

PNT-BEREDSKAPSVEILEDER

Veileder for virksomheter som er avhengige av posisjonsbestemmelse, navigasjon og tidsbestemmelse

Formål. Dette dokumentet skal hjelpe virksomheter med å forstå sin avhengighet av PNT (posisjon, navigasjon og tid), vurdere konsekvenser av bortfall eller forstyrrelser, og etablere en praktisk, ledelsesforankret PNT-beredskap som kan innlemmes i eksisterende styrings-, sikkerhets- og kontinuitetsarbeid.

1	Sammendrag	3
2	Innledning og formål	4
3	Hva er PNT – og hvorfor er det kritisk?	4
4	Hva menes med PNT-beredskap?	5
5	Trussel- og hendelsesbildet	5
6	Prinsipper for PNT-beredskap	6
7	En praktisk modell: Forberede – Håndtere – Gjenopprette	7
7.1	Forberede	7
7.1.1	Kartlegg avhengigheter	7
7.1.2	Identifiser kritiske funksjoner	7
7.1.3	Identifiser trusler og sårbarheter	7
7.1.4	Vurder konsekvenser og risiko	8
7.1.5	Etabler tiltak og reserveløsninger	8
7.2	Håndtere	9
7.2.1	Oppdage og bekrefte hendelsen	9
7.2.2	Varsle og etablere situasjonsforståelse	9
7.2.3	Gå over til degradert eller alternativ drift	9
7.2.4	Overvåk utviklingen	9
7.3	Gjenopprette	9
8	Roller, ansvar og styring	10
9	Hva en PNT-beredskapsplan bør inneholde	10
10	Eksempler på tiltak	10
10.1	Tekniske tiltak	10

10.2	Organisatoriske tiltak	10
10.3	Operative tiltak	11
11	Testing, øving og forbedring	11
12	Sjekkliste: ti spørsmål virksomheten bør kunne svare på	11
13	Kort underlag til styret eller ledelsen	12
14	Vedlegg A. Enkel mal for PNT-beredskapsplan	12
15	Vedlegg B. Spørsmål til workshop eller kartleggingsmøte	12
16	Vedlegg C. Modenhetsmodell for PNT-beredskap	13

Sammendrag

Hvorfor dette haster. Mange virksomheter er i dag avhengige av PNT uten at avhengigheten er fullt ut kjent og kartlagt. Satellittbasert PNT, særlig basert på globale satellittnavigasjonssystemer (GNSS), brukes direkte eller indirekte i alt fra transport, logistikk, ekom og kraft til finans, nødetater, droner, maritim virksomhet, bygg og anlegg, overvåking, synkronisering av systemer og tidsstempling av hendelser. Posisjon, navigasjon og presis tid er kritiske elementer i den digitale infrastrukturen: de gjør det mulig for IT-systemer å samhandle, registrere hendelser i riktig rekkefølge, synkronisere nettverk og koordinere tjenester på tvers av virksomheter og leverandørkjeder. Når PNT svikter, kan konsekvensene raskt spre seg på tvers av organisasjon, leverandørkjeder og samfunnskritiske funksjoner. Dette er ikke lenger en teoretisk mulighet, men en opplevd virkelighet med stadig økende omfang.

Samfunnsøkonomisk betydning. Menon Economics anslår at et sammenhengende bortfall av satellittbaserte PNT-tjenester i syv døgn kan gi om lag 3,4 milliarder kroner i prissatte direkte samfunnsøkonomiske kostnader i Norge. Analysen viser samtidig at de største sårbarhetene ikke nødvendigvis er der de direkte kostnadene er høyest. Sektorer som kraftforsyning, finans og elektronisk kommunikasjon kan ha begrensede direkte tap i et kortvarig bortfall, men likevel være systemkritiske fordi presis tid og synkronisering understøtter en rekke andre samfunnsfunksjoner. Det er også viktig å merke seg at Menon-analysen vurderer bortfall av satellittbaserte PNT-tjenester, ikke manipulering av signalene. DSBs analyse peker på at manipulering, for eksempel spoofing som gir feil posisjon eller tid uten at dette oppdages, kan gi betydelig større konsekvenser nettopp for slike systemkritiske funksjoner enn et rent bortfall. Dette gjør PNT-beredskap til et ledelses- og samfunnssikkerhetsspørsmål, ikke bare et teknisk spørsmål.

Hva PNT-beredskap betyr. PNT-beredskap handler ikke bare om teknologi. Det handler om virksomhetsstyring. En virksomhet med god PNT-beredskap har oversikt over hvor den er avhengig av PNT, vet hvilke funksjoner som er mest kritiske, har vurdert konsekvensene av bortfall over ulike tidsrom, har etablert tekniske og organisatoriske tiltak, og har planer for å opprettholde drift med redusert kapasitet, lavere presisjon eller alternative arbeidsmåter og for å gjenopprette normal drift på en kontrollert måte.

Hva ledelsen bør beslutte. Ledelsen bør gi et tydelig mandat til å kartlegge PNT-avhengighet, innarbeide PNT-relatert risiko i virksomhetens helhetlige risikostyring, og etablere en trinnvis plan for forebygging, håndtering og gjenoppretting. Arbeidet bør forankres i linjen, ikke bare hos teknologimiljøene, og sees i sammenheng med sikkerhet, beredskap, cybersikkerhet, kontinuitetsplanlegging, leverandørstyring og operativ drift.

Hva virksomheten får igjen. Systematisk PNT-beredskap reduserer sannsynligheten for uønskede driftsstans, reduserer konsekvensene når forstyrrelser oppstår, styrker etterlevelse av krav til sikkerhet og kontinuitet, og gjør organisasjonen bedre rustet til å håndtere sammensatte hendelser. PNT-beredskap gir også et bedre beslutningsgrunnlag for effektive investeringer i redundans, alternative løsninger og kompetanseutvikling.

Innledning og formål

Denne veilederen er laget for virksomheter som er avhengige av PNT-tjenester, direkte eller indirekte. Den gir en praktisk metode for å etablere PNT-beredskap som del av virksomhetens samlede arbeid med sikkerhet, robusthet og kontinuitet.

Veilederen er sektorovergripende. Den kan brukes av virksomheter innen transport, logistikk, maritim virksomhet, luftfart, beredskap, kraft, ekom, finans, bygg og anlegg, industri, offentlig forvaltning og andre sektorer hvor feil i posisjon, navigasjon eller tid kan gi operasjonelle, sikkerhetsmessige eller økonomiske konsekvenser.

Veilederen er skrevet som et arbeidsverktøy. Den skal kunne brukes både til å starte et arbeid med PNT-beredskap, og til å strukturere og videreutvikle et arbeid som allerede er påbegynt.

Videre lesning: [DSBs veiledning om kontinuitetsplanlegging](#) og [NISTs Foundational PNT Profile](#) er nyttige kilder for å koble PNT-beredskap til virksomhetsstyring, risikostyring og eksisterende planverk.

Hva er PNT – og hvorfor er det kritisk?

PNT står for posisjonsbestemmelse, navigasjon og tidsbestemmelse. I praksis omfatter dette tjenester, data, signaler, sensorer og systemer som brukes til å fastslå hvor noe er, hvordan det beveger seg eller hvilken tid som gjelder.

Mange virksomheter tenker først på satellittnavigasjon i kjøretøy, fartøy eller fly, «GPS» som et kart med en prikk og en rutebeskrivelse. Men PNT brukes også til synkronisering av nettverk, koordinering av transaksjoner og handel, styring av autonome systemer, hendelseslogging, kommunikasjon, kartlegging, sporing, lufttrafikk, maritim trafikk, nød- og redningstjenester, kritisk infrastruktur og industrielle prosesser.

Avhengigheten av PNT er ofte skjult i underliggende systemer, hos leverandører eller i tredjepartsløsninger. Derfor bør PNT ses som en grunnleggende innsatsfaktor, på linje med kraft, ekom, data, kompetanse og lokasjoner.

Nyere norsk kunnskapsgrunnlag understreker at PNT må forstås som kritisk infrastruktur, ikke bare som navigasjonshjelpemiddel. Menon Economics anslår at et syv dagers bortfall av satellittbaserte PNT-tjenester i Norge kan gi om lag 3,4 milliarder kroner i prissatte direkte samfunnsøkonomiske kostnader. Rapporten peker samtidig på at de mest alvorlige sårbarhetene ofte ligger i sektorovergripende funksjoner som kraftforsyning, finans og elektronisk kommunikasjon, der svikt i presis tid og synkronisering kan få ringvirkninger langt utover den enkelte sektor.

FFIs utredning *Posisjon, navigasjon og tid – og betydningen for totalforsvaret*, utarbeidet på oppdrag fra Nærings- og fiskeridepartementet, vurderer betydningen satellittbasert PNT har for totalforsvaret. Rapporten kartlegger bruksområder for GNSS i samfunnet, beskriver tilsiktede handlinger og farer som kan føre til bortfall eller forstyrrelser, og vurderer risiko for utvalgte kritiske samfunnsfunksjoner. FFI konkluderer med at satellittbasert PNT styrker totalforsvaret, men at forstyrrelser kan redusere effektivitet og kapasitet i flere kritiske samfunnsfunksjoner sammenlignet med dagens tilstand. Rapporten peker særlig på sektorovergripende sårbarheter, økende avhengighet av GNSS, usikkerhet om

konsekvenser ved spoofing og behovet for testing, nasjonale rammeverk, bakkebaserte tidsalternativer og robuste multi-sensor PNT-systemer.

DSBs risikoanalyse av manipulering av satellittbaserte tidssignaler viser at risikoen ikke bare handler om bortfall av PNT, men også om feil tid som kan fremstå som korrekt. Analysen beskriver et scenario der skjulte radiosendere manipulerer satellittbaserte tidssignaler nær mottakere som brukes av kritiske samfunnsfunksjoner. Fordi nøyaktig og synkronisert tid er en forutsetning for at digitale systemer skal kunne kommunisere, logge hendelser og samhandle, kan små tidsavvik få store konsekvenser for blant annet strømforsyning, elektronisk kommunikasjon, finansielle tjenester og transport. DSB peker særlig på høy grad av digitalisering, fravær av sikker nasjonal tidsinfrastruktur og manglende kunnskap om egen robusthet som sentrale sårbarheter.

Regjeringen har pekt på at rapportene gir viktig kunnskap om samfunnets sårbarhet, og at funnene skal brukes videre i beredskapsarbeidet. Dette styrker behovet for at virksomheter kartlegger PNT-avhengighet, prioriterer kritiske funksjoner og etablerer alternative løsninger og beredskapsplaner.

Videre lesning: [GOV.UKs PNT-oversikt](#), [CISAs PNT-side](#), [Direktoratet for romvirksomhets omtale av satellittnavigasjon, jamming og spoofing](#), [Menon-rapporten om samfunnsøkonomiske konsekvenser ved bortfall av satellittbaserte PNT-tjenester](#), [DSBs risikoanalyse av manipulering av satellittbaserte tidssignaler](#) og FFIs utredning *Posisjon, navigasjon og tid – og betydningen for totalforsvaret* kan brukes for å forklare hva PNT er, hvorfor avhengigheten ofte er skjult, og hvorfor temaet nå behandles som et beredskaps- og samfunnssikkerhetsspørsmål.

Hva menes med PNT-beredskap?

PNT-beredskap er virksomhetens evne til å forebygge, oppdage, håndtere og gjenopprette funksjoner som er avhengige av posisjon, navigasjon og tid når disse blir degradert, manipulert eller utilgjengelige.

En PNT-beredskapsplan beskriver hvordan virksomheten identifiserer avhengigheter, vurderer risiko og konsekvenser, etablerer alternative løsninger og prosedyrer, organiserer håndteringen av hendelser og lærer av øvelser og faktiske hendelser.

PNT-beredskap må forankres i eksisterende styringssystemer. Den bør ikke etableres som et isolert fagspor, men integreres i virksomhetsstyring, sikkerhetsledelse, cybersikkerhet, beredskap, kontinuitetsplanlegging, leverandørstyring og endringsstyring.

Videre lesning: [Royal Institute of Navigations veiledning om resilient PNT](#), [CISA/DHS' Best Practices for Resilient PNT](#) og [NISTs Foundational PNT Profile](#) gir praktiske rammer for å forstå PNT-beredskap som en del av helhetlig styring.

Trussel- og hendelsesbildet

PNT kan svikte, bli degradert eller manipuleres av tekniske, naturlige eller menneskeskapte årsaker. Dagens sikkerhetspolitiske situasjon, kombinert med at satellittbaserte PNT-signaler har blitt viktige for å opprettholde digitale og operative funksjoner i samfunnet, gjør slike signaler attraktive å angripe, forstyrre eller manipulere. I enkelte situasjoner kan myndigheter eller andre aktører også selv måtte

begrense eller påvirke signalbruk for å beskytte egne interesser. Dette gjør det enda viktigere at virksomheter er forberedt på bortfall, feil og usikkerhet i PNT.

Typiske årsaker til PNT-forstyrrelser inkluderer:

- Jamming: forstyrrelse av radiosignaler, ofte rettet mot GNSS-mottak.
- Spoofing: falske eller manipulerede signaler som får utstyr til å beregne feil posisjon eller tid.
- Tekniske feil: feil i mottakere, antenner, kabling, klokke, programvare eller integrasjoner.
- Romvær og naturlige forhold: solstormer, ionosfæriske effekter, lokale miljøforhold eller skyggeeffekter.
- Cyberhendelser: kompromittering av systemer som bruker eller distribuerer PNT-data.
- Leverandørsvikt: feil hos underleverandører, nettverk eller eksterne tjenesteleverandører.
- Menneskelige feil: feilkonfigurasjon, feiloperasjon eller manglende forståelse av avhengigheter.

Videre lesning: [FFIs omtale av jamming og samfunnsbeskyttelse](#), [EASAs informasjon om GNSS-forstyrrelser](#), [Nkoms risiko- og sårbarhetsanalyse](#) for ekomsektoren og norske jammetest-rapporter gir relevant bakgrunn for trussel- og hendelsesbildet.

Prinsipper for PNT-beredskap

PNT-beredskap må ta høyde for mer enn fullstendig bortfall av signaler. I mange situasjoner kan den største utfordringen være usikkerhet: at posisjon, navigasjon eller tid fortsatt er tilgjengelig, men at virksomheten ikke vet om dataene er korrekte eller til å stole på. Manipulering, spoofing, meaconing eller delvise forstyrrelser kan derfor være mer krevende å håndtere enn et tydelig utfall, fordi systemer og operatører kan fortsette å bruke feil informasjon. Et sentralt prinsipp for PNT-beredskap er derfor å etablere evne til å oppdage avvik, vurdere tillit til PNT-data og raskt gå over til alternative kilder, manuelle kontroller eller redusert drift når tilliten er usikker.

Ledelsesforankring. PNT-beredskap må ha et tydelig mandat og prioriteres ut fra virksomhetens risikoeksponering og samfunnsrolle.

Helhetlig styring. Arbeidet må kobles til eksisterende styringssystemer, risikoregistre og kontinuitetsplaner.

Kjenn egne avhengigheter. Virksomheten må vite hvor PNT er kritisk – også der avhengigheten er indirekte.

Planlegg for ulike hendelsestyper og varigheter. Konsekvenser og tiltak må vurderes både for korte og lange bortfall, og for situasjoner der PNT-signaler fortsatt er tilgjengelige, men kan være manipulerede, forstyrrede eller usikre.

Bruk flere barrierer. Organisatoriske, tekniske og operative tiltak må kombineres, slik at virksomheten kan oppdage avvik, verifisere PNT-data mot alternative kilder og unngå at feil posisjon eller tid automatisk får operative konsekvenser.

Legg til rette for degradert drift. Målet er å kunne opprettholde trygg og akseptabel drift selv om normal PNT ikke er tilgjengelig.

Test og lær. Planverk og tiltak må valideres gjennom testing, øvelser og etterarbeid.

Videre lesning: [Royal Institute of Navigations «Prepare-Act-Recover»-tilnærming](#), [DSBs kontinuitetsveiledning](#), [NISTs PNT-profil](#) og [ISO 22301 om kontinuitetsledelse](#) gir nyttige prinsipper for å

strukturere beredskapsarbeidet. ISO 22301 er en internasjonalt anerkjent standard for styringssystemer for kontinuitet og kan være særlig relevant for virksomheter som allerede arbeider systematisk med risikostyring, leverandøroppfølging, beredskapsplaner og gjenoppretting etter forstyrrende hendelser.

En praktisk modell: Forberede – Håndtere – Gjenopprette

Veilederen følger en tredelt modell for PNT-motstandsdyktighet: Forberede, Håndtere og Gjenopprette. Modellen skal gjøre arbeidet enkelt å kommunisere, samtidig som den forutsetter konkrete prosesser, roller og tiltak.

I praksis bør arbeidet gjennomføres som en styrt, tverrfaglig prosess. Ledelsen bør først gi et tydelig mandat og avklare ambisjonsnivå, ansvar og rapportering. Deretter bør virksomheten samle relevante miljøer fra drift, teknologi, sikkerhet, beredskap, virksomhetsstyring og innkjøp for å kartlegge PNT-avhengigheter, identifisere kritiske funksjoner og vurdere konsekvenser ved ulike nivåer av bortfall eller degradering. På dette grunnlaget kan virksomheten prioritere tekniske, organisatoriske og operative tiltak, utarbeide eller oppdatere PNT-beredskapsplanen og teste planverket gjennom øvelser, tekniske tester og scenarioarbeid. Arbeidet bør munne ut i en konkret forbedringsplan med ansvar, frister og ledelsesoppfølging.

Forberede

Målet i forberedelsesfasen er å forstå virksomhetens PNT-avhengighet, vurdere risiko og etablere tiltak før en hendelse oppstår.

Kartlegg avhengigheter

- Hvilke systemer, tjenester, prosesser og leverandører bruker PNT?
- Gjelder avhengigheten posisjon, navigasjon, tid – eller en kombinasjon?
- Er avhengigheten direkte eller indirekte?
- Hvilke forretningsprosesser eller samfunnskritiske funksjoner påvirkes?

Kartleggingen bør dekke egne systemer, leverandørkjeder, integrasjoner, tredjepartsløsninger, sensorkjeder, styringssystemer og tidssynkronisering.

Identifiser kritiske funksjoner

- Hvilke funksjoner må opprettholdes av hensyn til liv og helse, sikkerhet, samfunnsoppdrag, kontraktsforpliktelser eller økonomi?
- Hvilke funksjoner kan reduseres midlertidig?
- Hvilke funksjoner kan stanses uten uakseptable konsekvenser?

Det bør fastsettes akseptable nedetider og minimumsnivå for drift ved degradert situasjon. Dette er et kjernepunkt i all kontinuitetsplanlegging.

Identifiser trusler og sårbarheter

Når virksomheten har kartlagt verdier, kritiske funksjoner og PNT-avhengigheter, bør den identifisere hvilke trusler og sårbarheter som kan påvirke disse. Dette handler om å forstå hvordan PNT kan bli utilgjengelig, degradert, manipulert eller usikkert – og hvor virksomheten er særlig eksponert.



- Hvilke trusler er mest relevante: jamming, spoofing, meaconing, cyberhendelser, tekniske feil, romvær, leverandørsvikt eller menneskelige feil?
- Hvor kan feil eller usikre PNT-data oppstå uten at det oppdages raskt?
- Hvilke systemer, manuelle rutiner eller leverandørkjeder har enkeltpunktsvikt?
- Hvilke eksisterende barrierer finnes for å oppdage, verifisere og håndtere avvik?
- Hvilke avhengigheter eller sårbarheter er utilstrekkelig dokumentert eller forstått?

Sårbarhetsvurderingen bør sees i sammenheng med verdivurderingen i punkt 7.1.2: Jo viktigere funksjonen er for liv og helse, sikkerhet, samfunnsoppdrag, kontraktsforpliktelser eller økonomi, desto viktigere er det å forstå hvilke trusler og sårbarheter som kan påvirke den.

Vurder konsekvenser og risiko

- Hvilke konsekvenser kan oppstå for ulike funksjoner dersom PNT blir borte, degradert, manipulert eller usikkert?
- Hvordan utvikler konsekvensene seg over tid – for eksempel etter 1 minutt, 1 time, 1 døgn, 1 uke eller 1 måned?
- Hvordan påvirkes konsekvensene dersom PNT-data fortsatt er tilgjengelige, men viser feil posisjon eller tid?
- Hvilke samtidige hendelser kan forsterke konsekvensene, for eksempel ekomsvikt, cyberhendelser, kraftutfall eller leverandørsvikt?
- Hvilket risikonivå står virksomheten igjen med etter eksisterende barrierer og tiltak?

Scenarioarbeid er et nyttig verktøy for å vurdere samlede konsekvenser og risiko. Scenarioene bør bygges på kunnskapen virksomheten allerede har samlet om verdier, kritiske funksjoner, PNT-avhengigheter, trusler og sårbarheter. Hensikten er ikke å beskrive alle mulige hendelser, men å teste hvordan ulike kombinasjoner av bortfall, feil signaler, usikker tillit og samtidige hendelser kan påvirke virksomheten.

- Kortvarig GNSS-utfall i et begrenset geografisk område.
- Langvarig jamming som påvirker kjøretøy, fartøy, droner eller tidskritiske systemer.
- Spoofing eller meaconing som gir feil posisjon eller tid uten at dette oppdages umiddelbart.
- Delvis forstyrrelse der signalet fortsatt er tilgjengelig, men tilliten til posisjon, navigasjon eller tid er usikker.
- Feil i tidsdistribusjon som påvirker nettverk, logger, transaksjoner eller hendelsesrekkefølge.
- Sammensatt hendelse der PNT-forstyrrelser opptrer samtidig med ekomsvikt, cyberhendelse, kraftutfall eller leverandørsvikt.

For hvert scenario bør virksomheten beskrive utløsende indikatorer, hvordan hendelsen oppdages, hvordan tillit til PNT-data vurderes, hvilke funksjoner som påvirkes, hvilke tiltak som iverksettes, hvilke operative begrensninger som gjelder, og kriterier for eskalering, nedskalering og retur til normal drift.

Etabler tiltak og reserveløsninger

- Alternative PNT-kilder eller sensorer.
- Holdover-løsninger for tid.
- Lokale prosedyrer for manuell eller degradert drift.
- Reservemateriell og alternative arbeidsmåter.
- Forsterket overvåking og deteksjon.

- Kompetanseheving og tydelige beslutningskriterier.

Håndtere

Når en PNT-hendelse oppstår, må virksomheten raskt kunne oppdage, vurdere og håndtere den. Håndteringsfasen må være konkret og operasjonell.

Oppdage og bekrefte hendelsen

- Hvordan oppdages avvik i posisjon, navigasjon eller tid?
- Hvilke tekniske indikatorer eller driftsobservasjoner er relevante?
- Hvordan skilles mellom lokal feil, leverandørsvikt og ekstern forstyrrelse?
- Hvem har myndighet til å erklære at en PNT-hendelse foreligger?

Varsle og etablere situasjonsforståelse

- Hvem skal varsles internt?
- Når skal ledelse, beredskapsfunksjon, IT, drift eller sikkerhetsorganisasjon involveres?
- Hvilke eksterne aktører må varsles?
- Hvordan dokumenteres tid, omfang, påvirkede funksjoner og vurderte tiltak?

Gå over til degradert eller alternativ drift

- Hvilke tjenester skal prioriteres?
- Hvilke manuelle prosedyrer skal tas i bruk?
- Hvilke sikkerhetsgrenser gjelder ved redusert nøyaktighet eller usikker tid?
- Når skal virksomheten redusere kapasitet eller stanse enkelte aktiviteter?

Det bør finnes tydelige kriterier for når automatiske løsninger kan brukes, når manuell overstyring er nødvendig, og når drift må reduseres eller stanses.

Overvåk utviklingen

- Mål effekten på drift, kvalitet, sikkerhet og leveranser.
- Registrer hvilke tiltak som er iverksatt og hvilken effekt de har.
- Oppdater situasjonsbildet regelmessig og sikre sporbar dokumentasjon.

Gjenopprette

Når hendelsen avtar eller er avsluttet, må virksomheten gjenopprette normal drift kontrollert og samtidig sikre læring og forbedring.

- Definer hvem som kan beslutte retur til normal drift.
- Bekreft at ordinære PNT-kilder igjen er tilgjengelige og til å stole på.
- Vurder behov for kontroll, kalibrering, verifikasjon eller re-synkronisering.
- Dokumenter avvik, erfaringer og forbedringspunkter.
- Oppdater risikovurderinger, prosedyrer, opplæring og tekniske tiltak.

Videre lesning: [Royal Institute of Navigations veiledning om resilient PNT](#) og [CISA/DHS' beste praksis for kritisk infrastruktur](#) er særlig relevante for modellen Forberede–Håndtere–Gjenopprette.

Roller, ansvar og styring

PNT-beredskap må eies av virksomheten, ikke av en enkelt faggruppe. Følgende rollefordeling kan brukes som utgangspunkt:

- Styret / toppledelsen: setter ambisjon, aksepterer risiko og følger opp prioriteringer.
- Virksomhetsledelse: sørger for forankring, ressurser og tverrfaglig koordinering.
- Beredskapsansvarlig / kontinuitetsansvarlig: samordner planverk, øvelser og hendelseshåndtering.
- Fagansvarlige for drift, IT og sikkerhet: identifiserer tekniske avhengigheter og tiltak.
- Innkjøp og leverandøransvarlige: sikrer at PNT-avhengighet og krav til robusthet ivaretas i kontrakter og oppfølging.
- Linjeledere og operativt personell: kjenner prosedyrer for degradert drift og rapportering.

Det bør utpekes én ansvarlig funksjon for å samordne PNT-beredskap. Funksjonen eier ikke nødvendigvis alle tiltak, men har ansvar for helhet, framdrift og rapportering.

Hva en PNT-beredskapsplan bør inneholde

- Formål, omfang og avgrensninger.
- Beskrivelse av virksomhetens kritiske funksjoner og PNT-avhengighet.
- Oversikt over systemer, tjenester, leverandører og kontaktpunkter.
- Forutsetninger og scenarioer planen dekker.
- Varslings- og eskaleringsrutiner.
- Tiltak ved kort, mellomlang og langvarig PNT-degradering eller bortfall.
- Beskrivelse av alternative løsninger og degradert drift.
- Beslutningskriterier for reduksjon, omlegging eller stans i drift.
- Gjenopprettingsrutiner og verifikasjon før retur til normal drift.
- Krav til logging, rapportering, evaluering og revisjon.
- Plan for testing, øving og vedlikehold av planverket.

Eksempler på tiltak

Tekniske tiltak

- Redundans i PNT-kilder og sensorer.
- Lokal holdover eller reservetid.
- Overvåking av signalintegritet og avviksdeteksjon.
- Logging og sporing av avvik i egne operasjoner.
- Segmentering, hardening og cybersikkerhet for systemer som bruker eller distribuerer PNT-data.

Organisatoriske tiltak

- Tydelig rolle- og ansvarsfordeling.
- Rutiner for varslings og eskalering.
- Krav til leverandører og kontrakter.



- Opplæring av ledere, fagpersonell og operatører.
- Innarbeiding av PNT-risiko i styrende dokumenter.

Operative tiltak

- Prosedyrer for degradert drift.
- Manuelle alternativer og reservearbeidsmåter.
- Forhåndsdefinerte kapasitets- eller sikkerhetsbegrensninger.
- Papirbaserte eller offline støtteverktøy der det er relevant.
- Forhåndsplanlagt samarbeid med eksterne aktører ved hendelser.
- Informasjonshåndtering

Testing, øving og forbedring

Planverk som ikke er testet, gir begrenset verdi. PNT-beredskap bør derfor inngå i virksomhetens faste syklus for øving, evaluering og forbedring. Ulike øvelsesformer gir ulik verdi og bør velges ut fra virksomhetens modenhet, risiko og ambisjonsnivå. I en tidlig modenhetsfase kan det være stor verdi i en enkel skrivebordsøvelse der ledelse, fagmiljøer og drift diskuterer roller, beslutninger og tiltak med utgangspunkt i et realistisk PNT-scenário. Etter hvert som planverk og tiltak modnes, kan virksomheten gå videre med tekniske tester, leverandørtester og operative øvelser som prøver ut faktisk håndtering, alternativ drift, informasjonsdeling og gjenoppretting.

- Skrivebordsøvelser for å teste forståelse, roller, beslutningspunkter, eskalering og samhandling uten å forstyrre drift.
- Scenarioøvelser som utfordrer virksomheten på bortfall, feil signaler, usikker tillit til PNT-data og samtidige hendelser.
- Tekniske tester av avviksdeteksjon, automatisk omkobling, holdover, reserveløsninger og verifikasjon av alternative PNT-kilder.
- Operative øvelser i degradert eller alternativ drift, der personell trener på faktiske prosedyrer og prioriteringer.
- Leverandørinvolvering i test og evaluering, særlig der PNT-avhengigheter ligger i underleveranser, integrasjoner eller eksterne tjenester.
- Etterarbeid med tydelig ansvar for forbedringstiltak, frister og ledelsesoppfølging.

Sjekkliste: ti spørsmål virksomheten bør kunne svare på

1. Har vi oversikt over alle systemer, tjenester og leverandører som er avhengige av PNT?
2. Vet vi hvorfor vi trenger PNT og hva konsekvensen er dersom PNT blir feil eller utilgjengelig?
3. Er PNT-relatert risiko registrert i virksomhetens risikostyring?
4. Har vi en tydelig ansvarlig funksjon for å samordne PNT-beredskap?
5. Har kritiske funksjoner alternative kilder, sensorer eller arbeidsmåter som reduserer enkeltpunktsvikt?
6. Vet vi hvordan systemene våre oppfører seg ved kortvarig og langvarig bortfall av PNT?
7. Har vi dokumenterte tiltak og planer for degradert drift?
8. Tester og øver vi på PNT-relaterte hendelser?

9. Har vi en prioritert plan for å styrke robustheten over tid?
10. Følger vi utviklingen i trusselbildet, teknologimuligheter og krav som kan påvirke vår PNT-beredskap?

Kort underlag til styret eller ledelsen

Nedenfor følger et forslag til disposisjon for et kort beslutningsunderlag på én til to sider:

- Hva virksomheten er avhengig av: beskriv de viktigste prosessene, systemene eller tjenestene som krever PNT.
- Hva som kan gå galt: beskriv de mest relevante hendelsene og hvordan de kan påvirke virksomheten.
- Hva konsekvensene er: sikkerhet, drift, kunder, samfunnsoppdrag, økonomi og omdømme.
- Hva som allerede er gjort: eksisterende tiltak, alternative løsninger og relevant planverk.
- Hva som mangler: de viktigste gapene i dag.
- Hva som anbefales besluttet: mandat, prioriteringer, ressurser og tidsplan for videre arbeid.

Vedlegg A. Enkel mal for PNT-beredskapsplan

1. **Formål og omfang.** Hvilke deler av virksomheten omfatter planen, og hva er målsettingen med planen?
2. **Kritiske funksjoner.** Hvilke tjenester, prosesser eller operative funksjoner må opprettholdes?
3. **PNT-avhengigheter.** Hvilke systemer, leverandører og innsatsfaktorer bruker PNT?
4. **Scenarier og forutsetninger.** Hvilke typer PNT-hendelser er planen laget for?
5. **Varsling og eskalering.** Hvem varsles, når og på hvilken måte?
6. **Tiltak ved hendelse.** Hva skal gjøres ved kort, mellomlang og langvarig bortfall/degradering?
7. **Degradert drift.** Hvordan kan virksomheten opprettholde akseptabel drift uten normal PNT?
8. **Gjenoppretting.** Hvordan verifiseres og besluttes retur til normal drift?
9. **Øving og vedlikehold.** Hvordan skal planen testes, revideres og forbedres?

Vedlegg B. Spørsmål til workshop eller kartleggingsmøte

Spørsmålene under kan brukes som grunnlag for en intern workshop, kartlegging eller enkel skrivebordsøvelse om PNT-beredskap. DSB har publisert veiledning og eksempler på skrivebordsøvelser som kan brukes som inspirasjon til å bygge opp øvelsen, avklare roller og teste beslutninger, kommunikasjon og tiltak uten å gjennomføre en fullskalaøvelse.

- Hvor i vår virksomhet brukes posisjon, navigasjon eller tid i dag?
- Hvilke funksjoner stopper opp dersom PNT blir feil eller borte?
- Hvordan vil vi oppdage at PNT-data ikke lenger er til å stole på?
- Hvor lenge kan vi operere før konsekvensene blir uakseptable?
- Hva kan vi gjøre manuelt eller på alternative måter?
- Hvilke leverandører er kritiske for vår PNT-avhengighet?
- Hvilke tiltak er raske å innføre, og hvilke krever større investeringer?

Vedlegg C. Modenhetsmodell for PNT-beredskap

Nivå på planverkets modenhet	Beskrivelse	Kjennetegn
1. Ikke vurdert	Virksomheten har ikke systematisk vurdert PNT-avhengighet.	Ingen samlet oversikt, ingen tydelig forankring, PNT-risiko er i liten grad synlig.
2. Kartlagt	De viktigste avhengighetene er identifisert.	Enkel oversikt over sentrale systemer og funksjoner; begynnende risikoforståelse.
3. Planlagt	Risiko, konsekvenser og tiltak er dokumentert.	PNT-risiko er innarbeidet i styringssystemer; beredskapsplan er påbegynt eller etablert.
4. Implementert	Tiltak er iverksatt og ansvar er tydelig definert.	Tekniske og organisatoriske barrierer finnes; varslings- og eskaleringsrutiner er på plass.
5. Øvd og forbedret	Planverk og tiltak testes og forbedres jevnlig.	Regelmessige øvelser, ledelsesoppfølging, erfaringslæring og tydelig forbedringsplan.