

Sikkerhetspolicy i Sparebank 1 Nord-Norge



Innholdsfortegnelse

1. BAKGRUNN OG FORMÅL	3
2. SIKKERHETSMÅL	3
3. ORGANISERING OG ANSVAR	3
3.1 STYRET	3
3.2 KONSERNSJEF	3
3.3 LEDERE OG ANSATTE	3
3.4 AVDELING FOR RISIKOSTYRING	4
3.5 COMPLIANCEAVDELINGEN	4
3.6 PERSONVERNOMBUD (PVO)	4
3.7 SIKKERHETSANSVARLIG	4
3.8 INFORMASJONSSIKKERHETSANSVARLIG	4
3.9 BANKENS FORHOLD TIL SPAREBANK 1 UTVIKLING	4
4. STYRINGSSYSTEM OG KONTROLL	4
5. RISIKOVURDERING	5
6. SIKKERHETSTILTAK	5
7. UTKONTRAKTERING OG ANSKAFFELSE	5
8. UTVIKLING OG ENDRINGSHÅNDTERING	5
9. SYSTEMVEDLIKEHOLD OG DRIFT	5
10.HENDELSESHÅNDTERING OG KRISEBEREDSKAP	5
11.HÅNDTERING AV AVVIK	5
12.DEFINISJON AV SENTRALE BEGREPER	5
REFERANSER	FEIL! BOKMERKE ER IKKE DEFINERT.

1. BAKGRUNN OG FORMÅL

SpareBank 1 er en sterk merkevare, og en betydelig aktør i det norske finansmarkedet. Derfor er det viktig å ha en policy som gir et tilfredsstillende sikkerhetsnivå og bidrar til en hensiktsmessig organisering av sikkerhetsarbeidet og etterlevelse av gjeldende lovkrav. Sparebank1 Nord-Norge er også utvalgt som en samfunnskritisk virksomhet av Nasjonal Sikkerhetsmyndighet. Dette forplikter oss å ta jobben med sikkerhet og informasjonssikkerhet på alvor. Vi er i tillegg en betydelig aktør i de nord-norske samfunn som nyter stor tillit i befolkningen.

Ved utarbeidelsen av denne policyen har vi tatt utgangspunkt i Sparebank 1 Utviklings *Sikkerhetspolicy for SpareBank 1- alliansen* hvor bankenes representanter i SpareBank 1-alliansens sikkerhetsråd har gitt sine innspill.

Denne policy gjelder for alle selskap i Sparebank 1 Nord-Norge konsernet.

2. SIKKERHETSMÅL

Den overordnede målsetningen for alt sikkerhetsarbeidet i SpareBank 1 Nord-Norge AS er gjennom en systematisk og risikobasert tilnærming å:

- Beskytte liv og helse til ansatte, kunder og besøkende.
- Sikre SpareBank 1 Nord-Norges AS sine verdier og omdømme, samt den informasjon som behandles.
- Sørge for at myndigheter, kunder, ansatte og samarbeidspartnere, har tillit til at informasjon behandles på en betryggende måte.
- Å sørge for at sikkerhetsarbeidet understøtter den til enhver tid gjeldende forretnings og risikostrategien.
- Sørge for sikker og stabil drift.
- Sikre at vi til enhver tid er i samsvar med kravene til sikkerhetsarbeidet i gjeldende lover og forskrifter, herunder å ivareta kunders og ansattes personvern.

Konfidensialitet, integritet og tilgjengelighet må vektes med utgangspunkt i forretningsbehov og risikobilde.

3. ORGANISERING OG ANSVAR

Sikkerhet skal inngå som en naturlig prosess i den daglige driften, og det skal være nødvendig kapasitet og kompetanse til å ivareta sikkerhetsbehovene. I tillegg slår personvernlovgivningen fast at robusthet er viktig for å dekke den siden av regulatoriske krav.

3.1 Styret

Styret har det overordnede ansvaret for sikkerhetsarbeidet, og blir informert om denne policyen.

3.2 Konsernsjef

Konsernsjefen har ansvar for det daglige sikkerhetsarbeidet. Konsernsjefen *kan* delegerer utførelsen av sikkerhetsarbeidet til en eller flere definerte roller.

3.3 Ledere og ansatte

Ledere har et operativt sikkerhetsansvar for sitt område, og hver enkelt ansatt og innleid personell har ansvar for å sette seg inn i reglene for sikkerhet og etterleve disse.

3.4 Avdeling for risikostyring

Er ansvarlig for å etablere metoder, verktøy, systemer og rutiner for god, effektiv og helhetlig styring og kontroll av operasjonell risiko i organisasjonen. Avdeling for risikostyring er også ansvarlig for å støtte og utfordre styret, ledelsen og resten av organisasjonen for å sikre profesjonalisert styring av operasjonell risiko, samt produsere relevant rapportering på området slik at styret og ledelsen holdes løpende orientert på utvikling og risikonivå.

3.5 Complianceavdelingen

Er ansvarlig for å identifisere, vurdere, gi råd, overvåke og rapportere konsernets compliance-risiko.

3.6 Personvernombud (PVO)

PVO er en sentral, rådgivende, koordinerende, kontrollerende og rapporterende rolle i hele organisasjonen knyttet til etterlevelse av personvernregelverket.

3.7 Sikkerhetsansvarlig

Har ansvaret for konsernets sikkerhetsarbeid, og skal løpende vurdere trusselbildet sammen med felles sikkerhetsressurser i alliansen. Sikkerhetsansvarlig leder konsernets krisestab.

3.8 Informasjonssikkerhetsansvarlig

Skal sørge for påliteligheten og sikkerheten som knyttes til innhenting, overføring og lagring av informasjon i Sparebank1 Nord-Norge, og at konsernet følger de lover og regler samt interne krav og retningslinjer som er til enhver tid gjeldende for fagområdet. Rollen skal også være en rådgiver for konsernledelse og styret dersom de trenger avklaringer i forbindelse med behandling av saker som er knyttet til fagområdet.

3.9 Bankens forhold til Sparebank 1 Utvikling

SB1 Utvikling (SB1U) er koordinator og fasilitator for sikkerhetsaktiviteter i SpareBank 1-alliansen, og bistår Sparebank 1 Nord-Norge med kompetanse og gjennomføring av prosesser. SB1U ansvar overfor bankene og selskapene er regulert i egne tjenesteavtaler, herunder operativt sikkerhetsarbeid, felles infrastruktur og forhold til underleverandører.

Sparebank 1 Nord er premissgivere for løsninger som de leverer til sine kunder gjennom SB1U. SB1U kan være premissgiver for enkeltsselskaper når dette er avtalt.

4. STYRINGSSYSTEM OG KONTROLL

Sikkerhetsarbeidet skal gjennomføres i samsvar med et styringssystem for sikkerhet. Styringssystemet gir nødvendig struktur og føring for sikkerheten, og samler alle styrende dokumenter som er relevante for sikkerhetsarbeidet. Sparebank 1 Nord-Norge benytter seg av SB1U styringssystem for sikkerhet, men gjør løpende vurdering av om det må etableres eget styringssystem.

Vårt felles ISMS er basert på et ISO 27001 rammeverk for å sikre at det dekker alle områder rundt informasjonssikkerhetsarbeid.

5. RISIKOVURDERING

Det skal gjennomføres risikovurdering av systemer, lokasjoner, leveranser, prosesser og tiltak med betydning for virksomheten. Formålet med risikovurderingen er å påvise risiko, fastsette sikkerhetsbehov og hensiktsmessige sikkerhetstiltak. Utføring av risikovurdering skal gjøres i samsvar med etablerte standarder.

6. SIKKERHETSTILTAK

Sparebank 1 Nord-Norge og SB1U skal ha hensiktsmessige tiltak for å sikre kunder, personell, utstyr, lokasjoner, systemer og informasjon, samt gjennomføre nødvendig sikkerhetsopplæring og holdningsskapende arbeid av alt personell som utfører oppgaver for SpareBank 1 Nord-Norge konsernet.

7. UTKONTRAKTERING OG ANSKAFFELSE

Utkontraktering av virksomhet skal skje etter fastsatt policy for utkontraktering, og styrebehandles når dette er nødvendig. Alle anskaffelser skal gjøres iht. til interne styrende dokumenter.

8. UTVIKLING OG ENDRINGSHÅNDTERING

Før utviklet eller endret løsning produksjons-settes, skal risikovurdering og nødvendig testing gjennomføres. Løsning kan settes i ordinær drift når ansvarlig har akseptert risikoen.

9. SYSTEMVEDLIKEHOLD OG DRIFT

Drift og systemvedlikehold skal gjennomføres på en forsvarlig måte og etter gjeldende styrende dokumenter. Utviklingsressurser kan gis enkelte oppgaver knyttet til systemvedlikehold og drift.

10. HENDELSESHÅNDTERING OG KRISEBEREDSKAP

Alle ansatte har en plikt til å varsle ved mistanke om eller ved oppdagede sikkerhetshendelser. Sparebank 1 Nord-Norge skal følge SpareBank 1s felles krise- og kontinuitetsplanverk, og ha etablert egen kriseplan med beskrivelse av kriseløsninger. Det skal jevnlig gjennomføres opplæring, øvelser og testing av planverket.

11. HÅNDTERING AV AVVIK

Styret gir konsernsjefen fullmakt til å godkjenne avvik fra bestemmelsene i denne policy. Styret skal holdes orientert om slike avvik.

12. DEFINISJON AV SENTRALE BEGREPER

Felles infrastruktur: Med felles infrastruktur menes områder som Nettbank/Portal(er), felles kontorkanalapplikasjoner, webservere, felles nettverk (stamnett), Internettkoblinger, Internett mail-tjenester, felles brannmur og tilknytninger mot eksterne aktører.