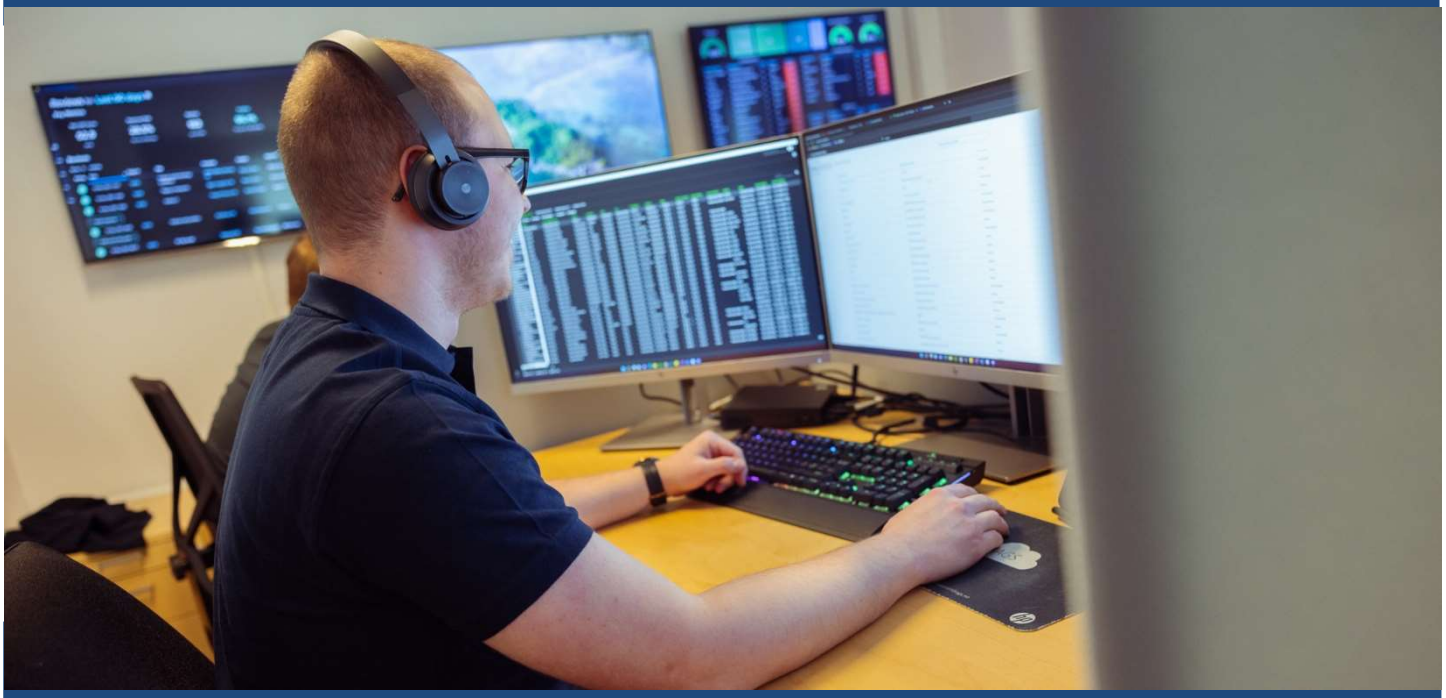

Generell sikkerhetspolicy for brukere

Utarbeidet av **AGS IT-partner AS**

Versjon 2.1

Vedlegg 1: Generell sikkerhetspolicy for brukere

Målet med den generelle IT-policyen er å etablere retningslinjer for ansattes bruk av IT og sikre en trygg og effektiv bruk av bedriftens digitale ressurser.

1. Brukeransvar og adferd

1.1 Alle ansatte forventes å bruke IT-ressurser ansvarlig og i samsvar med gjeldende, eksterne lover og regler.

1.2 Passord og brukerinformasjon skal behandles konfidensielt, og ansatte må ikke dele eller utlevere denne informasjonen til uautoriserte personer. Det anbefales å unngå å lagre passord i dokumenter eller oppbevare passord på steder som er lett tilgjengelig. Det anbefales heller å benytte sikrere metoder som passordhvelv for å beskytte og administrere påloggingsinformasjon.

1.3 Benytte to-faktor autentisering (2FA) på applikasjoner for å øke tilgangssikkerheten ved å kreve to separate autentiseringsmetoder.

1.4 Nedlasting og installasjon av programvare som ikke er godkjent på bedriftens enheter må godkjennes av daglig leder/sikkerhetsansvarlig for å sikre sikkerhet og kompatibilitet.

1.5 Unngå å benytte ukjente enheter som USB-minnepenn eller minnekort.

1.6 Unngå å koble til usikre nettverk. Bruk innebygget mobilt bredbånd eller del nettverk via mobil.

1.7 Lån ikke bort eller gi tilgang til enhetene dine uten din tilstedeværelse.

1.8 Unngå at utskrifter blir liggende i skriveren over lengre perioder slik at uautoriserte personer ikke får tilgang til dokumentene.

2. Informasjonssikkerhet

2.1 Ansatte skal være oppmerksomme på sikkerhetsrisikoer, rapportere mistenkelige aktiviteter og følge retningslinjer for informasjonssikkerhet, (personvernsforordningen (GDPR) og gjeldene bransjestandarder). Følge bedriftens prosedyreplan for håndtering av IT-sikkerhetshendelser.

2.2 Bruk av bedriftens nettverk og ressurser for å få tilgang til eller distribuere ulovlig eller støtende materiale er strengt forbudt.

3. Beskyttelse av data

3.1 Sensitiv informasjon, inkludert kunde- og forretningsdata, må beskyttes og deles kun i samsvar med retningslinjer for personvern og sikkerhet.

3.2 Regelmessig sikkerhetskopiering av data er pålagt for å unngå tap av informasjon og for å opprettholde forretningskontinuitet.

3.3 For å sikre at data blir sikkerhetskopiert er det essensielt at den blir lagret på rett måte. Derfor er det avgjørende at brukere lagrer informasjon på de digitale områdene som er spesifisert av bedriftens retningslinjer. Unngå å lagre data lokalt på datamaskiner eller på private lagringsenheter eller -tjenester, med mindre dette er i samsvar med ledelsens godkjennelse.

4. Bruk av e-post og kommunikasjon

4.1 E-post og andre digitale kommunikasjonsmidler skal brukes profesjonelt, og ansatte må unngå deling av sensitiv informasjon via usikrede kanaler.

4.2 Ansvarlig bruk av sosiale medier på arbeidsplassen oppfordres, og ansatte må være oppmerksomme på bedriftens retningslinjer for offentlig kommunikasjon.

4.3 Vær oppmerksom på potensielle e-post-spoofing-scenarier: Ved spoofing later e-posten til å være fra kjente avsendere, men er i realiteten falske avsenderadresser for å villede mottakeren. Kontroller nøye før du svarer på henvendelser eller utfører handlinger basert på e-postkommunikasjon.

4.4 Vær oppmerksom på potensielle e-post-phising-scenarier: Ved phising etterspør avsender sensitive opplysninger. Unngå å svare på e-poster som ber om sensitive opplysninger eller handlinger, spesielt hvis de virker mistenkelige eller uventede. Bekreft alltid slike forespørsler direkte med den påståtte avsenderen via en annen kommunikasjonsmetode for å bekrefte ektheten.

4.5 Ikke klikk på lenker eller vedlegg i e-post som du synes virker mistenkelige eller unormale. Bruk rapporter-funksjonen i Outlook på e-post som er mistenkelige.

5. Utstyr og ressurser

5.1 Bedriftens IT-utstyr og ressurser skal kun brukes til arbeidsrelaterte formål, med mindre annet er godkjent av ledelsen.

5.2 Private enheter kan ikke benyttes for tilgang til bedriftens tjenester med mindre dette er godkjent av bedriftens ledelse.

5.2 Tap eller tyveri av IT-utstyr må rapporteres umiddelbart til daglig leder (jf. standard prosedyreplan for håndtering av IT-sikkerhetshendelser)

6. Opplæring og overholdelse

6.1 Alle ansatte bør gjennomgå regelmessig opplæring om IT-sikkerhet for å opprettholde bevissthet og overholdelse av retningslinjene.