IKT-REGLEMENT

for ansatte i kommuner og interkommunale selskaper
i DDV-samarbeidet

Versjon: 1.2

Dato: 26. april 2024

REGLER FOR IKT-BRUKERE

Dette reglementet gjelder for bruk av IKT-ressurser levert av DDV. Med IKT-ressurser menes i denne sammenheng alle typer IKT-utstyr, inkludert programvare, skyløsninger, PC-er, mobiltelefoner, nettbrett og tilhørende tilleggsutstyr. Reglementet gjelder så lenge man er ansatt i kommunen.

Brukerne av IKT-systemene har plikt til å sette seg inn i gjeldende regler og tiltak for å oppnå god informasjonssikkerhet. For sikret informasjon, som for eksempel sensitive personopplysninger, enkelte virksomheter og systemer, kan det forekomme ekstra krav, rutiner og retningslinjer.

Tilgang til informasjon

Ansatte skal ha tilgang til den informasjon som man har tjenstlig behov for. Tilgang gjøres gjennom autorisasjon fra nærmeste leder. Dersom man oppdager tilgang til informasjon som man ikke har tjenstlig behov for, meldes dette til nærmeste leder umiddelbart. Det er ikke tillatt å søke opp opplysninger i systemer som man ikke har tjenstlig behov for.

Utarbeidelse, behandling og lagring av informasjon

Bruk av IKT-ressurser skal ikke være i strid med virksomhetens etiske retningslinjer. Innsamling og systematisering av data, herunder personopplysninger, som ikke inngår som en del av brukerens naturlige arbeidsområde eller tjenstlig behov, er ikke tillatt.

IKT-utstyr

PC-er og nettbrett som benyttes i tjenesten skal være godkjent av DDV. Ved avslutning av arbeidsforhold skal alt utstyr eid av virksomheten returneres til nærmeste leder.

Når en PC forlates skal den låses, logges av, eller sikres med passordbeskyttet skjermsparer.
Bruk WIN+L for å låse PC.

PC-er:

- En PC eid av arbeidsgiver skal kun benyttes til tjenstlige formål av pålogget bruker.
- Den enkelte bruker har ikke lov til å installere programvare på PC-en, annet enn det som ligger tilgjengelig for nedlasting i programvaresenteret.
- Brukeren må påse at konfidensiell informasjon ikke lagres på PC. Informasjon lagret lokalt på PC vil kunne leses av uvedkommende ved tap eller tyveri.
- Ved bruk av bærbar PC på hjemmekontor eller utenfor DDVs nettverk skal tilgang skje via godkjent hjemmekontorløsning (VPN) levert av DDV. Merk at dette er spesielt viktig ved bruk av åpne WiFi-nett.
- PC-er beskyttes med brannmur og oppdatert antivirusprogram, og må derfor omstartes jevnlig, helst daglig.

Mobiltelefoner og håndholdte enheter:

- Enheter som kan inneholde virksomhetsrelatert informasjon skal beskyttes ved passord, pin-kode e.l.
- Enheter skal ikke inneholde sensitiv informasjon.

Eksterne lagringsmedier:

Eksterne lagringsmedier, som for eksempel USB-baserte minnepinner, skal ikke inneholde konfidensiell eller sensitiv informasjon. Brukeren skal være kritisk til hva som lagres på slike medier og hvordan disse oppbevares.

Prinsipper for lagring av data

DDV har utarbeidet en rutine for hva som kan lagres hvor. Alle ansatte plikter å sette seg inn i denne.

Regler for bruk av e-post

Generelt

- E-post som er lagrings- eller arkivverdig skal lagres iht. regler for arkivering og journalføring, jfr. Arkivforskriften § 3-2.
- Virksomhetsrelatert e-post skal avsluttes med signatur.
- Ved planlagt fravær skal det legges inn automatisk fraværsmelding i Outlook.
- Kontroller mottaker adressene, også adressegrupper, slik at utilsiktet distribusjon av e-post unngås.
- Automatisk viderekobling av e-post til eksterne adresser, herunder private e-postadresser, er ikke tillatt.
- Vær obs på at e-post fra virksomhetens avsender kan oppfattes som å inneholde virksomhetens offisielle meninger.
- Vær restriktiv med å oppgi din e-post adresse, og med hva du svarer eller abonnerer på av nyhetslister og lignende. Dette for å hindre unødig risikoeksponering som virus, spam, innbruddsforsøk og lignende.

Sensitiv informasjon

- Opplysninger underlagt lovbestemt taushet etter offentlighetsloven § 2 skal ikke sendes som e-post. Herunder er blant annet opplysninger om noens personlige forhold og andre taushetsbelagte opplysninger etter forvaltningsloven § 13.
- Personopplysninger som røper enkeltpersoners klientforhold skal ikke sendes som e-post.
- Personnummer og sensitiv informasjon skal ikke sendes på e-post.

Privat bruk

- Det er en etisk utfordring at man framstår som kommunalt ansatte i private sammenhenger.
- Privat e-post skal ikke inneholde tekst som kan knytte innholdet til arbeidsgiver, eller medvirke til at private meninger tillegges denne.
- Kommunal e-postadresse skal ikke brukes som pålogging til private nettbaserte tjenester.
- Ansatte bør jevnlig slette gamle e-poster for å redusere størrelsen på epostkontoen.

Regler for bruk av Internett

- Den ansatte må selv være oppmerksom på trusler fra Internett, og bidra til at disse utgjør en lavest mulig risiko.
- Bruk av internett blir logget og overvåket av drifts- og sikkerhetsmessige årsaker.
- All bruk av internett fra DDVs systemer kan spores tilbake til virksomheten. Privat bruk tillates derfor kun i begrenset omfang, og innenfor virksomhetens normer.
- Det er ikke tillatt å besøke sider som strider mot nasjonale straffebestemmelser eller som på annen måte kan virke støtende eller krenkende.
- Nedlastning og distribusjon av programfiler og annen data som ikke er forretningsmessig eller virksomhetsrelatert skal unngås.

Regler for passord

- Passord skal beskytte virksomhetsrelatert informasjon og er ikke ment som beskyttelse av private handlinger, data og informasjon.
- Passord er strengt personlig, og det er forbudt iht. norsk lov å utlevere dette til andre.
- Passord skal ikke oppbevares på arbeidsplassen, eller sammen med utstyr hvor passord benyttes.
- Det er ikke tillatt å benytte andre personers brukeridentitet og passord.
- Ved mistanke om at passordet er blitt kjent, skal dette straks endres.
- Ved mistanke om at passord er blitt misbrukt, skal dette rapporteres umiddelbart i til DDV.
- For å hindre eksponering av passord i eksterne miljø, skal passord som benyttes i virksomhetens systemer ikke brukes i eksterne eller private sammenhenger.

Se ellers passordpolicy for DDV-samarbeidet.

Utskrifter

Brukere må påse at utskrifter ikke blir liggende på skrivere slik at uvedkommende kan få tilgang. «FollowMe print» skal benyttes når mulig.

Informasjonsbehandling i omgivelsene

- Vær bevisst på hvor du legger igjen dokumentasjon og informasjon.
- Vær bevisst på hva og til hvem du meddeler informasjon.
- Vær bevisst ved muntlig omtale av personopplysninger og forretningsmessige verdier.
- Konfidensielle dokumenter, papirbasert, skal makuleres ved destruksjon.
- Rydd arbeidsplassen din jevnlig for å holde oversikt over hva du har av dokumenter og informasjon tilgjengelig.

Arbeidsgivers rettigheter

Virksomhetene har som policy å ikke overvåke den enkeltes bruk av e-post eller internett, men i spesielle situasjoner har arbeidsgiver rett til innsyn. Dette kan for eksempel være ved lengre fravær og tilgang til e-postkassen er nødvendig for å ivareta den daglige driften. Sikkerhetslogger kan inneholde informasjon om trafikk knyttet til enkeltpersoner. Disse sikkerhetsloggene gjennomgås jevnlig av DDV, og ved mistanke om sikkerhetsbrudd vil logger for ansatte kunne bli vurdert.

Vi viser til utfyllende informasjon i «Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale».

Den ansattes plikter

Regler, retningslinjer og rutiner

Den ansatte skal gjøre seg kjent med og følge de til enhver tid gjeldende regler for IKT-ressurser levert av DDV. Oppdaterte regler og rutiner vil være tilgjengelig i opplæringsportalen.

Alle ansatte får IKT-reglementet på sin leseliste, og ved fullført lesing anses IKT-reglementet som lest og forstått.

Overtredelse av reglementet regnes som et tillitsbrudd mellom den ansatte og arbeidsgiver, og kan i alvorlige tilfeller gi grunnlag for oppsigelse/avskjed. Ved mistanke om straffbare forhold kan dette bli politianmeldt.

Ved avslutning av arbeidsforhold

Ved avslutning av arbeidsforhold må den ansatte rydde opp i e-postkassen og filer lagret på personlig område, samt sørge for at opplysninger overføres til arkiv eller til rett person i virksomheten. Nærmeste leder sørger for at den ansatte slettes som bruker av alle fagsystem, og melder fra til DDV, som sletter den ansatte som bruker. Ved dødsfall slettes personlig e-postkasse og private filer, med mindre det er sannsynlig at politiet vil ønske innsyn i opplysningene. Før sletting kan arbeidsgiver sortere ut virksomhetsrelatert e-post i tråd med «Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale».