Vedlegg A – Risikokriterier

Kriterier for å vurdere og evaluere risiko

Helse Midt-Norge har etablert felles anbefalte kriterier for vurdering av sannsynlighet, konsekvens og beskrivelse av risiko på tvers av virksomhetene i foretaksgruppen. Kriteriene *kan* i særlige tilfeller fravikes, men begrunnelse for valg av alternative kriterier *bør* redegjøres for.

Kriteriene for sannsynlighetsvurdering er differensiert ut fra om risikovurderingen omfatter strategiske mål, styringsmål, ordinær drift, prosjekt eller informasjonssikkerhet, og beskrevet i Tabell 1.

Tabell 1 Kriterier for sannsynlighetsvurdering

Type	Svært lav	Lav	Middels	Høy	Svært høy
Strategiske mål *	Estimert 0-10 % sannsynlig i målperioden	Estimert 10-35 % sannsynlig i målperioden	Estimert 35-65 % sannsynlig i målperioden	Estimert 65-90 % sannsynlig i målperioden	Estimert 90-100 % sannsynlig i målperioden
Styringsmål *					
Drift**	Sjeldnere enn 1 hendelser per X år	1-5 hendelser per X år	6-20 hendelser per X år.	21-100 hendelser X år	Flere enn hundre hendelser per X år.
Prosjekt	Estimert 0-10 % sannsynlig i prosjektperioden	Estimert 10-35 % sannsynlig i prosjektperioden	Estimert 35-65 % sannsynlig i prosjektperioden	Estimert 65-90 % sannsynlig i prosjektperioden	Estimert 90-100 % sannsynlig i prosjektperioden
Informasjonssikkerhet: Trusselbilde***	Foreligger ingen identifiserte aktører med evne og vilje til å begå uønskede handlinger	Foreligger kun aktører med lav evne og lav vilje til å begå uønskede handlinger	Foreligger aktører med moderat evne og moderat vilje til å begå uønskede handlinger	Foreligger aktører med moderat evne og høy vilje til å begå uønskede handlinger	Foreligger aktører med høy evne og høy vilje til å begå uønskede handlinger
Informasjonssikkerhet: Tiltaksstyrke***	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten • Tiltakene kan kun omgås/brytes av egne	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten • Tiltakene kan likevel omgås/brytes av egne	• Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter fullt ut etter hensikten • Egne medarbeidere trenger kun normale ressurser for å omgå/bryte	• Sikkerhetstiltak er ikke etablert, eller • Det er kjent at tiltakene omgås/brytes av egne medarbeidere • Kan omgås/brytes av eksternt personell med	• Sikkerhetstiltak er ikke etablert, eller • Det er kjent at tiltakene omgås/brytes av eksternt personell med normale ressurser uten kjennskap til tiltakene

Type	Svært lav	Lav	Middels	Høy	Svært høy
	medarbeidere med gode ressurser, og god/ fullstendig kjennskap til tiltakene • Eksternt personell kan ikke omgå/bryte tiltaket	medarbeidere med normale ressurser, som i tillegg har normal kjennskap til tiltakene • Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse	tiltakene – det er ikke nødvendig med kjennskap til tiltakene • Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke prosedyrer som gjelder, eller hvordan sikkerhetsteknologi er implementert) – i tillegg til små/normale ressurser	normale ressurser og uten kjennskap til tiltakene	

* Vurdering av sannsynlighet for *manglende* måloppnåelse.

** Risikovurdering av hendelser i ordinær drift vil kunne variere med tanke på tidsperspektivet på vurdering. Det anbefales derfor å inkludere dette tidsperspektivet i valget av sannsynlighetskriterier. Det anbefales at definisjonene for frekvens eller antall hendelser tilpasses i skalaen slik at dette harmonerer med det området som skal risiko-vurderes.

*** Sannsynlighetsnivå for informasjonssikkerhetshendelser vurderes og settes som en samlet vurdering av %-vis sannsynlighet (*), tilpasset frekvens (ref. Drift**), trusselbilde og tiltaksstyrke. Risikovurdering av informasjonssikkerhet omfatter tilsiktede og utilsiktede uønskede hendelser. Ved tilsiktede hendelser vurderes trussel-aktørers evne og vilje til å begå uønskede handlinger (trusselbildet) som en del av sannsynlighetsvurderingen. I tillegg vurderes hvor lett en hendelse (tilsiktet eller utilsiktet) kan skje, basert på styrken i eksisterende tiltak eller eventuell mangel av tiltak

Tabell 2 under, viser de ni definerte konsekvensområder i Helse Midt-Norge med tilhørende kriterier for vurdering av konsekvens. Det *kan* ved behov vurderes konsekvenser for øvrige områder. I slike tilfeller må konsekvenskriteriene fastsettes spesifikt, og i forkant av risikovurderingen. Ved vurderinger innenfor informasjonssikkerhet bør alltid konsekvensene i tabell 2 vurderes i lys av brudd på både konfidensialitet (K), integritet (I) og tilgjengelighet (T).

Tabell 2 Kriterier for konsekvensvurdering, fordelt på konsekvensområder

Konsekvensområde	Ubetydelig/ marginal	Liten	Moderat	Alvorlig	Svært alvorlig
Pasientsikkerhet	Ingen eller ubetydelig skader	Kortvarige eller små skader, eller for få personer.	Skader av middels alvorlighet eller varighet, eller for et betydelig antall personer.	Skader av alvorlig eller vedvarende karakter, eller for mange personer.	Kritiske skader eller tap av liv, eller for svært mange personer.
HMS/arbeidsmiljø	Ubetydelig personskade/plage. Ikke fravær.	Mindre alvorlig skade eller plage. Kan gi fravær.	Alvorlig skade/sykdom, langvarige følger.	Varige mèn/ invaliditet/ uførhet, eller flere enkelttilfeller av alvorlig skadde/syke.	Dødsfall eller mange alvorlig syke/skadde.
Personvern	Intet uautorisert innsyn i helse- og personopplysninger. Ikke brudd på personvernet	Uautorisert innsyn i enkelte helse- og personopplysninger *og/eller* brudd på personvernet for et lite antall individer	Uautorisert innsyn i flere helse- og personopplysninger, mulighet for endring *og/eller* brudd på person-vernet for et moderat antall individer	Uautorisert innsyn i store mengder helse- og personopplysninger, mulighet for endring *og/eller* brudd på person-vernet for et stort antall individer	Fullt uautorisert innsyn i eller mulighet for endring av alle helse- og person-opplysninger *og /eller* brudd på personvernet for svært mange individer
Ytre miljø	Minimal innvirkning på miljø tilnærmet normal drift.	Liten eller kortvarig miljøpåvirkning	Betydelig miljøpåvirkning med midlertidig varighet	Betydelig eller langvarig miljøpåvirkning	Omfattende og langvarig miljøpåvirkning
Drift/tjeneste-produksjon	Minimal innvirkning, tilnærmet normal drift.	Liten eller kortvarig reduksjon i tjenesteleveranse.	Betydelig reduksjon av tjeneste-leveransene eller middels varighet.	Omfattende eller langvarig reduksjon av tjeneste-leveransene.	Fullstendig eller langvarig tap av tjeneste-leveransene.

Konsekvensområde	Ubetydelig/ marginal	Liten	Moderat	Alvorlig	Svært alvorlig
Kapasitet	Ingen eller ubetydelig merarbeid.	Merarbeid for få ansatte eller av kort varighet.	Merarbeid for flere ansatte eller av middels varighet.	Merarbeid for mange ansatte eller av lang varighet.	Merarbeid for svært mange ansatte, av svært stort omfang eller av svært lang varighet.
Straff, sanksjoner, erstatningsansvar	Ingen eller ubetydelige avvik fra krav som ikke medfører sanksjoner eller erstatningsansvar.	Avvik fra krav som kan medføre mindre sanksjoner eller erstatningsansvar.	Avvik fra krav som kan medføre moderate sanksjoner eller erstatningsansvar.	Avvik fra krav som kan medføre store sanksjoner eller erstatningsansvar.	Avvik fra krav som kan medføre svært store sanksjoner, erstatningsansvar eller straff.
Økonomi	Ingen eller ubetydelig påvirkning på verdier, inntekter eller utgifter.	Mindre påvirkning på verdier, inntekter eller utgifter.	Tap av verdier, inntekter eller påførte utgifter med moderate konsekvenser for økonomisk handlingsrom.	Tap av verdier, inntekter eller påførte utgifter med store konsekvenser for økonomisk handlingsrom.	Tap av verdier, inntekter eller påførte utgifter med katastrofale konsekvenser for økonomisk handlingsrom.
Tillit, omdømme	Ingen eller minimal svekkelse av tillit / omdømme.	Liten eller kortvarig svekkelse av tillit / omdømme	Betydelig eller middels varig svekkelse av tillit / omdømme.	Alvorlig eller langvarig svekkelse av tillit / omdømme	Fullstendig eller uopprettelig svekkelse av tillit / omdømme

Kriterier for aksept av risiko

I Helse Midt-Norge *skal* følgende risikomatrise benyttes: