Policy for informasjonssikkerhet i SpareBank 1 SMN

Dato: 10.11.2022
Godkjent av: Styret

Formål

Formålet med Policy for informasjonssikkerhet for SpareBank 1 SMN konsernet er å sikre en systematisk og risikobasert tilnærming for å redusere sårbarheter og risiko for hendelser. Gjennom rutiner og tiltak sørge for å ivareta informasjonsverdier og unngå at data kommer på avveie, herunder integritet, konfidensialitet, tilgjengelighet og regulatoriske krav.

Informasjonssikkerhetspolicyen skal støtte opp under virksomhetens strategiske valg og de daglig drift.

Definisjoner

Målet for informasjonssikkerhet er at en skal ta vare på SpareBank 1 SMN sine verdier. I praksis vil det si at en ivaretar:

- ***Integritet***, som innebærer at informasjon og systemer skal være korrekt, komplett og oppdatert til enhver tid.
- ***Konfidensialitet***, som innebærer at informasjonen er klassifisert, der konfidensiell eller bedrifts sensitive informasjon ikke kommer på avveie, og kan kun aksesseres fra personer med tjenstlige behov.
- ***Tilgjengelighet***, som innebærer at informasjon og systemer skal være tilgjengelig for personer med tjenstlige behov. Dette innebærer også at en har definert roller og rettigheter.
- ***Regulatoriske krav***, som innebærer at en ivaretar integritet, konfidensialitet og tilgjengelighet gitt av regulatoriske forhold.

Ansvar

Styret er ansvarlig for å godkjenne Policy for informasjonssikkerhet.

Konserndirektør Teknologi og Utvikling har ansvaret for at virksomheten har et styringssystem for overholdelse av denne policyen, med klart definerte roller, ansvar og rapporteringsveier i organisasjonen.

Leder for IT og Sikkerhet er ansvarlig for å utvikle og gjennomføre den operative oppfølging av Policy for informasjonssikkerhet, i tillegg til å sette strategiske mål for informasjonssikkerhet.

Informasjonssikkerhetsansvarlig er ansvarlig for at påse at informasjonssikkerhetsmessige forhold ivaretas gjennom risikovurderinger, systemtekniske løsninger og opplæring av ansatte.

Informasjonssikkerhet i SpareBank 1 Utvikling er ansvarlig for hendelseshåndtering, operasjonell informasjonssikkerhet for felles infrastruktur og løsninger, risikovurderinger av felles systemer og tjenester og koordinering av felles aktiviteter mellom selskapene i alliansen.

Alle ledere med linje- eller prosjektledelse, eiere av IT-systemer og IT-infrastruktur har ansvar for at prinsippene gitt i Policy for informasjonssikkerhet blir fulgt for sitt ansvarsområde.

Alle ansatte skal gjennomføre obligatorisk opplæring og være kjent med SpareBank 1 SMN sine grunnleggende retningslinjer for informasjonssikkerhet. Spørsmål rettes til nærmeste leder eller informasjonssikkerhetsansvarlig.

Prinsipper

Krav og behov for implementering av informasjonssikkerhet skal være basert på risikovurderinger og regulatoriske forhold.

Løsepenger og utpressing

SpareBank 1 SMN skal ikke betales ut løsepenger eller tilsvarende ved et angrep eller en hendelse som medfører at data har blitt kryptert eller er kommet uvedkommende i hende.

Utkontraktering av IT

SpareBank 1 SMN skal der det er fordelaktig bruke eksterne leverandører for drift, vedlikehold og utvikling av sine IT-systemer og IT-infrastruktur. Tjenesteleverandørene skal følge SMN sine krav til informasjonssikkerhet.

Utkontrakteringer skal være i henhold til regulatoriske krav om ivaretakelse av kontroll med alle sider av utkontrakteringen. Utkontrakteringen skal gjennomføres i henhold til vår policy for utkontraktering av virksomhet i SpareBank 1 SMN og Policy for utkontraktering av IT-tjenester i SpareBank 1-alliansen.

SpareBank 1 SMN skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten i henhold til regulatoriske krav. Prosessen skal blant annet definere klare ansvarsforhold og omfatte oppfølging av tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen.

Generelle sikkerhetskrav

SpareBank 1 SMN skal ha egne dokumenterte rutiner for viktige sikkerhetsrelaterte prosesser. Rutinene nevnt under i dette kapitlet skal være gjenstand for årlige revisjon og oppdatering

a. Regulatoriske krav

SpareBank 1 SMN skal til enhver tid følge aktuelle regulatoriske krav.

b. Risikostyring

SpareBank 1 SMN sine krav til informasjonssikkerhet for IT-systemer og til prosesser for linjeledelse og prosjekter skal være basert på risikovurdering. Ansvarlige skal være klar over SpareBank 1 SMN sine trusler og sårbarheter og ha et bilde av hva virksomheten kan tåle av direkte og indirekte tap. Det skal utføres risikovurderinger ved innføring av nye systemer/tjenester eller ved endringer på eksisterende systemer/tjenester. Risikovurderinger skal også vurdere risiko knyttet til egne ansatte eller personer som er påvirket av virksomhetens aktiviteter.

c. Klassifisering av informasjon

SpareBank 1 SMN skal ha et system for klassifisering av informasjon.

d. Klassifisering av IT-systemer

SpareBank 1 SMN skal ha et system for klassifisering av IT-systemer. Det skal være en årlig gjennomgang for klassifiseringen av IT-systemer og det skal gi en klar forståelse for de forskjellige systemenes kritikalitet.

e. Tilgangskontroll

Tilgang til SpareBank 1 SMN sine IT-systemer skal være basert på roller og rettigheter. Tilgangen skal følge tjenstlig behov og tilpasses ved endringer i rolle/stilling. Det skal årlig gjennomføres revisjon av tilganger til IT-systemene, der en trekker tilbake rettigheter som ikke trengs lenger. Brukere med utvidete rettigheter, slik som administratorer, skal fortløpende være gjenstand for nødvendig kontroll.

f. Overvåkning av IT-systemer og infrastruktur

Mekanismer for teknisk overvåkning av aktiviteter i SpareBank 1 SMN sine IT-systemer og infrastruktur skal være implementert for å unngå ondsinnet eller uhensiktsmessige hendelser og for å gjøre undersøkelser 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. SpareBank 1 SMN skal ha en komplett og oppdatert systemoversikt.

g. Sikkerhetsarkitektur

SpareBank 1 SMN skal ha en gyldig dokumentert oversikt over tekniske sikkerhetsinstallasjoner og prosesser knyttet til sikkerhetsfunksjoner for IT-systemer og IT-infrastruktur.

h. Krisehåndtering og beredskap

Alle (informasjons-)sikkerhetshendelser skal behørig håndteres og ivaretas.
En prosedyre for hvordan en kommer tilbake fra krisetilstander, der komplette eller deler av viktige prosesser er satt ut av spill, skal være utviklet og dokumentert. Det skal jevnlig, og minimum årlig, gjennomføres øvelser for å teste prosedyrene.
Sikkerhetskopier og rutiner for oppdateringer av IT-systemer skal være innført som en del av prosessen for å unngå krisetilstand

i. Opplæring – sikkerhetskultur

Opplæring i forståelse av sikkerhetsmessige forhold og sikkerhetskultur skal være en del av den obligatoriske opplæringen av SpareBank 1 SMN sine ansatte. Den enkelte ansatte er selv ansvarlig for å gjennomføre obligatorisk opplæring. Formålet er å integrere sikkerhet i ansattes daglige gjøremål for å unngå hendelser som fører til økonomisk tap, tap av data eller tap av omdømme.
Opplæringen skal være en kontinuerlig prosess.

j. Fysisk sikkerhet

Fysisk sikkerhet omfatter adgangskontrollanlegg, videoovervåking, alarmsystemer, vektertjenester og tilhørende sikkerhetsteknisk overvåking. Grunnprinsippet for fysisk sikring av lokasjoner skal ta utgangspunkt i en risikobasert tilnærming.
Hovedformålet skal være å forebygge uønskede hendelser rettet mot liv og helse til ansatte, kunder og besøkende, verdier, omdømme, informasjon som behandles og forretningsdriften.
Tilgang til SpareBank 1 SMN-konsernets bygninger og arealer skal gis etter tjenstlig behov.
Omfang av videoovervåkning og utlevering av bilde-/videomateriale skal være hjemlet i regulatoriske krav.