1. Formål

Formålet med instruksen er å sammenfatte regler som skal sikre ivaretagelse av personvern og informasjonssikkerhet i Sarpsborg kommune.

2. Gjelder for

Instruksen gjelder alle ansatte i Sarpsborg kommune, eksterne konsulenter, folkevalgte og andre som gis tilgang til kommunens IKT-relatert utstyr og systemer, i eller utenfor kommunens lokaler.

3. Instruks

Område	Gjeldende regler og praksis
Tildeling, endring og sletting av tilganger	• Tildeling, endring og sletting av tilganger er et lederansvar • Medarbeider skal ha tilgang tilpasset sitt arbeide basert på tjenstlig behov • Nærmeste leder skal sørge for at den enkelte bruker gjennomgår nødvendig opplæring før det blir gitt tilgang til kommunens informasjonssystemer • Den enkelte bruker har selv en plikt til å melde fra til nærmeste leder dersom man har tilganger utover tjenstlig behov
Passord, pålogging og avlogging	• Passord er personlig og skal ikke gjøres kjent for andre • Ved mistanke om at passord er kjent for andre, skal passordet straks endres • Det er ikke tillatt å bruke en annens brukernavn og passord • Passord som benyttes i kommunens systemer skal ikke brukes andre steder • Når du går fra datamaskinen, nettbrett, mobiltelefon eller lignende, skal alltid skjermlås aktiveres, eventuelt logge av eller slå av utstyret
Logging og sporbarhet	• Bruk av kommunens informasjonssystemer, søk i kommunens registre og aktivitet på Internett, blir logget av sikkerhetsmessige og administrative årsaker • Logger kan bli gjennomgått av autorisert personell med det formål å kontrollere bruken av IKT-systemene, eller for å avdekke og håndtere sikkerhetshendelser • Ved avvik vil dette bli meldt som en sikkerhetshendelse i avvikssystemet
Søk i registre	• Det er kun tillatt å foreta søk i kommunens registre ved tjenstlig behov • Søk til private formål er ikke tillatt

Område	Gjeldende regler og praksis
Eierskap, saksbehandling, lagring av informasjon og IKT-utstyr	• IKT-utstyr og lagret informasjon er kommunens eiendom • Arkivverdig informasjon skal lagres i kommunens sak/arkivsystem • Annen informasjon knyttet til tjenesteproduksjonen skal lagres i det aktuelle fagsystemet for tjenesten • Andre arbeidsdokumenter skal i all hovedsak lagres i kommunens fellesløsning for samhandling • Særlige kategorier av personopplysninger (sensitive personopplysninger) skal alltid lagres sak/arkivsystemet eller fagsystemer i sikker sone • Data lagret lokalt på kommunens datautstyr eller i Microsoft One-drive vil ikke bli tatt sikkerhetskopi av og dermed kan slike data gå tapt ved for eksempel re-installering av utstyret, utilsiktet sletting, eller ved at filer blir ødelagt • Det er ikke tillatt for kommunens ansatte å lagre informasjon i skytjenester uten forutgående godkjenning av fagansvarlig informasjonssikkerhet • Den kommunalt tildelte Microsoft One-drive er godkjent for skybasert lagring (Dog ikke for særlige kategorier av personopplysninger) • Utlevert IKT-utstyr er ditt ansvar og skal beskyttes og benyttes med aktsomhet • Bærbart utstyr skal beskyttes mot hærverk, tyveri og misbruk • Det er kun tillatt å bruke IKT-utstyr som er godkjent av IT-avdelingen for oppkobling mot kommunens interne datanettverk • Installasjon av utstyr og programvare skal utføres av kommunens IT-avdeling eller den/de som IT-avdelingen godkjenner til dette.
Bruk av eksterne lagringsmedier	• Det er ikke tillatt å koble private lagringsmedier til kommunens datanettverk • Det skal utvises stor aktsomhet ved bruk av eksterne lagringsmedier • Eksterne lagringsenheter skal skannes for virus på PC som har oppdatert antivirus før de benyttes i nettverket • Ved mistanke om virus, ta kontakt med IKT-brukerservice
Bruk av programvare	• Det er ikke tillatt på eget initiativ å installere egen programvare • Vurdering og installasjon av programvare skal utføres av IT-avdelingen eller den de godkjenner til dette
Kartlegging av systemsvakheter	• Ansatte skal ikke på eget initiativ foreta kartlegging eller testing av mulige systemsvakheter eller forsøke å trenge inn i interne eller eksterne systemer • Hvis det foreligger mistanke om systemsvakheter, skal disse meldes IKT-Brukerservice og i kommunens avvikssystem.
Informasjon gradert etter Sikkerhetsloven	• Medarbeidere med behov for sikkerhetsklarering skal være autorisert for å få tilgang til gradert informasjon • Dette gjelder f.eks. ved samhandling med Fylkesmannen, Forsvaret, Politiet eller andre i forbindelse med planverk og graderte trusselvurderinger. • Gradert informasjon skal kun lagres og behandles på utstyr som er vurdert å ha tilstrekkelig sikring, og merket med graderingsnivå • Gradert informasjon skal ikke produseres, oppbevares eller mangfoldiggjøres på IKT-utstyr som ikke er godkjent for dette • Lagringsmedia som inneholder gradert informasjon, skal behandles i henhold til Lov om forebyggende sikkerhetstjenester (sikkerhetsloven)

Område	Gjeldende regler og praksis
Særlige kategorier av personopplysninger	• Den enkelte medarbeider skal være klarert og autorisert for å få tilgang til slik informasjon • Slik informasjon skal kun lagres og behandles på utstyr og i systemer som er vurdert å ha tilstrekkelig sikring. (Sikker sone)
Rapportering av hendelser/avvik	• Hendelser/avvik relatert til personvern og informasjonssikkerhet, sikkerhetstruende hendelser, kompromittering, lovbrudd eller brudd på kommunens regler, retningslinjer eller instrukser, skal registreres i avvikssystemet. • Uønskede hendelser som omfattes av sikkerhetslovens bestemmelser skal ikke føres i avvikssystemet, men rapporteres direkte til fagansvarlig informasjonssikkerhet
Brukerstøtte	• Ta kontakt med IKT-Brukerservice dersom du har problemer med tilgang til systemer, data eller har generelle spørsmål angående informasjonssikkerhet: 69116933 / support@sarpsborg.com
Dokumentsikkerhet	• Taushetsbelagt informasjon skal ryddes bort og sikres tilfredsstillende når du forlater plassen din • Der er den enkeltes ansvar å vurdere om informasjonen skal skjermes • Bruk sikker utskrift når du skriver ut taushetsbelagt informasjon • Taushetsbelagte opplysninger skal ikke bli liggende ved skriveren • Taushetsplikten gjelder også overfor kollegaer, med mindre det foreligger tjenstlig behov for opplysningene • Fjernaksess til kommunes informasjon tillates kun der det ikke er fare for innsyn fra andre • Ved makulering/destruksjon av dokumenter som er taushetsbelagte skal det benyttes beholder merket «makuleres» og med lås fra kommunen, eller en makuleringsmaskin • Ved makulering/destruksjon av sikkerhetsgradert informasjon skal det benyttes egne makuleringsmaskiner godkjent for dette

Område	Gjeldende regler og praksis
Mobiltelefoner, nettbrett, bærbare PC-er m.m.	• Alle mobile enheter skal være låst med kode, biometri eller passord • Telefoner/nettbrett som støtter fjernsletting skal ha denne funksjonen aktivert • Særlig kategorier av personopplysninger og annen gradert informasjon skal ikke produseres, lagres, sendes eller på annen måte mangfoldiggjøres, uten at enheten og systemet er godkjent for dette • Det er ikke tillatt å bruke mobile enheter med kobling til Internett til håndtering eller lagring av særlig kategorier av personopplysninger eller annen gradert informasjon, eksempelvis dokumenter, foto, film, lyd, m.m. • Bruk av privat e-post til overføring av taushetsbelagt informasjon fra mobil enhet til kommunens systemer, regnes som brudd på taushetsplikten • Privat e-post er ikke tillat brukt til saksbehandling og tjenesterelatert kommunikasjon • Det må vises aktsomhet ved bruk av mobile enheter på trådløse nettverk • Nedlasting av programvare/app-er innebærer risiko for uautorisert tilgang eller spredning av informasjons fra mobile enheter, og det må derfor utvises særlig varsomhet • Ved bruk av fjernaksess til kommunens datasystemer via løsning for mobilt kontor, nettbrett, telefon mv. skal det sikres at uvedkommende ikke får innsyn i, eller tilgang til, kommunes data eller utstyr • Telefon eller nettbrett som er mistet, stjålet, eller på annen måte misbrukt, skal meldes til nærmeste leder og IKT-Brukerservice med informasjon om hva telefonen/nettbrettet inneholder av opplysninger, samt at SIM-kortet skal sperres umiddelbart, og telefonen fjernslettes hvis mulig.
Bruk av Internett og e-post	• Det skal skilles mellom jobbrelatert og privat bruk av arbeidsgivers internettilgang og e-postsystemer • Kommunens e-postsystem er et arbeidsverktøy og privat bruk av dette må ikke belaste systemet unødig • Det er ikke tillatt å bruke kommunens e-postsystem til privat eller ekstern markedsføring som eksempelvis utleie av leilighet m.m. • Lagring/arkivering av e-postmeldinger til arkiv skal vurderes i henhold til arkivlovens bestemmelser og journalføres i sak- arkivsystemet i henhold til egne retningslinjer • Bruk av e-post til overføring av særlig kategori av personopplysninger eller taushetsbelagte opplysninger unngås i størst mulig grad, og skal krypteres før den sendes • Ved bruk av sosiale medier skal det utvises særlig varsomhet, taushetsplikten må ivaretas • Bilder eller opplysninger om andre skal ikke distribueres uten samtykke Det skal utvises særlig aktsomhet ved mottak av e-post med vedlegg eller innebygde linker, fra ukjente. Beste praksis er å sjekke hvor linken vil ta deg, og gjøre en vurdering før man evt. trykker på linken. Er man usikker på innholdet, kontakt IKT-Brukerservice. E-post kan inneholde datavirus og forsøk på svindel. Ved mistanke om dette, kontakt IKT-Brukerservice.

Område	Gjeldende regler og praksis
Arbeidsgivers innsynsrett	• Databaser for e-post, fil- og andre samhandlingssystemer i kommunen er arbeidsgivers eiendom • Arbeidsgiver skal følge lovverket i forbindelse med innsyn i ansattes e-post eller dokumenter • Innsyn kan skje dersom det er nødvendig av hensyn til videre drift, og ved mistanke om aktiviteter som kan bryte gjeldende sikkerhetsbestemmelser eller taushetsplikt • Samtykke skal alltid innhentes hvis mulig • Den ansatte gis informasjon om at innsyn er foretatt dersom dette er mulig • Innsyn skal foretas av nærmeste leder med teknisk støtte fra IT-avdelingen og i nærvær av representant for den ansatte • Innsyn vil skje i overenstemmelse med Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale (med hjemmel i AML §9-5).