

Retningslinjer for bruk av Ulvik herad sitt IT system

Autorisasjon ID

- 1 Du har fått tilgang til IT-systema i Ulvik herad. Desse systema kan innehalde sensitiv informasjon, og det er viktig at du behandlar informasjonen slik at den ikkje kjem på avvegar.
- 2 Dine tilgangar er basert på dine tenestlege behov du har for å utføra stillinga di. Får du tilgang til sensitive opplysningar du ikkje har behov for, skal du informere om dette til næraste leiar.
- 3 IT-systemet skal berre nyttast til kommunal verksemd. Du må være merksam på at IT-systema inneheld loggfunksjonar.

Dataområde:

- 1 Du får tilgang til eit personleg område som berre du har tilgang til, dette er kalt P:
- 2 Dataområde du deler med fleire er: L, for nokon brukarar og F: og S:
- 3 Berre data på desse områda vert sikkerheitskopierte.
- 4 Bruk av minnepennar o.l. skal minimerast, og skal ikkje innehalda sensitive data.
- 5 Kommunale lagringsområde bør ikkje innehalda private datafiler.
- 6 Bruk av Google drive, Dropbox o.l. er personleg. Arkivverdige og sensitive data skal ikkje lastast opp på slike område.

E-post

- 1 Du har fått eigen kommunal e-post adresse som er knytt til di stilling. E-post adressa bør berre nyttast til tenestlege behov. Det er viktig at du skil privat og kommunal e-post, då det elles vil sjå ut som din e-post er adressert til / frå Ulvik herad.
- 2 Ver varsam med ukjent e-post, og e-postar med linkar eller filer. Desse kan innehalde virus, som igjen kan medføra store konsekvensar for heradet. Er du i tvil, ta kontakt med IT.
- 3 Ikkje send personnummer, kontonummer, og liknande sensitiv informasjon på e-post.

PC / Nettbrett / Mobiltelefon.

- 1 Ditt IT-utstyr er kople saman med heradet sine andre IT-system. Ved virus eller andre uregelmessigheiter på IT-utstyret, kan IT bli varsla automatisk.
- 2 Utstyret bør berre brukast i kommunal teneste. Du kan difor ikkje låna bort utstyret, og ein skal vera varsam med å installera eigne program.
- 3 Utstyret skal være sikra med passord eller kode.

Utskrift / Skanning

- 1 Utskrifter med sensitiv informasjon skal være minimalt, og berre formidlast som info i samhandling med dei det gjeld.
- 2 Skanning av dokument med sensitiv informasjon må berre gjerast til systema som kan ta imot sensitiv informasjon.

Bruk av sosiale media, chat, skype, m.m.

- 1 Brukast fornuftig og med varsemd. Bruk nettvit.
- 2 Bruk berre original program og ikkje last ned tilleggsfunksjonar.

Tryggleik / arbeidsgjevar sine rettar.

Fagsystema som inneheld sensitive data har automatisk loggføring som standard, i forhold til lovpålagde krav.

Arbeidsgjevar kan i nokon tilfelle få innsyn i din e-post eller personlege dataområde.

For Helse og Omsorg gjeld følgjande tillegg:

Brukarar i Helse og Omsorg er i ein såkalla sikker sone. Den er avskilt frå heradet sine andre datanett, og har auka tryggleik. Denne sonen har redusert tilgang til internett, og må nytte Citrix for å få tilgang til ulike fagprogram, filområde m.m.

Dataområda i sikker sone:

Som brukar i Helse og Omsorg gjeld og følgjande

- 1 Dataområda som er lista opp tidlegare er berre tilgjengeleg via Citrix.
- 2 Du får tilgang til eit personleg område på sikker sone, P:
- 3 Dataområde du deler med fleire på sikker sone er: L, (t.d. Felles sjukheim, felles legekontor)
- 4 Berre data på desse områda vert sikkerheitskopierte.
- 5 Bruk av minnepinnar o.l. skal minimerast, og innhaldet bør vera kryptert.
- 6 Du kan ikkje kopiera data frå sikker sone.

Eg bekreftar at eg har fått informasjon, og fått ein kopi av retningslinene.

Dato:	Eg forstår retningslinene	
	Underskrift:	