POLITIET

Risikovurdering av politiets bruk av sosiale medier

Versjon 0.2

Politidirektoratet

Godkjent:

Sted, dato	Rolle	Navn	Signatur

1 Kontekst / Området

1.1 Deltagere i analysen

Rolle	Navn	Enhet
Kommunikasjonsrådgiver	Anne Margrete Alværn	POD: kommunikasjonsavdelingen
Kommunikasjonsrådgiver	Dag Gjærum	Utrykningspolitiet
Politioverbetjent på Sambandsavsnittet.	Runar Skarnes	Oslo PD: Ordensavdelingen
Kommunikasjonsrådgiver	Kari Anne Kvarving	Nordre Buskerud PD
Politibetjent	Håvard Skattum	Hordaland politidistrikt, Voss lensmannsdistrikt
Kommunikasjonsrådgiver	Kristian Tønne Ski	Oslo PD
Informasjonssikkerhetsrådgiver	Tommy Molnes	POD: Arbeidsgiver- og administrasjonsavdelingen
Prosessdriver/fasilitator	Anne Kristine Næss	POD (innleid fra PROMIS AS)

1.2 Analysen omhandler:

Informasjonsbehandling og tilgang til informasjon gjennom bruk av sosiale medier i kommunikasjonen med publikum, herunder Facebook og Twitter. Dette er en tjeneste som har blitt til gradvis, og som viser seg å ha samfunnsnyttige så vel som virksomhetsnyttige effekter. Et eksempel på dette er Utrykningspolitiets evne til å nå ut til en betydelig andel av befolkningen raskt dersom det oppstår tilstander i trafikken som kan volde skade på liv og helse. Årsaken til dette er at flere medier, herunder radiokanalene, raskt kan plukke opp UP's twittermeldinger, og i mange tilfeller avbryter ordinære sendinger for å gi disse meldingene videre til sine lyttere. Et annet eksempel er hvordan publikum viser seg å være svært positive til tilstedeværelsen fra politiet på sosiale medier. Dette oppfattes som å gjøre tilgjengeligheten til politiet kortere, noe som igjen kan gi politiet et bedre omdømme.

1.3 Begrensninger i analysen

Det er ikke foretatt noen verdivurdering av denne tjenesten og hvor viktig bruken av sosiale medier er blitt for politiet. Følgelig ble risikovurderingen foretatt uten den nødvendige konteksten. Risikoverdiene og de forslag til tiltak denne rapporten peker på må derfor sees på i lys av at tjenesten kan være mindre kritisk for politiet totalt sett, og at det derfor ikke er behov for strakstiltak knyttet til risikoverdier i rød sone i risikomatrisen. Likevel fremgikk det av vurderingen at det å kunne kommunisere med publikum gjennom sosiale medier er blitt et sterkt og raskt alternativ til de mer etablerte kanalene, og at det i krisesituasjoner kan vise seg å spare menneskeliv og unngå uønskede hendelser som kan gi andre typer store samfunnsmessige konsekvenser.

1.4 Målet med analysen

Målet er å avdekke risikofaktorer som krever tiltak, slik at disse blir identifisert og prioritert, samt at ledelsen blir i stand til å beslutte å gjennomføre nødvendige tiltak og akseptere eventuell restrisiko.

2 Basiskriteriene

2.1 Konsekvens

Matrisen nedenfor benyttes for å sette konsekvensene av hendelsen i rett kategori.

Konsekvensgradering / Konsekvens	Ubetydelig 1	Moderat 2	Alvorlig 3	Kritisk 4
Menneske	Mindre og kortvarige psykiske påkjennelser uten at det resultere i sykefravær.	Moderate psykiske påkjennelser. Kan resultere i kortvarig sykefravær.	Indirekte fare for menneskers liv og helse. Alvorlig psykisk påkjennelse. Kan resultere i lengre fravær (ukentlig til halvårlig)	Direkte fare for menneskers liv og helse. Kritisk psykisk påkjennelse. Vil resultere i fravær lengre enn 6 måneder.
Omdømme tap	Ubetydelig omdømmetap i en meget kort periode.	Moderat omdømmetap i en lengre periode.	Alvorlig omdømmetap som kan vedvare over lengre tid.	Uopprettelig tap av omdømme.
Økonomi / materielle skader	1 kr – 10 000 kr	10 000 kr – 100 000 kr	100 000 kr – 1 000 000 kr	> 1 000 000 kr
Ytre miljø	Ingen konsekvenser for ytre miljø.	Moderat fare for ytre miljø i begrenset område.	Alvorlig fare for ytre miljø i begrenset område	Alvorlig fare for ytre miljø i større område.
Normer, lover og regler	Brudd på uskrevne regler, normer og normal folkeskikk.	Brudd på generell policy og retningslinjer i Politietaten	Brudd på instrukser, og lover som vil føre til pålegg om opprettende tiltak.	Brudd på instrukser og den norske lov som vil medføre en straff.

2.2 Sannsynlighet

For å vurdere sannsynligheten for at en hendelse skal inntreffe benyttes begrepene i matrisen nedenfor. Følgende definisjoner ligger bak de forskjellige sannsynlighetsgradene:

Sannsynlighetsgrad	Svært lite sannsynlig 1	Lite sannsynlig 2	Sannsynlig 3	Svært sannsynlig 4
Sannsynlighet	**Aldri - 10 år** Hendelsen kan inntre hvert 10. år eller sjeldnere	**10 år – 1 år** Hendelsen kan inntre fra en gang per år til hvert 10. år.	**1 år - Ukentlig** Hendelsen kan inntre fra ukentlig til årlig	**Ukentlig – Hele tiden** Hendelsen kan inntre en eller flere ganger per uke.

2.3 Risiko

Identifisert risiko vil synliggjøres i risikomatrisen i samsvar med nedenstående figur:

Risikomatrise

Sannsynlighet		Svært lite sannsynlig	Lite sannsynlig	Sannsynlig	Svært sannsynlig
		1	2	3	4
Ubetydelig	1	1	2	3	4
Moderat	2	2	4	6	8
Alvorlig	3	3	6	9	12
Kritisk	4	4	8	12	16

2.4 Akseptkriterier

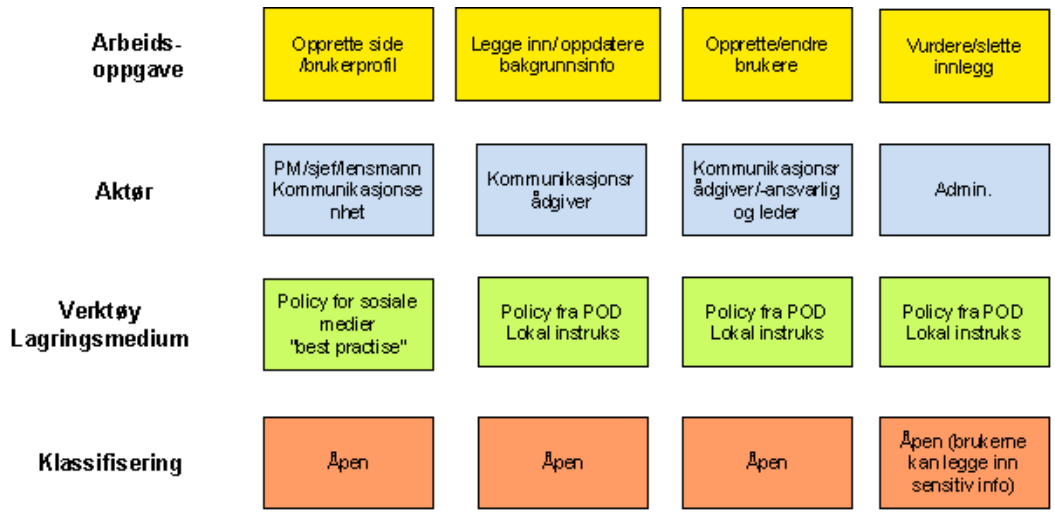
Politidirektoratet har definert følgende kriterier for risikoaksept:

Nivå for risikoaksept		
Lav risiko	1-3	Ingen tiltak nødvendig
Moderat risiko	4-11	Tiltak må vurderes. Velges ingen tiltak for en hendelse, så skal det valget begrunnes (kapittel 4.2)
Høy risiko	12-16	Tiltak skal iverksettes.

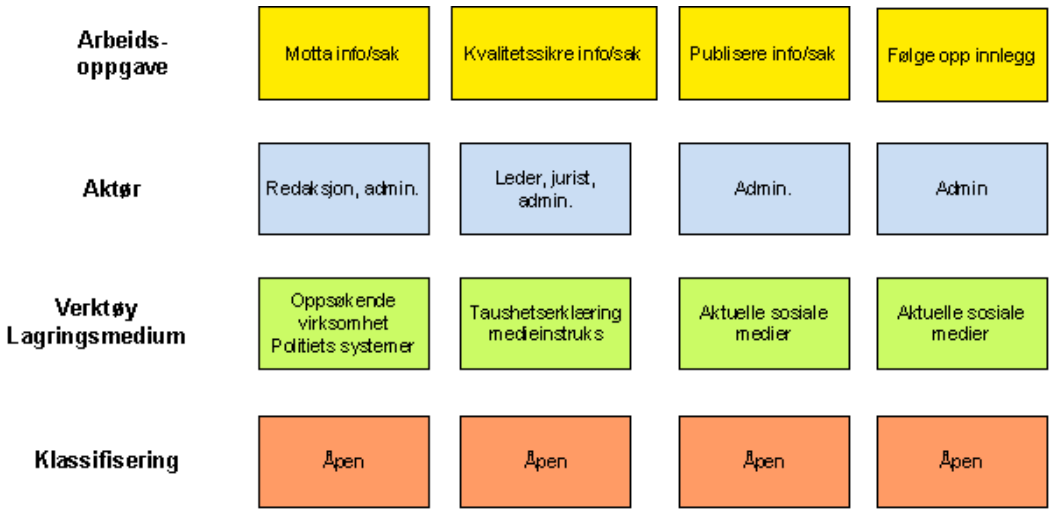
2.5 Kontekst

Beskrivelse av hvilke arbeidsoppgaver som inngår i tjenesten. Det er valgt å sette tjenesten opp i to strømmer. En for administrative oppgaver relatert til bruk av sosiale medier og en for publisering og oppfølging av nyhetssaker som kommuniseres ut.

2.5.1 Administrere side/brukere



2.5.2 Legge ut/følge opp nyhetssaker



2.6 Trusler

Beskrivelse av hvilke aktører eller fenomener som kan skape uønskede hendelser.

Kilde	Beskrivelse
Menneskelige trusselkilder	
Ansatte: ubetenksomme/ overivrige/ nysgjerrige/ frustrerte	Ubetenksomhet eller sterk iver etter å informere, samt nysgjerrighet eller frustrasjon over arbeidsplassen kan føre til at konfidensiell eller feil informasjon legges ut.
Nære relasjoner	Disse aktørene har ofte tilgang på mobile enheter (telefon, iPad, etc), og kjenner i noen grad til passord på disse. Dette er aktører som kan ha uedle motiver, men som også kan komme i skade for å gjøre noe med informasjonen (se på, endre, slette) uten å ha planlagt dette i forkant.
Publikum	Sosiale medier er toveis kommunikasjonskanaler. Dermed er også publikum selv skribenter. Ikke alle er klar over konsekvensene ved å publisere sensitiv informasjon på sosiale medier, slik som personsensitive opplysninger om naboer og andre de ønsker å tipse politiet om, eller opplysninger om seg selv som kan misbrukes av eksempelvis kriminelle.
Fremmed etterretning, kriminelle miljøer (eksempelvis MC-miljøet)	Dette er aktører som ønsker å skaffe seg informasjon om politiets ansatte for å bruke dette til å presse konfidensiell informasjon fra dem, eventuelt påvirke politansattes beslutninger.
Hackere, hacktivister, aktivister, terrorister	Dette er personer som kan ha et ønske om å lamme politiets evne til å kommunisere gjennom denne kanalen, eller å overta den for å skade politiets renomme eller skape destabiliserende situasjoner.
Journalister, mediefolk	Disse aktørene ønsker å få tilgang til informasjon som kan skape sensasjon eller stor oppmerksomhet. Dermed kan de også trekke informasjon ut av sin opprinnelige kontekst og gjengi den slik at den ikke lenger blir korrekt oppfattet.
Samarbeidspartnere	Disse kan reagere negativt på noe politiet har informert om via sosiale medier, og konkludere offentlig på en måte som er til

	skade for politet.
Naturlige og miljømessige	
Teknisk svikt	Kan føre til at internettforbindelsen i politiet blir utilgjengelig eller at de sosiale tjenestene er utilgjengelige .
Sykdom, skade, streik, ferie etc.	Kan føre til at de som publiserer og overvåker de sosiale mediene blir utilgjengelige.

2.7 Sårbarheter

Beskrivelse av hvilke faktorer som kan åpne for at uønskede hendelser kan inntreffe.

Sårbarhet	Skadepotensiale
Din private profil/brukerkonto blir sett på som din offentlige	Kan føre til omdømmetap og tap av trygghet og tillit til politiets ansatte.
Ingen begrensning på hva publikum kan skrive (Facebook og Twitter).	Konfidensiell informasjon kan komme uautoriserte i hende. Moderator må aktivt slette upassende innlegg. Dette kan ta noe tid avhengig av tidspunktet informasjonen legges inn.
Ved ”re-tvitring” mister man muligheten til å slette upassende innlegg.	Innlegg re-tvitres automatisk til de som abbonnerer på denne funksjonen. Dermed sendes potensielt upassende/personsensitive innlegg videre uten at moderator i ettertid kan gå inn og slette disse.
En åpen, uformell tone ”premieres” ved positiv feedback fra leserne/publikum.	De sosiale mediene påvirker den som publiserer gjennom positiv betinging av fleipete, uformelle innlegg. Dette kan føre til at informasjonen som legges ut kan oppfattes feil ut i fra opprinnelig intensjon.
Uklart hvor uformell man skal få lov til å være.	Hvor går grensa mellom flåsete og ”kledelig uformell”? Det er lett å tape omdømme hvis noen opplever at politiet spøker med ting de ikke burde spøke med. Samtidig ønsker ikke politiet å fremstå som byråkratisk.
Informasjon fra blant annet UP’s sider brukes i hovedoppgaver og andre skriftlige dokumenter utenfor politiets kontroll	Informasjonen kan benyttes utenfor opprinnelig kontekst (integriteten svekkes).
Det kan ta lang tid fra en leser legger inn et upassende/personsentivit innlegg og til moderator rekker å slette dette.	Konfidensiell informasjon kan komme uautoriserte i hende. Hvis moderator er syk, på ferie eller har andre oppgaver, kan det ta flere dager før upassende innlegg blir slettet.
Politiet har ingen kontroll på servicenivå eller funksjonalitet hos Facebook, Twitter og andre sosiale media.	Tilgjengeligheten kan svekkes uten at politiet kan gjøre noe med dette. Også opphavsrett til informasjon og hvordan denne eventuelt oppbevares og benyttes i ettertid er utenfor kontroll.
Lav forpliktelse fra politiets interne bidragsytere.	Tilgjengelighet på publisert informasjon varierer fra uke til uke, og det er vanskelig å skape større engasjement og forliktelse fra andre enn kommunikasjonsrådgiveren(-erne).
Overordnet policy for bruk av sosiale medier ikke	Det oppstår avvik i hvordan de sosiale mediene benyttes fra virksomhet til virksomhet.

tilstrekkelig forankret i virksomhetene.	
Det er ikke etablert kurs eller veiledninger i skriving for sosiale medier.	Konfidensialitet og integritet kan rammes. Ujevn kompetanse på sosiale medier i hver enhet. Få klarer å opprettholde en stabil, god tjeneste.
Ulike forvaltning av sidene fra enhet til enhet, mangel på nasjonal standard og "tjenestenivåavtaler" á la den man har for politiet.no eller pressehenvendelser.	Ingen felles "åpningstider". Ujevn responstid. Lav gjenkjennelsesfaktor fra profil til profil. Vanskelig å styre foreventingene til publikum/brukerne av politiets sider på sosiale medier.
Hvem som helst kan opprette en brukerkonto i politiets navn.	Vanskelig å vite for publikum om det er en reell eller fiktiv side de ser på. Vanskelig å fjerne falske politisider.