Sikkerhetsretningslinjer for eksterne konsulenter

I henhold til avtale forplikter eksterne konsulenter (heretter Konsulenten) seg til å følge Enovas sikkerhetspolicyer og retningslinjer. Ved å signere dette dokumentet bekrefter den undertegnede følgende:

- Konsulenten skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjon de behandler og hvilke krav som stilles til informasjonsbehandlingen og bruken av IKT.

- Konsulenten skal ta aktivt ansvar for informasjonssikkerheten i de applikasjonene og systemene konsulenten forvalter.

- Konsulenten plikter å gjøre seg kjent med og følge de retningslinjer og policyer som til enhver tid gjelder for Enovas ansatte. Der hvor det er konflikt mellom retningslinjene i dette dokumentet og Enovas øvrige policyer og retningslinjer, er det Enovas øvrige policyer og retningslinjer som gjelder.

Alt utstyr som benyttes i tilknytning til Enova, inkludert egen mobiltelefon og PC, skal:

  - holdes oppgradert og tilstrekkelig beskyttet mot ondsinnet programvare.
  - skal ikke brukes til aktiviteter som bryter norsk lov eller opphavsrett.
  - kun benytte programvare med gyldige lisenser.
  - oppbevares på et sikkert sted når det ikke brukes.
  - ikke deles med andre, inkludert andre familiemedlemmer.

- Ved tap av utstyr som benyttes i tilknytning til Enova skal Enova varsles.

- I Enovas tjeneste skal kun din e-postadresse fra Enova benyttes. Enovas e-postadresse skal ikke benyttes til utenfor Enovas tjeneste. Brukere skal være forsiktige med å åpne vedlegg eller klikke på lenker fra ukjente avsendere, da disse kan inneholde skadelig programvare. E-post skal brukes profesjonelt, og spam eller kjedebrev skal ikke videresendes.

- All kommunikasjon som angår Enova skal foregå over Enovas godkjente kommunikasjonskanaler.

- Enhver mistenkelig aktivitet eller sikkerhetsbrudd skal umiddelbart rapporteres til IT-avdelingen. Dette inkluderer mistenkelige e-poster, tap av data eller uautorisert tilgang til systemer.

    - Alle brukere er pålagt å rapportere sikkerhetshendelser umiddelbart. Dette inkluderer glemte eller kompromitterte passord. Slike hendelser skal rapporteres til driftsleverandøren uten opphold for å minimere risikoen og sikre rask håndtering.

- Enovas intellektuelle eiendom skal lagres på et eget område, for eksempel en egen mappe, og aldri blandes sammen med filer tilhørende andre. Dokumenter tilhørende Enova skal fortrinnsvis lagres på Enovas skytjenester for dokumenter.

- Brukere skal benytte sine egne tildelte brukernavn og passord for å få tilgang til IT-ressurser. Deling av påloggingsinformasjon er strengt forbudt.

Brudd på disse retningslinjene kan føre til tiltak. Ulovlig aktivitet vil bli rapportert til relevante myndigheter og kan medføre rettslige konsekvenser.
