og ansvar

- Logging
- Særlig taushetsplikt for Digitaliseringsseksjonen
- Kartlegging og utnyttelse av systemsvakheter
- Avvik
- Opphør av arbeidsforhold
- Permisjon
- Konsekvenser ved brudd på instruksen
- Definisjoner

Informasjonssikkerhet og personvern/GDPR

Kommunen behandler og forvalter store mengder personopplysninger. Mange av personopplysningene er sensitive, og vi er avhengige av at den som gir opplysninger til kommunen har tillit til at vi forvalter all informasjon på en god og trygg måte.

Personopplysningsloven (POL) med personopplysningsforskriften og annen lovgivning stiller strenge krav til hvordan Lørenskog kommune håndterer personvern og informasjonssikkerhet.

Arbeidet med informasjonssikkerhet i kommunen er organisert gjennom styringssystemet for informasjonssikker som blant annet inkluderer definisjon av mål, roller og rutiner. Kommunen har et uavhengig personvernombud som skal passe på at personvernet blir ivaretatt, og som kan hjelpe innbyggere, ledere og ansatte med spørsmål om personvern i kommunen.

Alle ansatte i kommunen har ansvar for å ivareta informasjonssikkerhet og personvern. For at du skal kunne ivareta ansvaret, har kommunen en rekke instrukser, retningslinjer og rutiner, som du finner samlet i Compilo. I tillegg har kommunen utarbeidet flere e-læringskurs som alle ansatte skal gjennomføre. I dette ligger også et ansvar for å bidra til at sensitiv informasjon ikke spres.

Tilbake til innholdsfortegnelsen

Hva er personvern, og hva er GDPR?

Norge innarbeidet i 2018 EUs fellespersonvernforordning, General Data Protection Regulation (GDPR) i personopplysningsloven. GDPR innebærer at innbyggerne i Europa får sterkere rettigheter og kontroll med hvordan data om en selv brukes.

Tilbake til innholdsfortegnelsen

Sentrale prinsipper i GDPR er:

1) Enhver innhenting og behandling av persondata skal være lovlig/ha lovhjemmel, og den skal foregå på en måte som er rettferdig og forutsigbar for den registrerte.

2) Data skal kun brukes til uttrykkelig angitte og legitime formål. Bruk som går utover dette formålet, krever samtykke fra den registrerte. Samtykke kan gis i samtykkeskjema, ansettelsesavtale e.l.

3) Det skal ikke samles inn eller lagres mer personinformasjon enn det som er nødvendig for formålet (dataminimering). Overskuddsinformasjon skal slettes.

4) Personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for.

5) Personopplysninger skal være korrekte, og de skal behandles slik at opplysningenes integritet og fortrolighet beskyttes.

Tilbake til innholdsfortegnelsen

For kommunen innebærer dette at:

1) Vi skal ha oversikt over hva vi har av personopplysninger, og hvorfor vi har dem (hjemmel og formål).

2) Vi skal ha oversikt over persondata og sikre trygg behandling og lagring.

3) Vi skal ha god oversikt over hvem som håndterer personopplysninger og har ansvar for opplysningene.

4) Vi skal utvikle en god sikkerhetskultur og bevissthet.

5) Vi skal følge kommunens personvernerklæring

Tilbake til innholdsfortegnelsen

Personvern i IKT

Ved behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler skal denne instruksen følges.

Hvis en bruker ønsker å registrere personopplysninger, plikter vedkommende å forsikre seg om at det er adgang til dette etter personopplysningsloven og forskrifter gitt med hjemmel i loven.

Informasjonssikkerhetsansvarlig, personvernombud eller nærmeste leder vil kunne gi nærmere opplysninger og være rådgiver i spørsmål omkring lovverk og beskrivelser som defineres i styringssystemet for informasjonssikkerhet i Compilo.

Tilbake til innholdsfortegnelsen

Taushetsplikt

Alle ansatte og andre som gis tilgang til kommunens IKT- systemer har taushetsplikt. Se rutine for taushetserklæring.

Tilbake til innholdsfortegnelsen

Datasikkerhet

Den enkelte bruker er selv ansvarlig for å klassifisere data og lagre disse i henhold til retningslinjer og regler for datakategorien. Data som er av verdi for Lørenskog kommune skal lagres på godkjente områder og i systemer der det blir tatt sikkerhetskopi, se Compilo: FELLES - Lagringsrutine for dokumentasjon.

Kommunen eier alle data som er fremkommet som en del av den løpende driften.

- Lagring av data med sensitive personopplysninger skal alltid lagres i kommunens godkjente sikker sone.
- Saksbehandling skal foregå i saksbehandlingssystemet. Her er det varig sikring av integritet og tilgjengelighet (sikkerhetskopiering).
- Der data behandles utenfor Lørenskog kommunes nettverk, skal det alltid foreligge databehandleravtale. Databehandleravtalen skal blant annet beskriver tjenesten og tilhørende sikkerhetsmekanismer. Noen eksempler på dette er sikkerhetskopiering, logging, antivirus mv.
- Bruker skal ikke gi andre adgang til å benytte tildelt IKT-utstyr, og skal heller ikke benytte eksterne fysiske lagringsmedier (f.eks USB-minnepenner) som ikke er kontrollert og godkjent av Digitaliseringsseksjonen. Eventuell privat bruk av kommunens IKT-utstyr skal ikke gå ut over kommunens oppgaver og funksjoner, og skal ikke gjøres dersom det krever stor lagringsplass. Følgende er gjeldende:

- Noe privat bruk tillates, inkludert mindre mengder e-post, nyheter og opplysningstjenester. Dette må imidlertid ikke påvirke jobbrelaterte oppgaver, eller være i strid med denne instruks, lover eller allmenne normer for oppførsel og sosial atferd. Privat e-post som lagres skal legges i mappe merket “Privat”.
- Mindre mengder private filer kan lagres i egen katalog på personlig område i kommunens nett, forutsatt at katalogen er merket "privat". Av kapasitetshensyn skal ikke private bilder, video, musikkfiler eller tilsvarende lagres.

Tilbake til innholdsfortegnelsen

Sikkerhetskopiering

For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på, eventuelt kopieres til, Microsoft 365 eller egnet fagsystem.

For jobb-PC som benyttes i forbindelse med reiser og hjemmearbeid, må fjerntilgang benyttes.

Ved behov for gjenoppretting av sikkerhetskopiert informasjon, kontakt IKT brukerstøtte.

Tilbake til innholdsfortegnelsen

Data som brukeren selv har ansvar for

Kommunen er ikke ansvarlig for sikkerhetskopiering av data på IKT-utstyr som brukes lokalt av den enkelte bruker (for eksempel av lokale harddisker og mobilt IKT-utstyr) og eksterne, lokale lagringsenheter som USB "minnepinner" og harddisker. Brukeren må derfor selv treffe de tiltak som er nødvendige for å unngå tap av data, programmer eller lignende på slike enheter. Dette gjelder også ved bytte av datamaskin.

Tilbake til innholdsfortegnelsen

Lagring og deling av personopplysninger i Microsoft 365

Personopplysninger skal som hovedregel lagres og behandles i fagsystemer.

Ved deling av personopplysninger i tjenester i Microsoft 365 (bl.a. OneDrive og Sharepoint) skal det nøye vurderes hvem det deles med og at taushetsplikten blir ivaretatt. Ved deling til feil person skal delingen oppheves umiddelbart.

Sensitive personopplysninger og 11-siffret fødselsnummer skal uansett ikke lagres eller deles i tjenester i Microsoft 365.

Tilbake til innholdsfortegnelsen

Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger

Som ansatt vil du kunne ha tilgang til mer opplysninger enn du trenger for å utføre ditt arbeid. Det er forbudt å aktivt søke etter personopplysninger og annen taushetsbelagt informasjon, f.eks. informasjon om ansatte, familiemedlemmer og kjente personer, uten at dette er nødvendig for ditt arbeid (tjenestlig behov).

Tilbake til innholdsfortegnelsen

Utlevering av sensitive personopplysninger

Utlevering av sensitive personopplysninger kan kun gjøres dersom det foreligger hjemmel.

Tilbake til innholdsfortegnelsen

Sikring mot ondsinnet programvare og "hacking"

Lørenskog kommune har sentrale systemer som stopper de fleste angrep på kommunens IKT-systemer. Angrep kan likevel slippe gjennom disse sikringene.

Det påhviler derfor den enkelte bruker å være aktsom ved bruk av kommunens IKT-utstyr og bidra i sikringen av dette ved å:

- Til enhver tid å ha IKT-utstyret med nyeste godkjente versjoner av programvare.
  - Antivirusprogram oppdateres automatisk
  - Operativsystemet oppdateres automatisk for sikkerhetskritiske oppdateringer.
- ALDRI oppgi brukernavn og passord annet enn ved pålogging i systemer og bytte av passord på kommunens sider for dette.
- Ikke omgå sikkerhetsmekanismer Lørenskog kommune har implementert på IKT-utstyret (for eksempel rettigheter tildelt brukeren).
- Ikke benytte programvare som ikke er godkjent av kommunen.

- Være kritisk til vedlegg og lenker i e-post.
- Være kritisk til innhold og lenker på nettsider.
- Unngå bruk av usikrede trådløse (gjeste)nett.

Digitaliseringsseksjonen kan uten varsel utestenge brukere som sprer ondsinnet programvare eller utgjør annen sikkerhetsrisiko for IKT-utstyret i kommunen. Kontakt IKT Brukerstøtte øyeblikkelig ved mistanke om at IKT-utstyret er angrepet av virus e.l.

Dersom kommunens IKT-utstyr rammes av et omfattende angrep som påvirker hele nettverket, kan kommunen uten forhåndsvarsling av brukerne stenge hele eller deler av nettverket til situasjonen er avklart og eventuelle skadevirkninger rettet. En slik stenging skal godkjennes av driftsansvarlige ved Digitaliseringsseksjonen.

Tilbake til innholdsfortegnelsen

Bruk av elektronisk postsystem (e-post)

Kommunens elektroniske postsystem er kommunens eiendom.

- Arbeidsgiver har tilgang til all e-post som befinner seg i systemet, eller blir sendt til og fra systemet. Arbeidsgiver kan kun i spesielle tilfeller gå inn e-postkassen og lese epost. etter nærmere regler. Se Innsyn i ansattes e-post mv.
- Brukeren har selv ansvar for å opprette egen mappe som er tydelig merket «privat», for lagring av privat e-post.
- Det er kun tillatt å hente privat e-post igjennom web-baserte e-posttjenester
- E-post skal ikke benyttes for overføring av sensitive personopplysninger eller 11-sifret fødselsnummer. E-post kan benyttes om vedlegg er kryptert med tilstrekkelig krypteringsstyrke.
- Ved planlagt fravær utover tre dager skal den ansatte selv sørge for at det sendes automatisk svar til avsender om at vedkommende ikke er å treffe og at virksomhetsrelatert e-post skal sendes til kommunen på adressen: *postmottak@lorenskog.kommune.no* eller annen kommunal e-post det er gjort avtale om.
- Lørenskog kommunes Post- og arkivrutiner gjelder også for arkivering av e-post. Se Arkivplan
- Du skal fortløpende behandle e-post du mottar på din kommunale e-postadresse.
- All arbeidsrelatert e-postkommunikasjon skal kun skje via din Lørenskog kommune-konto.
- Det er forbudt å sette opp automatisk videresending av e-post fra Lørenskog kommune-konto til e-posttjenester som ikke driftes av Lørenskog kommune.
- Å sende e-post fra din Lørenskog kommune-konto er å betrakte som å sende et brev med Lørenskog kommunes brevhode og representere Lørenskog kommune. E-post skal derfor benyttes til tjenstlig kommunikasjon og bare unntaksvis til kommunikasjon av privat karakter. Eksempler på slik kommunikasjon er e-post av privat og praktisk karakter til nær familie.
- Søppel-post, kjedebrev og liknende tillates ikke distribuert/videreformidlet.
- Det er forbudt å registrere Lørenskog kommunes e-postadresse til private tjenester.
- Lenker og vedlegg kan inneholde skadelig programvare. Tenk deg om før du åpner en e-post eller klikker på lenker eller filer i e-post. Du skal ikke åpne vedlegg og lenker i e-post, med mindre e-posten kommer fra en avsender det er rimelig å forvente ønsker saklig kontakt med deg eller Lørenskog kommune.

Kontroller alltid at en lenke er hva den utgir seg for, ved å føre musepekeren over lenken og verifisere at lenken går til et nettsted som virker sannsynlig/fornuftig. Husk at myndigheter og banker som regel aldri kommuniserer via åpen e-post.

Lørenskog kommune har et automatisert system for kontroll og filtrering av uønsket e-post (spam).

Din e-post-konto skal ikke brukes som et saksarkiv. Arkivloven og personvernlovgivningen pålegger deg å lagre e-post i saks- eller fagsystemer og slette e-post fra kontoen din når det er lagret i andre system eller ikke lenger er relevante.

Lørenskog kommune kan om det vurderes nødvendig, lage mekanismer for styring og sletting av e-post. Se for øvrig Lørenskog kommunes arkivplan for epost: Arkivplan

Tilbake til innholdsfortegnelsen

Internett, Samhandling, Sosiale medier

Internett

Alle ansatte har som et utgangspunkt tilgang til å benytte Internett fra kommunens IKT-utstyr.

Det er ikke tillatt å laste ned utuktig materiale, opphavsrettslig beskyttet materiale eller annet som er i strid med lovverket.

Tjenester for privat fildeling tillates ikke på grunn av sikkerhetsrisiko knyttet til disse tjenestene.

Ressurskrevende tjenester, eksempelvis radiolytting og TV/video-strømming, skal begrenses for ikke å påvirke negativt jobbrelatert trafikk i nettet.

Kommunen har anledning til å logge informasjon om Internett- og e-posttrafikk for å sikre alminnelig drift samt for sporing ved eventuelle sikkerhetsbrudd.

Tilbake til innholdsfortegnelsen

Samhandling

- All intern samhandling går gjennom de verktøy Lørenskog Kommune tilbyr, som er Microsoft Outlook, Microsoft Yammer og Microsoft Teams.
- Det er ikke tillatt å sette opp grupper og lignende i for eksempel Facebook og kommunisere på slike plattformer for jobbrelatert samhandling.

Tilbake til innholdsfortegnelsen

Retningslinjer for bruk av sosiale medier i kommunen

Se dokumentet Veileder for bruk av sosiale medier i Lørenskog kommune.

Tilbake til innholdsfortegnelsen

Tilgang til og bruk av IKT-utstyr og nettverk

Brukernavn og passord

- Alle brukere skal ha eget brukernavn og passord. Se Krav til passord og Endre passord.
- Ditt personlige passord til Lørenskog kommune skal ikke oppgis til andre. Må du skrive ned passordet ditt så oppbevar dette som et verdipapir
- Bruk et eget passord til din brukerkonto i kommunen, og ikke det samme passordet som du bruker på tjenester utenfor (for eksempel på privat e-post eller sosiale medier).
- Dersom du har mistanke om at passordet har blitt kjent av uvedkommende, skal passordet byttes og hendelsen rapporteres som et avvik i Compilo.
- Når man forlater datamaskinen skal maskinen låses umiddelbart (Windowstasten + L).

Du skal alltid logge ut før du overlater maskinen til andre.

Tilbake til innholdsfortegnelsen

Krav om to-faktors pålogging

To-faktor pålogging skal aktiveres der dette er mulig, på alle Lørenskog kommune tilknyttede kontoer.

I tillegg til brukernavn og passord vil det kreves bruk av to-faktor pålogging (dobbel pålogging) når man logger på følgende tjenester:

Krav om to-faktors pålogging til Microsoft 365

Tilbake til innholdsfortegnelsen

Oppsett og konfigurasjon av kommunens datamaskiner

Du har ikke lov til å installere ny programvare eller endre oppsett av datamaskinen. Dette skal gjøres av eller etter avtale med, IKT-enheten. Bevisste forsøk på å omgå logiske eller tekniske sikringstiltak, vil oppfattes som sikkerhetsbrudd og avvik skal rapporteres.

Det er ikke tillatt å benytte privat utstyr av noe slag i kommunens interne kablede nettverk. Dette inkluderer, men er ikke begrenset til, nettbrett, mobiltelefon, kamera, minnekort og minnepenn.

Eksterne konsulenter og vikarer skal ikke koble til egen PC i kommunens interne kablede nettverk, men få maskin av kommunen hvis de skal ha tilgang til fagsystemer og det interne nettet i Lørenskog kommune. Unntak for dette skal avtales med IKT-enheten.

Det skal ikke tilkobles separate eksterne forbindelser til kommunens nettverk (for eksempel via ekstra nettverkskort, trådløs forbindelse, aksesspunkt, modem og lignende). Nettverkskort med direkte tilgang til eksterne nett/Internett skal aldri tilkobles.

Tilbake til innholdsfortegnelsen

Bruk av bærbart utstyr

Beskyttelsesverdig informasjon skal ikke lagres på bærbar PC, nettbrett eller annet portabelt utstyr med mindre det er installert godkjente sikkerhetsløsninger (normalt med kryptert lagringsenhet).

Bærbar PC (jobb-PC), telefon og nettbrett som forvaltes i kommunens utstyrshåndteringssystem (Mobile Device Management - MDM) kan benyttes for fjerntilgang til kommunens nettverk i forbindelse med jobb på reiser, hjemme og ved besøk hos bruker/pasient. Dette gjøres via en kryptert VPN-løsning. Det er leders ansvar å godkjenne en slik tilgang. Legges under bærbart utstyr

Bærbar PC, telefon, nettbrett eller annet bærbart utstyr skal ikke ligge synlig uten tilsyn.

Tilbake til innholdsfortegnelsen

Egen-eid utstyr (Bring Your Own Device)

Egen-eid mobiltelefon eller andre lignende enheter (BYOD) som ønskes benyttet for å få tilgang på skytjenester tilknyttet M365 tillates, men bruker kan ikke påberegne support fra brukerstøtte.
Det stilles samme krav til innlogging og tilgang til tjenestene som en enhet eid av Lørenskog kommune (Mobile Device Management - MDM) og Krav om To-faktors pålogging til Microsoft 365

Tilbake til innholdsfortegnelsen

Reparasjon, service og vedlikehold

Alle feil eller mistanker om feil i informasjonssystemet (både maskinvare og programvare) skal rapporteres til IKT brukerstøtte snarest mulig.

Det er kun IKT brukerstøtte som kan iverksette arbeid som utføres av eksternt personell på datasystemer og utstyr.

Tilbake til innholdsfortegnelsen

Kassering av lagringsmedier

Disker, utstyr som inneholder lagringsenheter og annet lagringsmateriale (f.eks. pc, telefon, nettbrett etc.), skal leveres til IKT brukerstøtte for forsvarlig destruksjon.

Tilbake til innholdsfortegnelsen

AV-utstyr

Kommunens AV-utstyr er tett integrert med øvrig IKT-utstyr for å kunne opereres enkelt og hensiktsmessig. For å sikre stabil drift er det ikke lov til å demontere, trekke ut eller fjerne kabler fra kommunens IKT/AV-utstyr.

Tilbake til innholdsfortegnelsen

Eksplisitte forbudte aktiviteter

Følgende aktiviteter er strengt forbudt på kommunes IKT-utstyr:

- Låne ut, dele eller stille til disposisjon eget brukernavn og passord til andre. Dette gjelder også ved bruk av utstyret utenfor kommunens nettverk, herunder også til familiemedlemmer/venner.
- Bruke IKT-utstyret med annet enn egen brukerkonto, selv om en har tillatelse fra vedkommende til dette.
- All bruk av verktøy som brukes til kartlegging av nettverk og trafikk på nettverk (eksempelvis "sniffere", nettverksanalysatorer og lignende).
- Forsøk på å omgå sikkerhetsbarrierer for å oppnå tilgang til andres data, programmer med mer. Dette gjelder også om det skulle vise seg teknisk sett å være åpen adgang til områder som brukeren må forstå at han/hun ikke skal ha adgang til. Blir brukeren oppmerksom på at slik åpen adgang finnes, skal dette umiddelbart meldes til IKT-avdelingen.
- Bruk av fildelingsverktøy for nedlastning og distribusjon av data.
- Installere og bruke programvare som ikke er godkjent av IKT-avdelingen.

Unntatt fra disse reglene er ansatte i IKT-avdelingen når dette er nødvendig på grunn av brukerstøtte eller driftstekniske forhold.

Tilbake til innholdsfortegnelsen

Fjerntilgang

Ansatte kan få tilgang til interne systemer og ressurser. Dette gjøres via en kryptert VPN-løsning. Det er leders ansvar å godkjenne en slik tilgang.

Tilbake til innholdsfortegnelsen

Sikker print, kopiering og makulering

- Ikke legg igjen dokumenter på kopimaskin/skriver.

- Dokumenter eller notater med sensitivt innhold skal kastes skal alltid makuleres. Bruk makuleringsmaskin eller låst kontainer for sikkerhetsmakulering.
- Utskriften eller kopitjenesten skal kan ikke gjennomføres før brukeren har autentisert seg med kort eller kode på en angitt printer i løsningen (sikker print).

Tilbake til innholdsfortegnelsen

Telefaks

Telefaks skal ikke benyttes til oversendelse av sensitive personopplysninger eller 11-siffret fødselsnummer uten at det er av stor betydning for ytelsen til den registrerte.

Tilbake til innholdsfortegnelsen

Logging, sanksjoner og ansvar

Logging

Lørenskog kommune bruker ulike metoder for logging og overvåking av informasjonssystemene for å hindre informasjonstap og driftsforstyrrelser, samt for å avdekke interne og eksterne forsøk på å omgå sikkerhetsmekanismer.

Ved behov for identifisering av databrukere i kommunen, gjøres dette etter spesielle retningslinjer for behandling av logger.

Tilbake til innholdsfortegnelsen

Særlig taushetsplikt for IKT-ansatte

IKT-ansatte har en særlig taushetsplikt om en bruker eller brukerens virksomhet som følge av loggføring og overvåking av IKT-systemene. Unntaket er forhold som kan representere brudd på dette reglementet og norsk lov. Slike forhold meldes i avvikssystemet.

Tilbake til innholdsfortegnelsen

Kartlegging og utnyttelse av systemsvakheter

Ansatt i kommunen skal ikke på eget initiativ foreta kartlegging eller testing av mulige systemsvakheter, forsøke å trenge inn i interne eller eksterne systemer, forsøke å forbigå etablerte sikkerhetsmekanismer, tilegne seg utvidede tilgangsrettigheter på lokal maskin eller utnytte eventuelle sikkerhetssvakheter. Mistenker ansatte systemsvakheter skal disse meldes slik det fremgår under overskriften Avvik.

Tilbake til innholdsfortegnelsen

Avvik

Avvik fra regler og krav til informasjonssikkerhet og personvern skal behandles iht. kommunens avviksrutiner i Compilo hvor Informasjonssikkerhet og personvern/GDPR er definert som en egen avvikskategori.

Ethvert brudd på lov, forskrift eller interne retningslinjer og instrukser skal rapporteres snarest for om mulig å minimere skadeomfang og unngå gjentagelser.

Alle ansatte skal melde avvik når de oppdager brudd på sikkerhetstiltak og/eller når oppgaver er utført i strid med de rutinene som er besluttet.

Å melde avvik er utrykk for en sikkerhetskultur hvor de ansatte bidrar til tilfredsstillende informasjonssikkerhet i hele kommunen. Det er viktig at du som ansatte i kommunen, er bevisst ditt og kommunens ansvar for å sikre personvernet i det daglige arbeidet.

Behandling av personopplysninger og bruk av kommunens IKT-løsninger i strid med gjeldende lovverk og kommunens retningslinjer, kan medføre tjenstlige reaksjoner overfor den ansatte.

Tilbake til innholdsfortegnelsen

Opphør av arbeidsforhold

Ansatt som slutter skal levere alt utlevert IKT-utstyr og mobiltelefon, dersom ikke annet er avtalt.

Ansatt som slutter, skal rydde i egne filområder og e-post og sikre at all relevant informasjon blir lagret i tråd med gjeldende rutiner. Ansatt har ansvar for at gjenværende informasjon på brukerens område slettes innen ansettelsesforholdet er avsluttet. Arkivverdig informasjon skal lagres i kommunens sak/arkivsystem.

Ansatt som slutter, skal makulere eller avlevere egne dokumenter som beskrevet i punktet ovenfor.

E-post og personlig filområde vil bli slettet automatisk ved endt arbeidsforhold.

Tilbake til innholdsfortegnelsen

Permisjon

Ansatt som går ut i permisjon kan fortsatt bruke IKT utstyret sitt i permisjonstiden hvis ikke annet er avtalt med leder. Den ansatte i permisjon deaktiveres ikke i noen systemer, men blir bedt om å endre passord på samme måte som alle andre. Brukes ikke pålogging går passord ut.

Tilbake til innholdsfortegnelsen

Konsekvenser ved brudd på instruksen

Konsekvenser for ansatte som har forårsaket brudd på sikkerhetsreglene, vil bli vurdert i hvert enkelt tilfelle og kan ved alvorlige brudd føre til oppsigelse/avskjed.

Tilbake til innholdsfortegnelsen

Definisjoner på informasjonssikkerhet

Tilbake til innholdsfortegnelsen

Alle gjennomførende rutiner for IKT og teknologi finner du i denne mappen i Compilo:
https://x09.ksx.no/system.php?item=9877&ok=pjzhfvtb2rn0d8w

Definisjoner

Definisjoner

Hjemmel

Forskrift:
eForvaltningsforskriften
KAP 3

Referanser

styringssystem, informasjonssikkerhet, personvern, internkontroll, ansvar,