Policy for informasjonssikkerhet

Dok.nr.:	M-P-902	Versjon:	7	Dok. ansvarlig:	Idar Simonsen
Dok. type:	04. Formular	Rev. dato:	23.01.2025	Godkjent av:	John Roald Lohne

Innhold:

Formål: 2
Omfang: 2
Ansvar og myndighet: 2
Definisjoner: 2
1.0 Prinsipper 3
1.1 Omfanget av ledelsessystemet for informasjonssikkerhet 3
2.0 Tjenesteutsetting av IT 3
2.1 Bruk av eksterne leverandører 3
2.2 Krav til informasjonssikkerhet 3
2.3 Sikkerhetsevaluering 4
2.4 Krav til IT-driftsleverandører 4
3.0 Generelle sikkerhetskrav - prosedyrer 4
3.1 Regulatoriske krav 4
3.2 Risikostyring 4
3.3 Klassifisering av informasjon 5
3.4 Klassifisering av IT-systemer 5
3.5 Tilgangskontroll 5
3.6 Overvåkning av IT-systemer og infrastruktur 6
3.7 Sikkerhetsarkitektur 6
3.8 Krisehåndtering og beredskap 6
3.9 Opplæring – sikkerhetskultur 6
3.10 Fysisk sikkerhet 6
Referanser: 7

Formål:

En informasjonsbehandling som er målorientert, effektiv, lovlig og til å stole på er avgjørende for at Mecan skal lykkes. Tilstrekkelig og balansert informasjonssikkerhet er en kritisk faktor for å understøtte dette.

Policyen skal være et verktøy for ledelsen slik at de når sine mål og støtter Mecans strategiske valg og daglige drift.

Omfang:

Målet for informasjonssikkerhet er å ivareta Mecans verdier ved å sikre:

- ***Integritet***: Informasjon og systemer skal være korrekte, komplette og oppdaterte til enhver tid.
- ***Konfidensialitet***: Konfidensiell eller sensitiv informasjon skal ikke komme på avveie og kun være tilgjengelig for autoriserte personer.
- ***Tilgjengelighe***t: Informasjon og systemer skal være tilgjengelige for personer med tjenstlige behov, med definerte roller og rettigheter.
- ***Regulatoriske krav***: Overholdelse av integritet, konfidensialitet og tilgjengelighet i samsvar med regulatoriske krav som personvernreguleringer og regnskapslovgivning.

Ansvar og myndighet:

Styret i Mecan AS er ansvarlig for å godkjenne Policy for informasjonssikkerhet, og at det er etablert et styringssystem med definerte roller, ansvar og rapporteringsveier.

IKT Sikkerhetsleder er ansvarlig for ajourhold av policyen.

IKT Sikkerhetsleder og **Daglig leder** utvikler den operative oppfølging av policyen i tråd med styrets strategiske mål.

1.0 Prinsipper

Krav og behov for implementering av ledelsessystem for informasjonssikkerhet, cybersikkerhet og personvern skal være basert på risikovurderinger og/eller regulatoriske forhold. MECAN skal som utgangspunkt støtte seg på standarden NS-ISO/IEC 27001:2023.

1.1 Omfanget av ledelsessystemet for informasjonssikkerhet

Eksterne og interne interesseparter behov og forventninger:

Ledelsessystemet tar hensyn til kravene og forventningene fra både eksterne og interne interessenter, som kunder, samarbeidspartnere, ansatte og myndigheter. Disse kravene er identifisert i Landax/Risk: Interesseparter.

Omfang av ledelsessystemet:

a. Ledelsessystemet gjelder for organisasjonens interne informasjonshåndtering og tilknyttede prosesser.

b. Ledelsessystemet omfatter informasjonssikkerhet knyttet til de forretningsprosessene som utføres internt i organisasjonen.

c. Ledelsessystemet inkluderer industriområdet på Husøy og relaterte fysiske sikkerhetsaspekter.

d. Ledelsessystemet inkluderer IT-systemer som eies og driftes internt av organisasjonen, og adresserer nødvendige sikkerhetstiltak og kontroller for disse systemene.

e. Ledelsessystemet etablerer krav og retningslinjer for eksterne leverandører av IKT-tjenester for å sikre at de følger organisasjonens informasjonssikkerhetskrav.

f. Ledelsessystemet omfatter evaluering og overvåking av samsvar med informasjonssikkerhetskrav for tredjepartsleverandørene.

2.0 Tjenesteutsetting av IT

2.1 Bruk av eksterne leverandører

Mecan skal benytte eksterne leverandører for drift, vedlikehold og utvikling av sine IT-systemer og IT-infrastruktur når det er hensiktsmessig og fordelaktig. Dette kan omfatte outsourcing av IT-tjenester, skybaserte løsninger eller andre former for ekstern leveranse.

2.2 Krav til informasjonssikkerhet

Minimumskravet til eksterne tjenesteleverandører er at de skal følge Mecan sin Policy for informasjonssikkerhet. Dette sikrer at leverandørene opererer i samsvar med Mecan sine krav til informasjonssikkerhet og beskyttelse av organisasjonens data og ressurser.

2.3 Sikkerhetsevaluering

Sikkerhetsevaluering skal være en obligatorisk del av prosessene knyttet til tjenesteutsetting. Dette inkluderer evaluering av sikkerhet ved idéfasen for tjenesteutsetting, gjennomføring av leverandørpresentasjoner, valg av leverandør og jevnlig oppfølging av leverandørene.

2.4 Krav til IT-driftsleverandører

Ved tjenesteutsetting av IKT-drift skal kravene angitt i dokumentet "M-AI-023-05 Krav til IT Driftsleverandør" følges. Dette dokumentet spesifiserer de nødvendige kravene og standardene for informasjonssikkerhet som må oppfylles av IT-driftsleverandørene. Det inkluderer blant annet krav til datasikkerhet, tilgangskontroll, sikkerhetskopiering og kontinuitetsplanlegging.

3.0 Generelle sikkerhetskrav - prosedyrer

Mecan skal ha egne dokumenterte prosedyrer for viktige sikkerhetsrelaterte prosesser. Disse prosedyrene skal være gjenstand for årlige revisjoner og oppdateringer for å sikre at de er i tråd med beste praksis og endrede krav.

Se oversikt over «Styrende dokumenter for sikkerhetsrelaterte prosesser» (merkelapp ISO 27001) for en fullstendig liste over prosedyrene som er relevante for informasjonssikkerhet i Mecan.

3.1 Regulatoriske krav

Mecan skal til enhver tid dokumentere og følge aktuelle regulatoriske krav som gjelder for virksomheten. I tillegg til følgende krav, kan det være andre regulatoriske forhold som også gjelder for organisasjonen:

- Lov om behandling av personopplysninger (personopplysningsloven) Mecan skal overholde bestemmelsene i personopplysningsloven og andre relevante personvernreguleringer som gjelder for behandling av personopplysninger. Dette innebærer blant annet at personopplysninger skal behandles på en sikker og lovlig måte, og at de registrertes rettigheter ivaretas.

- Krav med kunder og samarbeidspartnere, regulert i avtaler: Mecan kan være underlagt spesifikke krav fra kunder eller samarbeidspartnere gjennom avtaler som er inngått. Disse kravene må dokumenteres og etterfølges i tråd med avtalens bestemmelser.

3.2 Risikostyring

Mecan sine krav til informasjonssikkerhet for IT-systemer og til prosesser for linjeledelse og prosjekter skal være basert på risikovurdering. Ansvarlige skal være klar over Mecan sine trusler og sårbarheter, og ha et bilde av hva selskapet kan tåle av direkte og indirekte tap. Risikovurderinger skal også vurdere risiko knyttet til egne ansatte eller personer som er påvirket av virksomhetens aktiviteter.

3.3 Klassifisering av informasjon

Mecan skal ha et system for klassifisering av informasjon. Klassifiseringen skal gi en klar forståelse for hvilken informasjon som er:

- **Konfidensiell (Confidential)**; Informasjon som er av virksomhetskritisk eller sensitiv karakter og som kun skal være tilgjengelig for oppnevnte personer. Uautorisert tilgang til eller avsløring av konfidensiell informasjon kan medføre betydelig skade for virksomheten. Konfidensiell informasjon skal tydelig merkes med sin klassifisering, både i elektronisk form og på papir.

- **Intern (Internal)**; Informasjon som er ment å behandles kun internt i virksomheten og som kan skade virksomheten hvis den kommer på avveie. Selv om intern informasjon ikke nødvendigvis er like kritisk som konfidensiell informasjon, er det fortsatt viktig å opprettholde et visst beskyttelsesnivå og begrense tilgangen til denne informasjonen. Intern informasjon skal også merkes med sin klassifisering.

- **Ekstern (External):** Informasjon som deles med eksterne aktører og krever spesifikke retningslinjer for håndtering. Dette inkluderer informasjon som deles med samarbeidspartnere, kunder eller andre

eksterne parter. Det er viktig å sikre at slik informasjon deles på en sikker måte i samsvar med gjeldende retningslinjer og avtaler.

- **Åpen (Public)**; Informasjon som kan betraktes som offentlig tilgjengelig og kan deles med allmennheten uten å påføre skade eller uønskede konsekvenser for virksomheten.

3.4 Klassifisering av IT-systemer

Mecan skal ha et system for klassifisering av IT-systemer. Klassifiseringen skal gjennomgås årlig, og oppsettet skal gi ledelsen en klar forståelse for hvilke som er:

- **Avgjørende**; et system som er kritisk for virksomheten verdikjeder
- **Nyttig**; et system som gjør virksomhetens verdikjeder effektive
- **Støttende**; et system som spiller en mindre rolle i virksomhets verdikjeder

Se «M-AI-023-07 Klassifisering av informasjonssystemer»

3.5 Tilgangskontroll

Tilgang til Mecan sine IT-systemer skal være basert på roller og rettigheter. Tilgangen skal følge tjenstlig behov.

Adgangskontroll-lister til IT-systemene skal gjennomgås minimum 4 ganger hvert år (kvartalsvis). I gjennomgangene skal det vurderes brukernes rettigheter, og en skal trekke tilbake rettigheter som ikke trengs lenger. Brukere med utvidete rettigheter, slik som administratorer, skal fortløpende være gjenstand for nødvendig kontroll.

Adgang til data og systemer som har vital betydning, ref. klassifisert som Avgjørende i pkt 3.4, skal ha sterk autentisering f.eks. totrinnsautentisering.

Alle brukere med tilgang til IKT infrastrukturen skal følge og signere: «M-AI-023-01 Sikkerhetsinstruks og avtale om bruk av IKT infrastruktur og behandling av personopplysninger».

Brukere med utvidede rettigheter skal som et tillegg følge og signere: «M-AI-023-04 Informasjonssikkerhetsinstruks og samtykkeerklæring for brukere med utvidede rettigheter».

Eksterne parter som skal ha tilgang til IKT infrastrukturen skal følge og signere «M-AI-023-03 Informasjonssikkerhetsinstruks og samtykkeerklæring for 3. pars tilgang til IT systemer».

3.6 Overvåkning av IT-systemer og infrastruktur

Mekanismer for teknisk overvåkning av aktiviteter i Mecan sine IT-systemer og infrastruktur skal iverksettes for å unngå ondsinnede eller uhensiktsmessige hendelser, og for å gjøre etterforsking av en eventuell uønsket hendelse enklere. Overvåkningen skal være teknisk, og ikke bryte med personvern, men være av en slik karakter at det tjener formålet for å oppdage og å kunne sette inn tiltak mot uønskede hendelser.

3.7 Sikkerhetsarkitektur

Mecan skal ha en gyldig dokumentert oversikt over tekniske sikkerhetsinstallasjoner og prosesser knyttet til sikkerhetsfunksjoner for IT-systemer og IT-infrastruktur. Denne skal inkludere faste installasjoner, mobile enheter og bruk av remote løsninger.

3.8 Krisehåndtering og beredskap

En prosedyre for hvordan en kommer tilbake fra krisetilstander, der komplette eller deler av vitale prosesser er satt ut av spill, skal være utviklet og dokumentert. En øvelse for å se om prosedyren fungerer i praksis skal utføres årlig. Roller og alternative rolle i krisestab skal oppnevnes.

Sikkerhetskopier og rutiner for oppdateringer av IT-systemer skal være innført som en del av prosessen for å unngå krisetilstand.

Se «M-AI-023-08 IKT Beredskapsinstruks»

3.9 Opplæring – sikkerhetskultur

Opplæring i forståelse av sikkerhet skal være en del av den generelle opplæringen av Mecan sine ansatte. Målet er at IKT sikkerhetskultur skal i alltid skal være en del av de ansatte sine daglige gjøremål. IKT Sikkerhetsleder skal kontinuerlig vurdere behovet for ytterligere opplæring og sikkerhetskampanjer. På generelt grunnlag skal IKT opplæringen være en kontinuerlig prosess.

3.10 Fysisk sikkerhet

I hovedsak skal fysisk sikring av bygninger, arealer og produksjonsutstyr reguleres i egne prosedyrer. Fysisk sikring av IKT Infrastruktur skal inngå i risikoevaluering for IKT og reguleres av denne policy.

Referanser:

- NS-ISO/IEC 27001:2023
- Risikoevaluering