

Sikkerhet – Konsernpolicy

Innhold

1	Formål.....	2
2	Virkeområde.....	2
3	Roller og ansvar	2
4	Overordnede sikkerhetsmål.....	3
4.1	DNB skal ha et riktig og styrt sikkerhetsnivå	3
4.2	Sikkerhetsarbeidet skal være godt integrert i DNBs virksomhet	3
4.3	DNB skal prioritere sikkerhetsarbeidet	3
4.4	DNB skal fremme åpenhet og god sikkerhetskultur.....	4
4.5	Sikkerhetsnivået i DNB skal evalueres.....	4

1 Formål

DNB har ansvar for å beskytte verdier hos DNB som tilhører kunder, ansatte, våre eiere, virksomheten, partnere og samfunnet ellers. Sikkerhet i DNB handler om å sikre vår evne til å unngå skade eller tap av verdier som følge av uønskede, tilsiktede handlinger, samt teknologiske, miljømessige eller menneskelige feil og uhell.

I tillegg er god sikkerhetsstyring og -kontroll en viktig driver for å styrke innovasjonskraften og kundenes tillit til banken. God sikkerhet er viktig for DNBs omdømme og samfunnsansvar.

Denne policyen fastsetter roller og ansvar innenfor sikkerhetsarbeidet og hvordan DNB skal styre sikkerheten og sette overordnede mål for arbeidet med sikkerhet i DNB. Dokumentet omfatter ikke arbeid med sikkert arbeidsmiljø/HMS. Se People Guide for informasjon om arbeidsmiljø/HMS.

2 Virkeområde

Dette dokumentet gjelder for alle fast og midlertidig ansatte i konsernet.

Videre gjelder dokumentet som utgangspunkt for alle selskaper i DNB-konsernet, inkludert konsernets internasjonale virksomhet.

Det styrende dokumentet gjelder ikke for:

1. Selskaper der DNB ikke har bestemmende innflytelse som definert i aksjeloven, eller selskaper DNB eier i fellesskap med andre finansforetak. I slike selskaper bør DNB gjennom sin eierinnflytelse i styringsorganer arbeide for at selskapet skal ha styringsprinsipper knyttet til samfunnsansvar og etikk som er i tråd med DNBs egne styringsprinsipper.
2. Selskaper som DNB har overtatt eller anskaffet med sikte på midlertidig eie. Slike selskaper skal implementere og etterleve prinsipper for etikk og samfunnsansvar som er i tråd med DNBs egne styringsprinsipper.

Lover og andre bindende eksterne regler går ved motstrid foran dette dokumentet. Ansvarlig for implementering skal varsle dokumenteier ved slik motstrid.

3 Roller og ansvar

Konsernsjefen er ansvarlig for sikkerheten i DNBs daglige virksomhet og skal minimum årlig gjennomgå og evaluere ytelse og grad av sikkerhetsmåloppnåelse med hele eller deler av konsernledelsen. Gjennomgangen skal sikre at konsernsjefen kjenner status for sikkerheten i DNB og tar nødvendige beslutninger. Konsernsjefen skal informere styret om resultatene av gjennomgangen.

Konserndirektøren for Technology & Services (T&S) er dokumenteier og ansvarlig for å etablere konsernets funksjon for helhetlig sikkerhetsstyring, og for å sikre god styringsinformasjon til konsernledelsen og styret.

Sikkerhetsdirektøren (CSO/CISO¹) har et konsernansvar for sikkerhet og leder Group Security. Sikkerhetsdirektøren skal lede sikkerhetsarbeidet i konsernet og iverksette sentraliserte tiltak og aktiviteter som skal benyttes i hele konsernet for å fastsette sikkerhetsmål for konsernet og opprettholde et riktig sikkerhetsnivå. Sikkerhetsdirektøren skal evaluere sikkerhetsnivået og rapportere dette til konsernsjefen og styret.

¹ Chief Security Officer (CSO) og Chief Information Security Officer (CISO)

Konserndirektørene eier risiko knyttet til eget område og har ansvar for gjennomføringen av sikkerhetsarbeidet i egne forretnings-, stabs- og støtteområder. Konserndirektørene skal sikre at sikkerhetsdirektøren involveres i prosesser og beslutninger som kan ha betydning for sikkerhetsansvaret på konsernnivå. Konserndirektørene skal påse at sikkerhetsdirektøren varsles om sikkerhetsrisikoer og avvik fra etterlevelse av sikkerhetsrutiner og -prosedyrer, som grunnlag for ledelsens evaluering og gjennomgang av sikkerhet.

Group Risk Management og Group Compliance utgjør konsernets andre forsvarslinje og er ansvarlig for å gjennomføre en uavhengig kontroll av sikkerheten i DNB.

Konsernrevisjonen gjennomgår og reviderer sikkerhet som tredje forsvarslinje.

Alle ansatte skal sette seg inn i hvilke sikkerhetsregler som gjelder, og aktivt bidra til god sikkerhet i DNB.

Avvik fra denne policyen skal håndteres av ansvarlig enhet og rapporteres i henhold til prosess for avviksrapportering.

4 Overordnede sikkerhetsmål

4.1 DNB skal ha et riktig og styrt sikkerhetsnivå

DNBs sikkerhetsmål settes på grunnlag av regulatoriske krav og forventinger gitt av myndigheter i de land vi opererer i og inngåtte avtaler, samt konsernets mål og risikoappetitt. Sikkerhetsmål utdypes basert på internasjonalt akseptert sikkerhetspraksis.

Sikkerhetsnivået skal innfri de sikkerhetsmålene som er satt, muliggjøre håndtering av risiko og støtte konsernets forretningsmessige behov og forventninger.

Sikkerhetsarbeidet i DNB skal forebygge sikkerhetshendelser, men også oppdage, håndtere og forhindre gjentakelse av sikkerhetshendelser.

DNB skal styre sikkerhet i tredjepartsforhold, og oppdragsgiver² er ansvarlig for et riktig sikkerhetsnivå når hele eller deler av virksomheten utføres av eksterne leverandører og tredjeparter.

4.2 Sikkerhetsarbeidet skal være godt integrert i DNBs virksomhet

Sentrale faktorer for å oppnå riktig sikkerhetsnivå er godt integrert sikkerhetsorganisering, hensiktsmessige sikkerhetsaktiviteter og tekniske tiltak, som utføres og vedlikeholdes som en del av virksomheten ellers.

Virksomhetens risikometodikk og verktøy skal bidra til å identifisere, vurdere og håndtere sikkerhetsrisiko som en del av den helhetlige risikostyringen i konsernet.

4.3 DNB skal prioritere sikkerhetsarbeidet

Etablering og opprettholdelse av et riktig sikkerhetsnivå er avgjørende for DNBs virksomhet, for konsernets gjennomføring av samfunnsoppdraget, og for samarbeidspartnere og kunder.

DNB må ha tilstrekkelig kompetanse og kapasitet til å oppnå riktig sikkerhetsnivå og gjennomføre sikkerhetsarbeidet på alle nivåer. DNB skal organisere spesialistfunksjoner for å ivareta nødvendig sikkerhetskompetanse til å støtte virksomheten i utøvelsen av sikkerhetsarbeidet. Det skal avsettes tilstrekkelige drifts- og investeringsmidler som er nødvendige for å ivareta et riktig sikkerhetsnivå.

² IT contract owner eller IT supplier manager

4.4 DNB skal fremme åpenhet og god sikkerhetskultur

DNB har en viktig samfunnsrolle og skal så langt det lar seg gjøre være åpne om sikkerhetsarbeidet internt og eksternt. CSO kan dele informasjon og erfaringer med aktuelle interessenter og fagmiljøer for å styrke bevissthet og kompetanse rundt sikkerheten i samfunnet generelt, og i finansnæringen spesielt.

DNB skal aktivt fremme positive holdninger, nødvendig kompetanse og god adferd rundt sikkerhetsarbeidet. Det skal gjennomføres periodiske, og minimum årlige, aktiviteter der de ansatte øver på rutiner og prosedyrer. Dette skal utvikle holdninger og kompetanse blant de ansatte som fremmer god sikkerhet, slik at en hensiktsmessig sikkerhetskultur innarbeides som en naturlig del av virksomheten. Det skal være enkelt og trygt å stille spørsmål og å melde fra om uklarheter, feil, mangler og brudd på sikkerhet i DNB.

4.5 Sikkerhetsnivået i DNB skal evalueres

Oppfølging og kontroll av sikkerhetsnivået gjøres i henhold til de **tre forsvarslinjene**³.

DNB skal følge opp at organisasjonen, eksterne leverandører og tredjeparter oppnår riktig sikkerhetsnivå og ha en prosess for å evaluere sikkerhetsarbeidet. Prosessen skal være integrert med konsernets styringsprosesser og internkontrollen. Det skal legges til rette for at effekten av sikkerhetsarbeidet kan måles på en enhetlig måte.

Sikkerhetshendelser skal gjennomgås og evalueres av involverte funksjoner slik at læring fra hendelser forbedrer og styrker DNBs sikkerhetsarbeid.

³ Se «DNBs styringsprinsipper»