Policy for informasjonssikkerhet og digital motstandsdyktighet

Dokumentet beskriver sentrale overordnede prinsipper knyttet til informasjonssikkerhet og digital motstandsdyktighet i SpareBank 1 SMN konsern.

Innholdsansvarlig	Informasjonssikkerhetsansvarlig
Innholdseier	Konserndirektør Teknologi og Utvikling
Informasjonsklassifisering	Intern
Gjelder for	SpareBank 1 SMN konsern
Godkjenningsnivå	Styret
Sist godkjent	11.02.2025
Sist revidert	29.01.2025
Krav om styregodkjenning i datterselskaper?	Nei

Innhold

1. FORMÅL

Formålet med Policy for Informasjonssikkerhet og digital motstandsdyktighet for SpareBank 1 SMN (SMN) er å sikre en systematisk og risikobasert tilnærming til informasjonssikkerhetskrav og rutiner, samt å kontinuerlig forbedre og øke konsernets digitale motstandsdyktighet, samt redusere sårbarheter og risiko for informasjonssikkerhetshendelser. Informasjonssikkerhetsrisiko skal håndteres og aksepteres innenfor rammene som er satt for risikotoleranse i virksomheten.

Informasjonssikkerhetspolicyen skal sørge for at informasjonssikkerhetsmål og prinsipper støtter konsernets strategiske mål om kvalitet i alt vi gjør, bidra til å skape ett SMN og samtidig øke digitaliseringen og bruk av datadrevet innsikt. Informasjonssikkerhetsarbeidet skal legge til rette for at SMN kan lede an utviklingen av sparebank-Norge, og at arbeidet vi gjør er bærekraftig.

Dette policydokumentet skal revideres årlig og godkjennes av styret ved vesentlige endringer. Policyen skal uansett styregodkjennes hvert tredje år.

2. MÅLGRUPPE

Informasjonssikkerhetspolicyen gjelder for SMN konsernet, inkludert datterselskaper.

3. DEFINISJONER

Autentisitet – informasjon er autentisk, at den er ekte og ikke forfalsket.
Integritet – informasjon og systemer skal være korrekt, komplett og oppdatert til enhver tid.
Konfidensialitet – informasjonen er klassifisert, der konfidensiell eller bedrifts sensitive informasjon ikke kommer på avveie, og kan kun aksesseres fra personer med tjenstlige behov.
Robusthet – virksomhetens eller systemers motstandskraft og evne til å tåle påkjenninger og hendelser, og komme godt og styrket ut av hendelsen.
Tilgjengelighet – informasjon og systemer skal være tilgjengelig for personer med tjenstlige behov. Dette innebærer også at en har definert roller og rettigheter.

4. STYRENDE PRINSIPPER OG KRAV

SpareBank1 SMN skal ha et styringssystem for informasjonssikkerhet som fungerer som virksomhetens internkontroll på informasjonssikkerhetsområdet. Styringssystemet skal sikre konfidensialitet, integritet og tilgjengelighet for informasjon som benyttes og behandles i konsernet, og sikre god robusthet.

Implementering og prioritering av informasjonssikkerhetstiltak skal være risikobasert, og følge endringer i trusselbildet og regulatoriske forhold. SMN skal bidra til bedre sikkerhet og stabilitet i samfunnet og i finansiell sektor gjennom jevnlig innhenting og deling av relevant trusselinformasjon.

Informasjonssikkerhetsarbeidet skal integreres i arbeidet i linjen, og informasjonssikkerhetsarbeidet skal bygge på gode holdninger blant medarbeiderne og en god sikkerhetskultur.

Nye trusler skal identifiseres og vurderes fortløpende, og når uønskede hendelser inntreffer skal hendelseshåndterings- og beredskapstiltak være på plass og bidra til å begrense skaden og gjenopprette normal drift.

Løsepenger og utpressing
SMN skal ikke utbetale løsepenger eller tilsvarende ved et digitalt angrep eller en hendelse som medfører at data har blitt kryptert og/eller er kommet uvedkommende i hende.

4.1 Generelle sikkerhetskrav

SMN skal ha egne dokumenterte standarder med sikkerhetsprinsipper og -krav, og tilhørende rutiner for viktige sikkerhetsrelaterte prosesser. Sikkerhetskrav og rutiner skal være gjenstand for årlig revisjon og oppdatering.

Informasjonssikkerhetsarbeidet skal gjennomføres og kontrolleres i samsvar med SMNs internkontrollsystem. Styringssystem for informasjonssikkerhet er en del av internkontrollen, og skal gi nødvendig struktur og føringer for arbeidet med informasjonssikkerhet, og det skal samle alle styrende dokumenter som er relevante for informasjonssikkerhetsarbeidet.

4.1.1 Regulatoriske krav

SMN skal til enhver tid etterleve gjeldende regulatoriske krav innenfor informasjonssikkerhetsområdet.

4.1.2 Risikostyring

SMNs arbeid med informasjonssikkerhet, inkludert prioritering og implementering av risikoreduserende sikringstiltak, skal gjennomføres ved en risikobasert tilnærming. Ved innføring av nye systemer/tjenester eller ved endringer på eksisterende systemer/tjenester, skal det utføres risikovurderinger. Endringer som kan få betydning for informasjonssikkerheten skal risikovurderes.

SMN skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IT-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. SMN skal ha fastsatte kriterier for akseptabel risiko forbundet med informasjonssikkerhet og bruk av IT-systemer.

Styring av informasjonssikkerhetsrisiko skal inngå i konsernets samlede styringsarbeid. Risikovurderinger knyttet til informasjonssikkerhet skal inngå i grunnlag for konsernets overordnede risikovurderinger slik at total informasjonssikkerhetsrisiko for virksomheten kan reduseres, og mulighetene for hensiktsmessig sikring av konsernets viktigste verdier, verdikjeder og infrastruktur, samt strategisk måloppnåelse øker.

Risikovurdering innenfor informasjonssikkerhet skal minst gjennomføres årlig eller ved vesentlige endringer iht. IKT-forskriften eller annet relevant lovverk.

4.1.3 Klassifisering av informasjon og systemer

SMN skal ha fastsatte prinsipper for klassifisering av informasjon. SMN skal ha et system for klassifisering av IT-systemer som skal ta utgangspunkt i forretningskritikalitet. Klassifiseringen av IT-systemer skal gjennomgås årlig, og det skal foreligge en klar indikasjon på årsaken til de forskjellige systemenes kritikalitet.

4.1.4 Identitets- og tilgangsstyring

SMN skal ha en standard for identitets- og tilgangsstyring. Tilgang til informasjon, systemer og infrastruktur skal være basert på tjenstlig behov, være rollebasert og i henhold til “least privilege" prinsippet slik at ansatte kun skal ha tilganger de trenger for å løse deres arbeidsoppgaver.

4.1.5 IT-systemer og -infrastruktur

SMN skal ha styrende prinsipper og krav til bruk av IT-systemer og -verktøy, som skal inkludere krav til bruk av PC, flyttbare medier, skytjenester, passord, logging, e-post og mobile enheter. SMN skal ha en komplett og oppdatert IT-systemoversikt. SMN skal ha mekanismer for teknisk overvåkning av aktiviteter i SMNs IT-systemer og infrastruktur. Teknisk overvåkning skal ikke bryte med personvern- og menneskerettigheter. Rutiner for sikkerhetskopier og oppdateringer av IT-systemer skal dokumenteres som preventive tiltak.

4.1.6 Sikkerhetsarkitektur

SMN skal ha en standard for- og dokumenterte krav til en sikkerhetsarkitektur, samt en gyldig dokumentert oversikt over tekniske sikkerhetsinstallasjoner og prosesser knyttet til sikkerhetsfunksjoner for IT-systemer og IT-infrastruktur.

4.1.7 Krisehåndtering og beredskap

SMN skal ha en plan for forretningskontinuitet og en tilhørende øvingsplan som står i forhold til trusselbildet og forretningskritikalitet. SMN skal ha dokumenterte rutiner for vurdering, klassifisering, kontrollering, håndtering og læring av (informasjons-)sikkerhetshendelser. Det skal jevnlig, og minimum årlig, gjennomføres øvelser for å teste rutinene.

SMN skal ha dokumenterte rutiner for å vurdere- og sikre forretningskontinuitet, som skal beskrive hvordan organisasjonen kommer tilbake fra krisetilstander der hele eller deler av viktige prosesser er utilgjengelige.

4.1.8 Sikkerhetskultur

SMN skal ha et program for opplæring og bevisstgjøring innen informasjonssikkerhet og digital motstandsdyktighet, og opplæringen skal ha et kompleksitetsnivå som står i samsvar med de ansattes roller, ansvar og funksjoner. Programmet skal også inneholde trening/testing. Programmet skal være obligatorisk for alle ansatte. Alle ansatte i SMN skal få informasjon om policyer, standarder og rutiner innen informasjonssikkerhet som er relevant for deres rolle, samt nødvendig opplæring innen informasjonssikkerhet for å kunne ivareta sitt sikkerhetsansvar.

SMN skal ha etablerte prosesser, rutiner, tiltak og kontrollmekanismer som gir god beskyttelse av verdier mot tilsiktede uønskede handlinger utført av egne ansatte, konsulenter, vikarer og leverandører. Tiltakene skal omfatte hele livsløpet i et ansettelsesforhold, - før, under, etter og ved avslutning.

4.1.9 Fysisk sikkerhet og personellsikkerhet

All fysisk sikkerhet skal ta utgangspunkt i en risikobasert tilnærming basert på det til enhver tid gjeldende trusselbilde. SMN skal følge Alliansens sikkerhetsstandard for fysisk sikring av lokasjoner.

Tilgang til SMN-konsernets bygninger og arealer skal gis etter tjenstlig behov. Utlevering av bilde-/videomateriale skal være hjemlet i regulatoriske krav.

4.1.10 Innkjøp og utkontraktering av IT

SMN skal ha en policy for utkontraktering, med tydelig definerte sikkerhetsprinsipper og krav til utkontrakteringsprosessen, til leverandører, og en strukturert prosess for leverandøroppfølging.

Utkontrakteringer skal gjennomføres i henhold til Policy for utkontraktering av virksomhet i SpareBank 1 SMN og Policy for utkontraktering av IT-tjenester i SpareBank 1-alliansen.

SMN skal sikre at informasjonssikkerhet er en integrert del av alle innkjøp knyttet til IT og Informasjonssystemer, og skal derfor ha dokumenterte krav til informasjonssikkerhet i innkjøpsprosesser.

4.1.11 Utvikling og bruk av kunstig intelligens

SMN skal ha dokumenterte sikkerhetsprinsipper og -krav til utvikling og bruk av kunstig intelligens i konsernet.

"Innhold i retningslinjen som er av sensitiv eller konfidensiell art er tilbakeholdt for offentlig publisering."

5. ORGANISERING OG ANSVAR

Styret har ansvar for at den digitale infrastrukturen forvaltes og beskyttes på lik linje med andre viktige verdier i SMN. Styret er ansvarlig for å godkjenne Policy for informasjonssikkerhet. Styret skal til enhver tid aktivt holde seg oppdatert på trussel- og risikobildet for finansbransjen, slik at de har tilstrekkelig kunnskap og ferdigheter til å forstå og vurdere IKT-risiko og dens påvirkning på SMN som virksomhet. Styret skal delta på all obligatorisk informasjonssikkerhetsopplæring.
Styret skal minst årlig oppdateres på sikkerhetstilstanden i konsernet med en vurdering av og anbefalinger for digital motstandsdyktighet. Styret skal også ved større IT-hendelser informeres innen rimelig tid om håndtering og konsekvenser av hendelsen, samt tiltak/etablerte kontroller for å hindre gjentakelse av en slik hendelse i etterkant.

Konsernsjef er risikoeier for virksomhetens samlede måloppnåelse, og sammen med styret har konsernsjef det overordnede og endelige ansvaret for informasjonssikkerheten.

Konserndirektør Teknologi og Utvikling har ansvaret for at virksomheten har et styringssystem for informasjonssikkerhet og en policy for informasjonssikkerhet.

Konserndirektører for forretningsområder/divisjoner er ansvarlige for at prinsippene gitt i informasjonssikkerhetspolicyen etterleves innen sitt ansvarsområde

Leder for IT og Sikkerhet er ansvarlig for å utvikle og gjennomføre den operative oppfølgingen av Policy for informasjonssikkerhet sammen med informasjonssikkerhetsansvarlig.

Informasjonssikkerhetsansvarlig er ansvarlig for å sette strategiske mål for informasjonssikkerhet og har det forvaltningsmessige ansvaret for styringssystem for informasjonssikkerhet i henhold til denne policyen. I tillegg skal informasjonssikkerhetsansvarlig påse at informasjonssikkerhetsmessige forhold ivaretas gjennom risikovurderinger, systemtekniske løsninger og bevisstgjøring og opplæring av ansatte.

6. FORVALTNING OG REVISJON AV POLICY

Policyen skal revideres ved behov og godkjennes av styret ved endringer. Policyen skal uansett godkjennes av styret hvert tredje år.

7. HÅNDTERING AV AVVIK OG SIKKERHETSBRUDD

Avvik fra denne policyen skal registreres i hendelsesregistreringssystemet i henhold til interne rutiner.

Dersom informasjon blir tilgjengelig for uvedkomne (brudd på konfidensialitet), blir endret utilsiktet eller av uvedkomne (brudd på integritet), eller at nødvendig informasjon ikke er tilgjengelig ved behov (brudd på tilgjengelighet) skal dette registreres som et inforasjonssikkerhetsbrudd i hendelsesregistreringssystemet i henhold til interne rutiner.