IKT-REGLEMENT

for folkevalgte i DDV-kommunene

Versjon: 1.0

Dato: 18. oktober 2023

REGLER FOR FOLKEVALGTE 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 folkevalgt i kommunen.

Brukerne av IKT-systemene har plikt til å sette seg inn i gjeldende regler og tiltak for å oppnå god informasjonssikkerhet.

Tilgang til informasjon

Folkevalgte skal ha tilgang til den informasjon som man har tjenstlig behov for. Dersom man oppdager tilgang til informasjon som man ikke har tjenstlig behov for, meldes dette til politisk sekretariat 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 politisk verv skal alt utstyr eid av virksomheten returneres til politisk sekretariat.

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

PC-er og nettbrett:

- En PC / et nettbrett 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.
- På nettbrett skal man kun bruke app-er som er relevante for å utføre sitt politiske verv. DDV anbefaler å ikke laste ned TikTok og Telegram.
- Brukeren må påse at konfidensiell informasjon ikke lagres lokalt. Informasjon lagret lokalt 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.
- Både PC-er og nettbrett må holdes oppdatert.

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 skal kun benyttes til politisk informasjonsutveksling.
- Kontroller mottakeradressene, 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.

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.

Regler for bruk av Internett

- Den folkevalgte 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.

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.

Kommunens rettigheter

Virksomhetene har som policy å ikke overvåke den enkeltes bruk av e-post eller internett, men i alvorlige situasjoner har kommunen rett til innsyn. Sikkerhetslogger kan inneholde informasjon om trafikk knyttet til enkeltpersoner. Disse sikkerhetsloggene gjennomgås jevnlig av DDV, og ved mistanke om sikkerhetsbrudd vil logger for brukere kunne bli vurdert.

Den folkevalgtes plikter

Regler, retningslinjer og rutiner

Den folkevalgte 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.

Overtredelse av reglementet regnes som et tillitsbrudd. Ved mistanke om straffbare forhold kan dette bli politianmeldt.

Ved avslutning av politisk verv

Ved avslutning av politisk verv må den folkevalgte rydde opp i e-postkassen og filer lagret på personlig område. Politisk sekretariat sørger for at den folkevalgte slettes som bruker av alle fagsystem, og melder fra til DDV, som sletter den ansatte som bruker.