Revisjonsdato	Revisjonsnummer	Eier	Godkjent av	
20.01.2025	01	Bjørn Tore Sundvor-Halleland	Lars Hauge	
Dokument ID: PRO-244-01				

Policy for informasjonssikkerhet

1. Formål

Denne policyen etablerer minimumsstandarder for informasjonssikkerhet som må oppfylles av enheten. Den tillater forbedringer basert på unike forretningskrav og juridiske retningslinjer, men krever at sikkerhetsstandardene som er beskrevet her, minst oppfylles.

Policyen gir retning for alle andre sikkerhetspolicyer og standarder, og beskriver forpliktelsen til å:

1. Beskytte konfidensialiteten, integriteten og tilgjengeligheten av informasjon;
2. Håndtere risikoer for sikkerhetsbrudd;
3. Sikre et pålitelig IT-rammeverk;
4. Oppdage og handle ved sikkerhetshendelser;
5. Overvåke systemer for sikkerhetskompromisser; og
6. Fremme bevissthet om informasjonssikkerhet.

2. Omfang

Denne policyen gjelder for alle systemer under Ambios kontroll, inkludert de som administreres av tredjepartstjenester. Den dekker all informasjon som produseres eller brukes i forretningsaktiviteter.

3. Erklæring om Informasjonssikkerhet

3.1. Organisatorisk sikkerhetsstyring

Effektiv informasjonssikkerhet krever etablering av både en informasjonsrisikostyringsfunksjon og en informasjonsteknologisikkerhetsfunksjon. Organisasjoner skal utnevne en enkeltperson eller et team til å overvåke risikostyring og tekniske aspekter ved informasjonssikkerhet.

Grunnleggende informasjonssikkerhetsfunksjoner leveres av Hjelseth Computer AS.

3.2. Funksjonelle ansvarsområder

Ledelsen er ansvarlig for å evaluere risikoer, definere sikkerhetsmål, sikre bruk av sikkerhetspolicyer, og øke sikkerhetsbevisstheten. IT-ledelsen skal veilede og innlemme sikkerhetstiltak, allokere ressurser, og trene teknisk personell. CISO skal tilby sikkerhetsrådgivning, iverksette sikkerhetsstrategier, og håndtere hendelsesrespons.

3.3. Separasjon av oppgaver

Iverksette separasjon av oppgaver for å redusere risikoen for misbruk. Hvis dette ikke er mulig, bruk alternative kontroller som aktivitetsovervåking.

3.4. Risikostyring

Systemer må håndtere informasjonsrisikoer og ha årlige risikovurderinger. Nye prosjekter og større endringer krever sikkerhetsrisikovurderinger.

3.5. IT ressursforvaltning

Tilordne alt IT-utstyr til en spesifikk enhet eller person, og holde et detaljert inventar av alle IT-ressurser.

3.6. Hendelseshåndtering

Etablere en hendelsesresponsplan og rapportere sikkerhetshendelser til relevant ledelse og ISO.

3.7. Konto-administrasjon og tilgangskontroll

Hver konto må ha en ansvarlig person, og tilgang krever unike bruker-IDer og autentisering. Fjernarbeid krever godkjenning og sikre datahåndteringsprosedyrer.

3.8. Sårbarhetsstyring

Systemer må gjennomgå sårbarhetsskanninger før produksjonsutrulling og regelmessig etterpå. Kritiske systemer krever periodisk penetrasjonstesting.