Retningslinjer for klassifisering av informasjon og daglig informasjonssikkerhet

1. Formål

VID må ifølge personopplysningsloven ha kontroll på sin håndtering av personopplysninger og taushetsbelagt informasjon. Alle medarbeidere skal opptre på en slik måte i det daglige at de ivaretar god informasjonssikkerhet i virksomheten.

Instruksen er teknologinøytral og gjelder uavhengig av hvordan informasjonen er lagret/oppbevart, enten det er på papir, lyd og bilde eller digitalt i en eller annen form.

2. Ansvar og målgruppe

- Ansatte (fulltid, deltid og midlertidige ansatte)
- Alle som har tilgang til, og/eller bearbeider og forvalter informasjon gjennom VIDs IKT infrastruktur

Virksomhetens ledelse er ansvarlig for at alle medarbeidere er kjent med og følger retningslinjer for informasjonssikkerhet.

Den enkelte bruker er personlig ansvarlig for sin håndtering av gradert informasjon. Brudd på denne instruks og/eller annet regelverk, vil kunne medføre ulike former disiplinær reaksjon.

3. Klassifisering av informasjon

Klassifisering	Beskrivelser	Eksempel	Tilgang/overføring av data
Åpen informasjon	Åpen informasjon som er tilgjengelig for alle uten særskilte tilgangsrettigheter. Informasjon som ikke kan skade noen.	• Åpen kilde informasjon • Publiserte policy, regler • Offentlige websider • Kursoversikter og innhold • Offentlig informasjon om personer i VIDs ledelsen og kontaktpersoner i VID	**Åpen**
Intern informasjon 1	Intern benyttes om informasjon som er begrenset til å være tilgjengelig for medarbeidere for å gjennomføre pålagte oppgaver. Informasjon på avveie kan gi moderate økonomiske skader og/eller svekket omdømme for VID, enkeltindivider eller samarbeidspartnere hvis den kommer uautoriserte i hende.	• Enkelte arbeidsdokumenter • Informasjon som er unntatt offentlighet • Grunnleggende personopplysninger om ansatte og student som standard kontakt informasjon (navn, telefonnummer, e-post adresse, kontorsted) og ansettelsesforhold (ansattnummer, student nummer, stillingstallet/nivå, til fratredelse data org tilhørighet og leder) • Interne regler, policy osv.	Begrenset tilgang til interne medarbeider. Informasjonen kan være tilgjengelig for eksterne med kontrollerte som har tjenstlig behov for informasjon, tilgangsrettigheter. Informasjon kan sendes via e-post både internt og eksternt. Papirkopier skal ikke henlegges utenfor VID lokaler uten tilsyn
Konfidensiell informasjon 1	Fortrolig benyttes dersom det vil kunne skade offentlige interesser, VID, enkeltindivider eller samarbeidspartnere at dokumentets innhold blir kjent for uvedkommende. Informasjon som er omfattet av lovbestemt og avtalemessig taushetsplikt. Informasjon på avveie som kan medføre alvorlig skade for VIDs formål, samarbeidspartnere, enkeltpersoner og/eller samfunnet om den kommer uautoriserte i hende.	• Personopplysninger, (uten grunnleggende informasjon) fødselsnummer • Grunndata, • Taushetsbelagte opplysninger • Dokumentasjon av tekniske løsninger driftsrutiner eller prosedyre som kan utnyttes i angrep på IT systemer, • Informasjon om sårbarheter som ved utnyttelse kan medføre stor skader for eksempel is risikovurdering eller revisjons rapporter	Informasjon skal kun være tilgjengelig for medarbeidere med kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. I spesielle tilfeller kan fortrolig informasjon også gjøres tilgjengelig for eksterne under samme kontrollerte tilgangsrettigheter. Informasjon kan sendes via intern e-post. Eksternt så må det benyttes kryptert løsning om det sendes via epost. Papirer kopier: Utskrift skal skje mens man er tilstede ved skriver Makuleres eller legges i beholder for makulering Papirer oppbevares i låst skap

		• Forskningsdata og publikasjoner hvor autentisering av data er svært viktig.	Sendes i lukket konvolutt il navngitt
Konfidensiell informasjon 2	Strengt fortrolig benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, VID, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende. Utilsiktet eller tilsiktet feilinformasjon og/eller redusert ytelse, vil kunne føre til feilvurderinger eller beslutninger med fatale konsekvenser. Brudd kan medføre katastrofal skade på VIDs interesser, samarbeidspartnere, enkeltpersoner og samfunnet om den kommer uautoriserte i hende.	• Særlige kategorier av personopplysninger herunder helseopplysninger • Andre økonomi, eller styre sensitiv opplysninger Gjennomføring av eksamen blir avbrutt. Utbetaling av lønn. Feil i informasjonen kan medføre tap av liv, f.eks. ved feilbehandling av pasienter.	Informasjon skal kun være tilgjengelig for medarbeidere med strengt kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. I spesielle tilfeller kan strengt fortrolig informasjon også gjøres tilgjengelig for eksterne Det er av kritisk betydning at det avleveres autentisk og gyldig informasjon. IKT-infrastrukturen har høyeste prioritet, feilretting starter umiddelbart og fortsetter inntil feilen er løst. Vurdere ekstra krav til tilgangsstyring, logging og revisjon, f.eks. multi-faktor autentisering. Overføring, overføringstiltak og bevaringstiltak må godkjennes av utførende databehandlingsansvarlig eller personvernombudet eller informasjonssikkerhetsleder Papirkopier: Utskrift skal skje mens man er tilsted ved pålogget skriver Makuleres eller legges i beholder for makulering Papirer oppbevares i låst skap Sendes i dobbel konvolutt, innerste konvolutt merkes strengt konfidensielt, ytterste konvolutt adressers autorisert mottaker Papirkopier bør ikke tas ut av VIDs lokaler

4. Daglig informasjonssikkerhetsretningslinjer

- Brukernavn og passord må ikke deles med andre.
- Man skal alltid logge av PC, lås alltid når du går i fra.
- Du skal ikke lagre konfidensielle opplysninger ukryptert på bærbart utstyr som for eksempel minnepinne, eller sende det via åpen e-post. Ta ikke med bærbart utstyr med ukrypterte konfidensielle opplysninger utenfor kontoret/arbeidsplassen.
- Du skal ha kontroll på dokumentene dine. Dette innebærer at du skal passe på:
    - å hente utskrifter med en gang.
    - å skrive ut kun det du må.
    - å ikke legge igjen dokumenter på møterom.
    - å ha gode makuleringsrutiner.
- Det er forbudt å lese, søke eller på annen måte tilegne seg eller bruke opplysninger uten at det er begrunnet, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.
- Taushetsplikt gjelder også mellom personell.
- Pass på at ikke uvedkommende lytter når du snakker om konfidensielle informasjon med en kollega, i telefon eller på offentlig sted.
- Pass på at uvedkomne ikke har innsyn.
- Når du deler konfidensielle opplysninger med andre må du forsikre deg om at vedkommende du kommuniserer med har rett til å få opplysningene. Mottar du f.eks. telefonsamtaler om pasienter, og du er i tvil om identiteten til innringer, kan du be om å få ringe vedkommende tilbake.
- Dobbeltsjekk at e-post og SMS du sender ikke inneholder konfidensiell informasjon. Ikke svar pasienter på e-post eller SMS, benytt godkjente løsninger.
- Ikke kommenterer jobbinformasjon på sosiale medier, og vær forsiktig når du bruker nettsamfunn.
- Følg avviksrutiner og bruk avvikssystemet.
- E-post og vedlegg til e-post fra mistenkelig ukjent avsender skal ikke åpnes.
- Vær kritisk til lenker og innhold i e-post (uærlige aktører med baktanker). Du kan få virus og spam på datamaskinen.
- Privat bruk av IT-utstyr og applikasjoner skal godkjennes av IT-seksjonen og vil normalt ikke bli gitt.
- Flytting/kopiering av helse- og personopplysninger (over på minnepinne, ekstern disk) skal godkjennes av daglig behandlingsansvarlig.
- Alle data skal sikkerhetskopieres.
- Utskrifter med personopplysninger skal oppbevares i låsbart skap og makuleres etter bruk.
- Elektronisk forsendelse av helse- og personopplysninger (e-post, meldingsutveksling mv.) skal krypteres.
- Når man forlater arbeidsplassen og ved arbeidsdagens slutt skal bruker logge ut av alle systemer.
- Alle brukere skal ha eget brukernavn og passord til alle systemer.

- Oppbevaring, bruk og sikring av passord/PIN-kode/sikkerhetskoder for elektronisk ID skal være i henhold til fastlagte prosedyrer. NB! Må aldri oppgis på telefon eller i e-post.
- Det er ikke tillatt å søke etter informasjon man ikke har behov for eller ikke er autorisert for.
- Kun jobbrelatert informasjon fra internett kan lastes ned.
- Programvare skal ikke installeres uten godkjennelse fra IT-seksjonen.