Generell IT Sikkerhetsrutine for ansatte i Polaris Media.

Jeg er klar over at:

1. Jeg må selv være oppmerksom på trusler fra Internett, og bidra til at disse utgjør en lavest mulig risiko. Det må spesielt utøves varsomhet rundt åpning av ukjente filer.
2. Bruk av Internett blir logget og overvåket av drifts- og sikkerhetsmessige årsaker herunder også https-trafikk. Ved mistanke om sikkerhetsbrudd vil loggene kunne benyttes i vurderingen.
3. All bruk av Internett fra konsernet og dets datterselskap sine systemer kan spores tilbake til konsernet og det enkelte selskap. Det er ikke tillatt å søke etter eller surfe på sider eller laste ned og lagre filer med straffbart innhold, sider med tjenester som kan lede til straffeforfølgelse for tilbyder eller sider med innhold som er pornografisk, uetisk, støtende, trakasserende, obskønt, truende eller rasistisk.
4. Det er ikke tillatt å oppgi passord til andre, det samme gjelder mht å «låne bort» brukernavn og passord.
5. Deling av ressurser på en PC, som f.eks. den lokale harddisken er ikke tillatt.
6. Ved tilkobling til interne ressurser fra eksterne nett, skal alogin.adressa.no benyttes.
7. Passordet skal skiftes **hver 180 dag**. Dette gjøres vha pålagte rutiner.
8. Passordet SKAL være komplekst, dvs. minst 6 tegn og inneholde, tall, små og store bokstaver evt spesialtegn.
9. Passordet skal ikke ha vært benyttet det siste året.
10. Det skal settes skjermbeskytter som slår til etter 30 minutter og må låses opp med passord.

Sikkerhet ved bruk av mobile enheter i Polaris Media

1. Enheten **SKAL** være beskyttet enten ved form av en PIN kode eller passord som skal slås på automatisk etter minst 5 minutter. PIN koden skal ha minst 4 tegn.
2. Sensitiv informasjon bør ikke lagres på en mobil enhet, hvis dette er nødvendig skal data krypteres.
3. Vær kritisk ved installasjon av 3 part programvare. Mobiltelefoner er like utsatt for skadevare som en PC.
4. Det er ikke tillatt og modifisere / endre mobiltelefonens OS (ref «Jailbreak» , «rooting» og «side-loading»).
5. Det er brukeren sitt ansvar at data på mobil enhet er sikkerhetskopiert.

Generelt

Dersom det er tvil rundt håndheving av disse reglene, sjekk med Adresseavisens Teknologiavdeling (ATEK) eller din nærmeste leder.

Brudd på reglene kan medføre arbeidsrettslige konsekvenser, og i alvorlige tilfeller oppsigelse eller avskjed. Grove brudd vil normalt bli politianmeldt og påtalt.

Alle ansatte i Polaris Media skal lese og sette seg inn i denne IT Sikkerhetsrutinen. Oppdatert rutine ligger til enhver tid i personalhåndboken. Denne er gjeldende og bruker har selv ansvar for å være oppdatert til enhver tid.