Instruks

Informasjonssikkerhet og personvern

Instruks for bruk av kommunens IKT-løsninger

Gjelder for: Alle ansatte

Vedtatt av: Rådmannen

Dato: 20.09.2018 **JpID:** 18/30486

Dokumentansvarlig (Enhet): Interne tjenester

Revisjonsintervall: Årlig

Distribusjon: Intranett, hjemmeside, QM+

Merknad: Denne instruksen er en del av instruks «Informasjonssikkerhet for ansatte».

Innholdsfortegnelse

1. INNLEDNING

Denne brukerinstruksen er en del av "Instruks for alle ansatte – informasjonssikkerhet" og dermed en del av den grunnleggende opplæringen i informasjonssikkerhet.

Instruksen gjelder for alle ansatte og innleid personell med tilgang til kommunens IKT-løsninger.

1.1. Hensikt

Instruksen regulerer ansvar, plikter og retningslinjer for alle som benytter IKT-løsninger i Eigersund kommune.

Instruksen skal bidra til å hindre uønsket bruk av kommunens IKT-løsninger og til å styrke informasjonssikkerheten i kommunen.

1.2. Ansvarsforhold

Den enkelte ansatte er selv ansvarlig for at denne brukerinstruksen følges.

Enhetsleder er ansvarlig for å gjøre instruksen kjent for den ansatte, og påse at ingen nye ansatte får tilgang til kommunens informasjonssystemer før denne instruksen er kjent og forstått.

Brudd på instruksen håndteres i henhold til kommunens avvikshåndteringsrutiner.

Etterlevelse av denne instruksen vil bli sporadisk kontrollert gjennom kommunens internkontrollsystem.

1.3. Definisjoner

Se dokumentet "Definisjoner" som du finner her: Definisjoner – Informasjonssikkerhet og personvern.

2. BRUK AV KOMMUNENS IKT-LØSNINGER

Informasjonssikkerhet er tiltak og mekanismer for å ivareta konfidensialitet, tilgjengelighet og integritet for informasjon og systemer som behandler disse. Alle brukere plikter å sette seg inn i lover, regelverk og retningslinjer som har som formål å ivareta informasjonssikkerheten i deres daglige virke.

Brukere av kommunens IKT-løsninger skal bidra til å opprettholde sikkerhetsnivået, for eksempel ved å forhindre uautorisert tilgang til IKT-løsninger, forhindre krenking av personlig informasjon og være oppmerksom på trusler som skadelig programvare. Alle har et ansvar for informasjonssikkerheten.

Ved mistanker om hendelser som truer informasjonssikkerheten skal brukeren rapportere dette til sin leder eller til IKT-kontoret/sikkerhetsleder.

2.1. Generelt

2.1.1 IKT-utstyr som datamaskin, mobiltelefon, minnepenn osv. tildelt av Eigersund kommune skal benyttes i henhold til tjenstlig behov.

2.1.2 Datautstyr som eies av Eigersund kommune skal oppbevares slik at det er lav risiko for at det blir stjålet eller ødelagt.

2.1.3 Kommunalt IKT-utstyr skal i utgangspunktet ikke brukes av andre enn ansatte i Eigersund kommune.

2.1.4 Det er ikke tillatt å bruke kommunens IKT-løsninger til et formål som strider mot etiske og moralske normer eller som er i konflikt med norsk lov.

2.1.5 Det er ikke tillatt å bruke kommunens IKT-løsninger på en måte som legger beslag på unødvendig mye IKT ressurser (f.eks. lagringsplass, nedlasting, streaming).

2.1.6 Kun programvare lisensiert til Eigersund kommune, og som IKT-kontoret har godkjent, kan benyttes på kommunens datautstyr og nettverk. Evt. andre behov må meldes til IKT Brukerhjelpen.

2.1.7 Kopiering av programvare til privat bruk uten tillatelse er forbudt.

2.1.8 Ondsinnet eller skadelig programvare skal ikke kjøres med hensikt på kommunalt IKT-utstyr.

2.1.9 Det er ikke tillatt for brukere å selv installere programvare på terminalservere i kommunens nett. Evt. behov må meldes til IKT Brukerhjelpen.

2.1.10 Det tas backup av data som lagres sentralt i kommunens nettverk (fagsystemer, fellesområder, hjemmeområde (P:)). Den ansatte er selv ansvarlig for å ta backup av data lagret lokalt på sin datamaskin, mobiltelefon, nettbrett o.l.

2.1.11 Lagring og sikkerhetskopiering er en begrenset ressurs, og filer som ikke lenger er aktuelle skal slettes.

2.1.12 Bruk av kommunalt IKT-utstyr til private formål skal kun foregå i begrenset utstrekning så lenge:

- *Det ikke påvirker jobbrelaterte oppgaver*
- *Det ikke legger beslag på betydelige ressurser (f.eks. bruk av mye lagringsplass)*
- *Det ikke utsetter kommunen for unødvendig risiko. Er man i tvil, kontakt nærmeste leder og få gjennomført en risikovurdering.*

2.1.13 Bruk av kommunalt IKT-utstyr til private formål forutsetter at privat materiale skilles klart fra det arbeidsrelaterte. Privat materiale skal lagre i egen mappe merket "Privat". Dette gjelder også e-postkonto, eget hjemmeområde på server (P:) og lokal harddisk på den ansattes klientutstyr.

2.1.14 Unngå så langt som mulig å tillate utenforstående å koble seg til kommunens utstyr og nettverk, med unntak av trådløst gjestenett. Det er i utgangspunktet ikke tillatt å bruke fjernstyringsverktøy (Teamviewer o.l.) med mindre dette er godkjent av IKT-kontoret.

2.1.15 Handlinger for å omgå sikkerhetsinnstillinger og mekanismer rundt dette er under ingen omstendigheter tillatt.

2.1.16 Brukere av kommunens IKT-løsninger har krav på at deres personvern ikke blir krenket på noe vis gjennom deres tilgang til IKT-løsningene. Det skal ikke utleveres opplysninger om brukere eller data tilhørende brukere der dette ikke er nødvendig som følge av vedtatte reglement eller norsk lov.

2.1.17 Det er ikke tillatt å behandle gradert informasjon på privat utstyr. Dette gjelder også for periferiutstyr. Unntak er ved bruk av privat utstyr for tilgang til kommunens hjemmekontorløsning.

2.1.18 Bestilling av tilgang til kommunens hjemmekontorløsning gjøres av nærmeste leder. Ved bruk av hjemmekontorløsningen er det ikke tillatt å foreta lokal lagring av gradert informasjon på klientutstyret som benyttes (PC, nettbrett o.l.).

2.1.19 Alt kommunalt IKT-utstyr skal leveres tilbake ved avslutning av arbeidsforhold, evt. også ved endring av arbeidsforhold.

Som et generelt prinsipp er det ikke tillatt å formidle gradert informasjon gjennom ukryptert elektronisk kommunikasjon. Eksempler på dette er e-post, nettbaserte meldingstjenester, sosiale medier, telefaks, tekstmeldinger (SMS), mv.

Dersom det er nødvendig å formidle gradert informasjon gjennom ukryptert elektronisk kommunikasjon skal slik informasjon sladdes og anonymiseres på en slik måte at det ikke fremkommer gradert informasjon.

2.1.20 Dersom eventuell sladding gjøres elektronisk, skal dette enten gjøres ved godkjent spesialprogramvare eller ved at dokumentet skrives ut etter at det er sladdet og skannes på nytt før dokumentene kan overføres elektronisk. Sentralarkivet vil kunne veilede i slike tilfeller.

2.2. Brukerkonto, systemtilganger, passord, pin-koder o.l.

2.2.1 Det er viktig å merke seg at systemtilganger, passord, PIN-kode o.l. er personlige, og skal ALDRI oppgis til andre, heller ikke til IKT-ansatte.

2.2.2 Passord, PIN-koder o.l. skal holdes hemmelig og ikke oppbevares slik at andre kan finne det, for eksempel nedskrevet på en lapp.

2.2.3 I Eigersund kommune skal man bruke ulike passord, PIN-koder o.l. for ulike tilganger, så langt dette er praktisk gjennomførbart.

2.2.4 Passord må endres straks når det er mistanke om at det er kjent for andre.

2.2.5 Passord til fagsystemer og kommunens nettverk skal skiftes minimum 1 gang i året.

2.2.6 Passordregler:

- Passord skal endres minst hver 12. mnd.
- Passord må oppfylle følgende krav:
  - *være minst 8 tegn*
  - *inneholde små bokstaver*
  - *inneholde store bokstaver*
  - *inneholde tall (0-9)*
- Passordet må være forskjellig fra de tre siste passordene dine.
- Passordet bør ikke inneholde ord eller navn som kan knyttes til brukeren, for eksempel navn på familiemedlemmer, stedsnavn, titler, årstall o.l.

2.2.7 Det er viktig at passord ikke gjenbrukes, for eksempel at den ansatte har samme passord på kommunens systemer som i andre tjenester.

2.2.8 I tilfeller der det eksisterer fellesbrukere hvor flere personer har kjennskap til brukernavn og passord (eller annen type tilgangskoder), plikter de som har denne tilgangen å påse at ingen uautoriserte personer får kjennskap til dette.

2.2.9 Den enkelte ansatte er selv ansvarlig for handlinger som han/hun utfører som pålogget bruker.

2.2.10 Det er ikke tillatt å utgi seg for å være en annen ansatt ved bruk av kommunens IKT-løsninger.

2.2.11 Bestilling av nye eller endrede tilganger til kommunens IKT-løsninger skal foretas av nærmeste leder.

2.2.12 Ved glemt passord, mistanke om passord / koder på avveie eller andre påloggingsproblemer, ta umiddelbart kontakt med IKT Brukerhjelpen.

2.3. Mobilt utstyr og eksterne lagringsmedier

2.3.1 Sørg for at tilgangskontroll er slått på på alt mobilt utstyr som benyttes. Dette kan du for eksempel gjøre ved å skru på PIN-kode eller passord.

2.3.2 Vær restriktiv med hva som lagres på mobilt utstyr og eksterne lagringsmedier, disse enhetene kan fort havne på avveie.

2.3.3 Sørg for at mobiltelefon, minnepinne, minnekort o.l. er beskyttet (kryptert) der dette er gjennomførbart.

2.3.4 Gradert informasjon skal ikke lagres på mobilt utstyr og eksterne lagringsmedier med mindre det er installert godkjente krypteringsløsninger.

2.3.5 Tekstmeldinger kan bare i begrenset grad brukes til å formidle gradert informasjon. Sendte og mottatte tekstmeldinger bør slettes fortløpende og ikke oppbevares på telefonen utover det som er påkrevd. Vær klar over at også tekstmeldinger vil kunne være omfattet av arkiv- og journalplikt.

2.4. Internett

2.4.1 Ikke trykk på lenker eller knapper i sprettoppvinduer som dukker opp uten at du er sikker på hva du trykker på.

2.4.2 Ikke godkjenn endringer på din datamaskin, mobiltelefon o.l. uten å være trygg på endringene.

2.4.3 Følge kommunens retningslinjer for bruk av digital kommunikasjon og sosiale medier, jf. kommunens Vær varsom-plakat - sosiale medier.

2.4.4 Ikke bruk Facebook, Google Disk, Dropbox eller andre lignende internettbaserte tjenester til saksbehandling, men bruk i stedet kommunens sak-/arkivsystem eller annet aktuelt fagsystem.

2.4.5 Det er ikke tillatt å bruke private kontoer for skytjenester der det er synkronisering mellom kommunens IKT-løsninger og slike tjenester. Eksempler på disse er Dropbox, OneDrive og Jottacloud.

2.4.6 Informasjon som er taushetsbelagt, intern, sensitiv eller som på annen måte stiller krav til lagring, arkivering og informasjonssikkerhet skal IKKE lagres utenfor Eigersund kommunes interne systemer, uten at det foreligger en databehandleravtale.

2.4.7 Sensitiv informasjon må ikke utveksles via internett med mindre godkjente krypteringsløsninger benyttes.

2.4.8 Vis nettvett: Nettvettsreglene

2.5. E-post og kalender

2.5.1 Enhver som benytter kommunens e-postløsninger skal bruke dette på en fornuftig måte. Dette innebærer blant annet å begrense privat bruk av postboksen, samt å slette e-poster som ikke lenger er aktuelle. Postboksen er ikke et arkivsystem.

2.5.2 All bruk av kommunal e-post er på vegne av Eigersund kommune og kan ikke benyttes til privat formål. Hvis du mottar privat e-post på kommunens e-postkonto, skal dette arkiveres i egen mappe merket «Privat», jf. pkt. 2.1.12.

2.5.3 E-post er ikke et verktøy for sikker kommunikasjon med mindre den er kryptert.

2.5.4 Ikke send taushetsbelagt eller sensitiv informasjon per e-post. Dersom det mottas e-post med sensitiv eller taushetsbelagt informasjon skal denne ikke videresendes eller besvares uten at den graderte informasjonen er slettet.

Avsender bør normalt alltid varsles om at det ikke er ønskelig å sende e-post med gradert informasjon til kommunen av personvernhensyn, samt at kommunen ikke kan bruke e-post til slik informasjon.

2.5.5 Ved mistanke om at e-post inneholder skadelig programvare eller forsøk på svindel, skal e-posten slettes umiddelbart. Linker eller vedlegg må ikke åpnes hvis avsenderen eller meldingen ikke kan tolkes som en seriøs henvendelse.

2.5.6 Det må utvises aktsomhet når e-postadresser legges igjen på nettsider og registreringsskjema. Dette for å forebygge at e-postadressen blir inkludert i lister som brukes for spam.

2.5.7 Ved utsending av e-post til mange mottakere som ikke er en distribusjonsliste, skal mottakere legges inn i feltet for blind-kopi. Dette for å hindre uønsket spredning av e-postadresser.

2.5.8 Husk at e-post og sms benyttet i saksbehandling også skal arkiveres i kommunens sak-/arkivsystem.

2.5.9 Din kalender er offentlig og skal være åpen for alle. Ikke skriv sensitiv eller taushetsbelagt informasjon i kalenderen.

2.5.10 Vær generelt bevisst på hva du skriver i møteoppføringer, både i emne- og notatfeltet, ta utgangspunkt i at kalenderoppføringer er synlige for alle i Eigersund kommune.

2.5.11 Ved planlagt fravær over lengre tid er det den ansattes ansvar å aktivere fraværsassistent slik at avsendere får beskjed om hvem som kan ta imot og følge opp e-posthenvendelser som haster.

2.6. Snoking

2.6.1 Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter helseregisterloven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift, jf. helseregisterloven §18.

2.6.2 Det er ikke tillatt for kommunalt ansatte å søke etter, tilegne seg, bruke eller besitte andre opplysninger i journaler, fagsystemer eller andre registre uten at det er saklig begrunnet i den ansattes arbeidsoppgaver.

2.7. Innsyn og overvåking

2.7.1 Det kan tas beslutning om innsyn i den enkelte ansattes postboks eller hjemmeområde hvis det er behov i forhold til å kunne ivareta daglig drift, kommunens ansvar eller omdømme. Beslutning om slikt innsyn tas av nærmeste leder eller kommunalsjef.

2.7.2 Det kan tas beslutning om innsyn hvis det er mistanke om at postboks eller hjemmeområde inneholder materiale som er i strid med norsk lov eller ved brudd på de plikter som følger arbeidsforholdet.

2.7.3 Den ansatte skal varsles om innsynet på forhånd og få mulighet til å være til stede hvis dette er praktisk og tidsmessig mulig og det ikke er fare for bevisødeleggelser.

2.7.4 Gjennomføring av innsyn skal dokumenteres i en rapport som arkiveres i kommunens sak-/arkivsystem.

2.7.5 Den enkelte ansatte kan selv gi ledere og andre ansatte innsyn i sine e-post- og filområder ved behov, for eksempel ved sykdom eller permisjon. En slik tillatelse skal alltid gis skriftlig og arkiveres i kommunens sak-/arkivsystem.

2.7.6 IKT-kontoret i kommunen benytter systemverktøy som overvåker IKT-løsningene. Informasjon og logger fra disse brukes kun til driftsformål. I tillegg har alle datasystemer i kommunen varierende grad av sporbarhet gjennom ulike loggfunksjoner der brukernes aktivitet lagres. Alle slike logger vil bli kontrollert, systematisk eller gjennom stikkprøver.

2.7.7 IKT-kontorets ansatte, systemansvarlige og andre med en spesiell rolle i drift av kommunens IKT-løsninger, har taushetsplikt med hensyn til informasjon de på denne måten får tilgang til om den enkelte ansattes bruk av disse løsningene.

2.8. Avslutning av ansettelsesforhold

2.8.1 Når et ansettelsesforhold avsluttes skal brukeren rydde i sin postboks og sitt hjemmeområde. Den ansatte har selv ansvar for å videreformidle informasjon som skal bevares, enten til rett person eller legge inn i aktuelt fagsystem.

2.8.2 Data lagret i postboksen og på hjemmeområdet vil bli bevart i 3 måneder etter endt ansettelsesforhold. Deretter vil informasjonen bli slettet.

2.8.3 Brukerkontoer til den ansatte som slutter vil bli sperret når ansettelsesforholdet avsluttes.

2.8.4 Ved dødsfall vil postboks og hjemmeområde bli slettet etter 3 måneder, med mindre det er sannsynlig at politiet ønsker innsyn i opplysningene. Før sletting finner sted kan det foretas innsyn for å sortere ut virksomhetsrelatert e-post og dokumenter i tråd med rutiner for dette.

Ved behov for assistanse i forbindelse med bruk av kommunens IKT-løsninger så

Ta kontakt med IKT Brukerhjelpen

E-post: *brukerhjelpen@eigersund.kommune.no*
Telefon*: *51 46 81 11