IKT-REGLEMENT

for alle ansatte i DDV-samarbeidet

Versjon: 1.3

Dato: 28. august 2026

Regler for IKT-brukere

IKT-reglementet gjelder for alle ansatte som bruker IKT-ressurser levert av DDV. Med IKT-ressurser menes PCer, mobiltelefoner, nettbrett, programvare, skyløsninger og annet relevant utstyr. Målet er å sikre trygg behandling av arbeidsgivers informasjon og gi rammer for sikker, forsvarlig og effektiv bruk av digitale tjenester.

Ansvar og grunnprinsipper

Som ansatt skal du følge gjeldende regler og rutiner for bruk av IKT-ressurser. Alle ansatte plikter å sette seg inn i tiltak som bidrar til god informasjonssikkerhet, og enkelte systemer eller typer informasjon kan ha egne tilleggskrav.

Du skal bare bruke informasjon du har tjenstlig behov for, og melde fra til leder hvis du oppdager tilgang du ikke skal ha.

Behandling og lagring av informasjon

Informasjon skal behandles i tråd med arbeidsgivers etiske retningslinjer, og ansatte skal ikke samle inn eller systematisere data utover det tjenesten krever.

Konfidensiell og sensitiv informasjon skal behandles spesielt varsomt – tenk igjennom hva du lagrer hvor. Alle ansatte skal følge DDVs lagringsstrategi og sette seg inn i hva som kan lagres hvor.

Bruk av PC og annet arbeidsutstyr

PC og nettbrett brukt i tjenesten skal være godkjent av DDV, og skal leveres tilbake ved endt arbeidsforhold.

Når du forlater PC-en, skal den låses eller sikres med passordbeskyttet skjermsparer (WIN+L). Som bruker har du ansvar for å ha kontroll på hvor utstyret befinner seg, og du må umiddelbart kontakte leder ved mistanke om sikkerhetshendelser, skade, tap eller tyveri.

Du kan ikke installere egen programvare, og du må unngå å lagre konfidensiell informasjon lokalt på PC-en.

Når du jobber utenfor DDVs nettverk, skal du bruke DDVs godkjente VPN-løsning, særlig ved bruk av åpne WiFi-nett.

PC-en skal startes jevnlig for å sikre oppdateringer og antivirusbeskyttelse.

Mobil og håndholdte enheter

Slike enheter skal alltid være sikret med PIN eller passord, og det skal ikke lagres sensitiv informasjon på enhetene.

Eksterne lagringsmedier

USB-minnepinner og lignende skal ikke inneholde konfidensiell eller sensitiv informasjon, og du må vurdere hva som lagres og hvordan det oppbevares.

Privat utstyr

Hovedregelen er at du skal bruke utstyr du har fått av arbeidsgiver når du arbeider med kommunal informasjon. Privat utstyr kan brukes til enkle oppgaver, som e-post eller Office-apper, men krever ekstra varsomhet siden det ikke har samme sikkerhet som jobb-utstyr. DDV gir ikke brukerstøtte eller setter opp VPN på privat utstyr.

E-postbruk

Din jobb e-postadresse skal kun brukes til arbeidsrelaterte oppgaver og kontakt som er en naturlig del av rollen din hos din arbeidsgiver. Bruk privat e-postkonto til private bestillinger, abonnementer, registreringer, kommunikasjon m.m.

E-post som skal lagres eller arkiveres må håndteres i tråd med arkivreglene. Virksomhetsrelatert e-post skal avsluttes med signatur, og du skal bruke automatisk fraværsmelding ved planlagt fravær.

Kontroller mottakere før sending, og unngå utilsiktet deling av informasjon. Automatisk videresending til private e-postadresser er ikke tillatt, og heller ikke teknisk mulig.

Gamle e-poster bør slettes jevnlig.

Følgende skal ikke sendes på e-post:

- Sensitiv informasjon
- Personopplysninger som røper klientforhold
- Fødselsnummer og lovpålagt taushetsbelagt informasjon

Privat bruk av jobb e-post

Din jobb e-postadresse skal ikke brukes som pålogging til private tjenester, ettersom privat e-postbruk kan skape sikkerhetsrisiko og rolleblandinger.

Hvis en privat e-post sendes fra arbeidsgivers adresse, kan mottaker lett oppfatte at avsender uttaler seg på vegne av denne.

Kommunens e-postsystemer er underlagt arkivlovgivningen og innsynsregler. Å blande privat og arbeid kan gjøre dette vanskeligere å håndtere korrekt.

Bruk av Internett

All bruk av internett blir logget og kan spores tilbake til virksomheten, og privat bruk tillates kun i begrenset omfang. Ulovlige, støtende eller risikofylte nettsider er ikke tillatt, og nedlasting av filer som ikke er jobbrelevante skal unngås.

Passord

Passord er personlig og skal aldri deles med andre. Det skal ikke oppbevares skrevet ned på arbeidsplassen, og du kan ikke bruke andres identitet eller passord.

Ved mistanke om at passordet er kjent eller misbrukt, skal det endres umiddelbart og meldes 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.

DDVs passordpolicy gir utfyllende regler for passordbruk.

Utskrifter

Bruk «DDV.Utskrift» når det er mulig. Pass på at du får med deg alle arkene når du henter utskriften.

Du skal være bevisst på hvor du legger igjen informasjon, både digitalt og fysisk, og makulere konfidensielle dokumenter når de ikke lenger skal oppbevares.

Arbeidsgivers innsyn og sikkerhetslogger

Arbeidsgiver overvåker ikke løpende ansattes bruk av e-post eller internett, men kan ha innsyn i spesielle situasjoner, for eksempel ved lengre fravær eller ved mistanke om brudd på sikkerheten. Sikkerhetslogger gjennomgås jevnlig for å oppdage mistenkelig aktivitet.

Den ansattes plikter

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

Den ansatte skal rydde opp i filer og e-post, og sørge for at nødvendig informasjon arkiveres eller overføres til rette personer. Utstyr skal leveres tilbake, og leder sluttmelder den ansatte slik at tilgangene slettes. Ved dødsfall kan virksomheten sortere ut virksomhetsrelatert e-post før sletting, i tråd med «Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale».