FORSVARET

Policy for bruk av sosiale medier i Forsvaret

20. mai 2020

Hans Kristian Herland
Kommandør
Sjef Forsvarets sikkerhetsavdeling

Metadata

KORTTITTEL:	Policy for bruk av sosiale medier
SIKKERHETSGRADERING:	Ugradert
HJEMMEL:	Særskilt instruks for sjef Forsvarets sikkerhetsavdeling av 2020-03-01 pkt. 3 a.
GJELDER FOR:	Forsvaret
UTGIVER:	Sjef Forsvarets sikkerhetsavdeling
FAGMYNDIGHET:	Sjef Forsvarets sikkerhetsavdeling
FAGANSVAR:	-
IKRAFTTREDELSE:	2020-05-20
FORRIGE VERSJON:	Policy for bruk av sosiale medier av 2017-10-15

Innhold

Forord **3**

1 Innledning **4**

1.1 FORMÅL 4

1.2 MÅLGRUPPE 4

1.3 DEFINISJONER 4

2 Bruk av sosiale medier **4**

2.1 GENERELT 4

2.2 TAUSHETSPLIKT 5

2.3 PUBLISERING AV INFORMASJON PÅ VEGNE AV FORSVARET 5

2.4 DELING AV INFORMASJON 5

2.4.1 Grunnleggende prinsipper 5

2.4.2 Delingstjenester 5

2.4.3 Kommentarfelt 6

2.4.4 Deling av bilder 6

2.5 PERSONLIG PROFIL OG PASSORD 6

2.6 STEDSTJENESTER 6

2.7 SPAM OG MÅLRETTEDE E-POSTANGREP 7

2.8 BRUK AV BILDE OG VIDEO FRA TJENESTEN I FORSVARET 7

2.9 OPPRETTING AV PROFILER OG GRUPPER 8

2.10 ROLLER 8

2.11 GENERELLE RÅD OG ANBEFALINGER 8

3 Ansvar **9**

4 Risikovurdering **9**

5 Kontakt **9**

6 Rapportering **10**

7 Ikrafttredelse **10**

Forord

Sosiale medier er for mange i Forsvaret en naturlig og enkel måte å kommunisere på og holde kontakten med familie, venner og bekjente. Sosiale medier er internett-tjenester som gir muligheter til deltakelse, dialog, åpenhet og fellesskap, som er viktig for hver enkelt. Dette er også viktig for Forsvaret.

Sosiale medier er nyttige verktøy, men kan også utnyttes av andre, som for eksempel fremmed etterretning, kriminelle og terrorister, for å innhente verdifull informasjon. Denne informasjonen kan brukes for å påvirke deg, dine nærmeste eller Forsvaret på en negativ måte.

Ved å være bevisst på risiko og reflektert over egen bruk av sosiale medier kan du forhindre at verdifull informasjon kommer i feil hender. Denne policyen er ment som et verktøy for å bidra til å forebygge sårbarhet ved å skape refleksjon rundt bruken av sosiale medier.

I denne policyen søkes det å beskrive noen problemstillinger ved bruk av noen eksempler. Det vil ikke være mulig å dekke alle eventualiteter da det sosiale medielandskapet er stort og komplekst. Nye typer sosiale medier og anvendelsen av de eksisterende vil stadig endres, og det er viktig at hver enkelt er bevisst bruken av disse.

1 Innledning

1.1 Formål

Denne policyen har som formål å øke bevisstheten til den enkelte i Forsvaret når det gjelder forholdet til og bruken av internett, herunder spesielt sosiale medier. Forsvarets personell har rett til å ytre seg på lik linje med andre borgere. Det er likevel viktig å være oppmerksom på at ytringsfriheten ikke er absolutt og at det finnes flere lovfestede unntak. For Forsvarets personell innebærer dette en særlig bevissthet om ikke å bryte reglene for personvern og lovpålagt taushetsplikt. Dette gjelder i all bruk av sosiale medier for å unngå at riket, organisasjonen eller personellet utsettes for en risiko, samt å hindre offentliggjøring og kompromittering av skjermingsverdig informasjon.

1.2 Målgruppe

Policyen retter seg mot alle tilsatte og tjenestegjørende i Forsvaret, og omhandler tjenstlig og privat aktivitet i sosiale medier.

1.3 Definisjoner

I denne policyen menes:

a) Sosiale medier[1]: nettbaserte tjenester som via ugraderte kanaler eller plattformer gjør det mulig med mange-til-mange kommunikasjon/interaksjon. Det kan gjøres ved å skrive, dele, kommentere, rangere eller tagge bilder, video eller informasjon. Innholdet skapes i stor grad av brukeren selv. Eksempler på sosiale medier er Facebook, applikasjoner (apper) og kommentarfelt.

b) Skjermingsverdig informasjon: informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig[2].

c) Informasjon: enhver form for opplysninger i materiell eller immateriell form, herunder tekst, bilder og video.

2 Bruk av sosiale medier

2.1 Generelt[3]

Det er viktig å delta i samfunnsdebatter og bruke ytringsfriheten, også ved bruk av sosiale medier. Ytringsfriheten må brukes med bevissthet. Sosiale medier har ubegrenset spredningspotensiale for informasjon, og sensitiv informasjon publisert på sosiale medier gjør skadepotensialet ekstra stort fordi mange har tilgang til den. Informasjon som er publisert på sosiale medier er tilnærmet umulig å fjerne og den vil for alltid være utenfor egen kontroll.

Personlig informasjon publisert på nett kan lett bli utnyttet til å framskaffe informasjon av enda større verdi. Vær bevisst risikoen ved å legge ut kontaktinformasjon eller andre opplysninger som kan identifisere deg, dine nærmeste eller kollegaer. Slik informasjon kan utnyttes til manipulasjon, press, trusler eller som forsøk på å verve insidere.

Det er enkelt å finne ut mye om deg og dine omgivelser bare ved å følge deg på sosiale medier. Din bruk av sosiale medier kan bli kartlagt av flere aktører. Kartleggingen gjøres ved å se på hva du faktisk gjør, men også hvem du kommuniserer med. På denne måten kan det avdekkes hvem du er og hva du gjør, selv om du ikke har publisert noe i din profil eller på dine egne sider.

Det du publiserer på sosiale medier er å regne som offentlig informasjon[4]. Det er uavhengig av hvilke sikkerhetsinnstillinger du har satt på tjenestene du benytter. Selv om enkelte grupper har

[1] Deler av definisjonen er hentet fra store norske leksikon, www.snl.no
[2] Jfr. Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven) § 5-1
[3] For mer informasjon, se Nasjonal sikkerhetsmyndighet (NSM) sitt temahefte 1/2008 «Nettsamfunn og sikkerhet» på nsm.stat.no, samt nettvett.no
[4] Lov 20 mai 2005 nr.28 (straffeloven) § 10.

tilgangsstyring, er de fortsatt på internett og må regnes som åpne. Forvent derfor at alle kan se informasjonen du deler på sosiale medier om jobb, privatliv og hvor du befinner deg. Ikke undervurder verdien av din informasjon. Det vil alltid være fremmede aktører som er interessert i Forsvarets virksomhet og Forsvarets personell, jf. trusselvurderinger fra Politiets sikkerhetstjeneste (PST) og Forsvaret.

2.2 Taushetsplikt

Forsvarets personell er underlagt lovbestemt taushetsplikt. Alle tilsatte og tjenestegjørende i Forsvaret skal ha signert en taushetserklæring. Ved å signere denne bekrefter du at du har satt deg inn i et bestemt sett regler og plikter, og at du er klar over at brudd på taushetserklæringen kan medføre et strafferettslig ansvar. Dette gjelder også etter avsluttet tjeneste eller ansettelsesforhold[5]. Dette setter begrensninger for ytringsfriheten. Det er viktig å være klar over at ytringer i det offentlige rom kan gi etiske, moralske, disiplinære eller strafferettslige konsekvenser. En annen konsekvens kan være tap av autorisasjon eller nedsatt, eller tap av, sikkerhetsklarering.

Vær forsiktig med hva slags informasjon du legger ut på sosiale medier, da du kan kompromittere skjermingsverdig informasjon, skade Forsvarets omdømme eller skape sårbarheter. I tillegg er det viktig å være bevisst trusselen mot Forsvarets personell[6] før du legger ut informasjon om deg selv og dine nærmeste.

2.3 Publisering av informasjon på vegne av Forsvaret

Forsvarets offisielle bruk av sosiale medier reguleres i Direktiv for kommunikasjonsvirksomhet, som fastsetter ansvar og myndighet for kommunikasjonsvirksomhet i Forsvaret. Direktivet beskriver også hvem som uttaler seg i forskjellige medier på Forsvarets vegne.

2.4 Deling av informasjon

2.4.1 Grunnleggende prinsipper

Ved deling av informasjon på sosiale medier er det viktig å være forsiktig og tenke nøye gjennom hva du gjør før du publiserer noe. Er informasjonen allerede lagt ut, er det for sent å få det fullstendig fjernet. Det finnes tjenester, som for eksempel slettmeg.no, som kan gi hjelp.

Det viktigste er hva slags informasjon du legger ut og ikke når du gjør det. Tjenesterelatert informasjon kan være Forsvarets informasjon selv om delingen skjer utenfor tjenestetid. Nedenfor beskrives noen eksempler på deling av informasjon på sosiale medier.

2.4.2 Delingstjenester

Skal du bruke en nettjeneste, som for eksempel Facebook, Instagram eller Snapchat, er det viktig at du setter deg inn i hva det innebærer. Bli kjent med tjenesten, les vilkårene og sett deg inn i hvilke sikkerhetsmessige utfordringer dette kan by på for deg. Vurder hvilke muligheter du har for å ivareta personvernet for deg selv og de rundt deg, og bruk sikkerhetsinnstillingene aktivt. Informasjonen du deler gjøres tilgjengelig for en rekke aktører. «Hemmelige» eller «lukkede» grupper må håndteres som om de er tilgjengelige for alle da det er svært enkelt for uvedkommende å få tilgang til disse gruppene.

Husk at vilkårene for tjenesten kan endre seg, så hold deg oppdatert på det som er gjeldene til enhver tid.

---

[5] Jfr. Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven) § 5-4 og Militær straffelov § 69 mfl

[6] Se årlig trusselvurdering gitt ut av Politiets sikkerhetstjeneste, www.pst.politiet.no, årlig sikkerhetstilstand og risikovurderinger gitt ut av Forsvarets sikkerhetstjeneste (FSA), http://intranett2.mil.no/organisasjon/fsa/Sider/default.aspx, Etterretningstjenestens årlige utgivelse av rapport om sikkerhetsutfordringer FOKUS, www.forsvaret.no samt NSM sine aktuelle nyheter på www.nsm.stat.no

2.4.3 Kommentarfelt

Kommentarfelt er ikke det man tradisjonelt anser som et sosialt medium, men er en arena for meningsutveksling og informasjonsdeling. Det kan oppstå opphetede diskusjoner på nett, og det er fort gjort å la seg rive med. Mange har blitt dratt inn i diskusjoner som kommer ut av kontroll, og flere har kommet med ytringer som kan brukes mot dem på et senere tidspunkt.

Nett-troll og mobbere står ofte bak ondskapsfulle eller provoserende ytringer som kun er ment for å provosere andre i debatten.

Vær kritisk til hva du diskuterer i forum og kommentarfelter, og ikke la deg trekke opp og bli lurt til å komme med ytringer du ikke kan stå for senere.

Tenk over hvordan du ønsker å fremstille deg selv og eventuelt Forsvaret, og at du alltid skal kunne stå inne for det du deler.

2.4.4 Deling av bilder

Et bilde sier mer om deg og omgivelsene dine enn hva du er klar over. Tenk nøye gjennom hva slags bilder du ønsker å publisere, hvordan du ønsker å fremstå offentlig eller hvordan dette kan reflektere deg som person og din rolle i Forsvaret.

Bilder kan si noe om Forsvarets utrustning og kapasiteter som kan være skjermingsverdig informasjon. En større mengde med ugradert informasjon kan samlet være skjermingsverdig informasjon.

Bilder av familie og venner kan manipuleres og utnyttes.

Det er ikke anbefalt å legge ut bilder hvor du er i uniform. Unntaket er om det er i et overordnet samarbeid med Forsvaret eller om du har en offentlig rolle. Forsvarets personell som opptrer i uniform i sosiale medier, kan oppfattes som representanter for Forsvaret. I tillegg er det en attraktiv gruppe for uønsket tilnærming fra fremmede aktører. Se også pkt. 2.1.

Publisering av bilder av andre personer er som en hovedregel ikke tillatt uten deres tillatelse[7]. Det gjelder uansett om det er tjenesterelatert eller privat. Ved publisering av bilder av barn under 15 år er det barnets foresatte som eventuelt gir samtykke[8].

2.5 Personlig profil og passord

Ved opprettelse av bruker på sosiale medier godtar du de retningslinjer som er angitt for tjenesten på det tidspunktet du registrerer deg og for eventuelle endringer i fremtiden. Brukeren som opprettes er personlig og det anbefales ikke at andre gis tilgang til denne.

Det oppfordres til at det brukes passord og tofaktor-autentisering (SMS-kode eller lignende) for pålogging til tjenester på internett for å hindre at kontoen din blir misbrukt av uvedkommende. Bytt passord jevnlig og ved mistanke om kompromittering. Ikke bruk samme passord på mange ulike tjenester.

2.6 Stedstjenester

Mange apper registrerer hvor du er til enhver tid, og flere av disse sender denne informasjonen videre til ukjent tredjepart som kan kartlegge dine bevegelser. Informasjonen kan være interessant grunnet markedsføring eller for aktører som er interessert i informasjon om deg og Forsvaret for å påføre skade. Jo flere apper du laster ned på din telefon eller nettbrett, dess større er sannsynligheten for at din geografiske plassering er tilgjengelig for andre aktører. Ved å sammenstille posisjonsdata, informasjon fra sosiale medier samt offentlig tilgjengelig informasjon, er det ikke vanskelig å avdekke mye detaljert informasjon om deg, din familie, Forsvarets personell, aktivitet og kapasiteter.

[7] Lov 15 juni 2018 nr. 40 om opphavsrett til åndsverk mv. (Åndsverkloven) § 104
[8] Datatilsynet «I beste mening» 2017 pkt. 1 og Åndsverkloven § 104 jf.

Slike stedstjenester eller posisjonsdata kan stort sett blokkeres eller slås av. Det finnes informasjon om hvordan dette gjøres flere steder, avhengig av hvilken type telefon eller nettbrett du har. Vurder å slå av disse stedstjenestene for å redusere skadepotensiale mot deg og Forsvaret.

2.7 Spam og målrettede e-postangrep

Spam er et samlebegrep som benyttes om uønskede e-poster som sendes ut i store kvanta. Begrepet omfatter reklame, propaganda, svindel og forsøk på å stjele personopplysninger. I motsetning til målrettede e-postangrep regnes ikke spam som målrettet, og utformes for å nå flest mulig personer. Temaet og innholdet i e-postene er derfor upersonlig og generelt, og vil ofte framstå mistenkelig.

E-poster med ondsinnet vedlegg er også svært vanlig, og cyberkriminelle sender ut slike e-poster for økonomisk vinning. Konsekvensene av å åpne slike vedlegg kan potensielt bli store.

For å sjekke den faktiske linken tar du musepekeren over linken uten å trykke på den. Det vil da komme opp en boks som viser den faktiske adressen. I slike tilfeller må du ikke tykke på linken.

Ved å eksponere deg på internett kan du gjøre deg til et mål for cyberkriminelle, og ved å tilhøre Forsvaret kan du også utgjøre et mål for fremmed etterretning.

Handlinger som å klikke på linker fra ukjente avsendere eller i mistenkelige e-poster og åpne usikre vedlegg, kan føre til at du kompromitterer din klient og Forsvarets systemer, filområder kan bli kryptert eller man kan bli frastjålet personlig informasjon.

Forsvarspersonell som bruker ugraderte epostkontoer og profiler på sosiale medier, anbefales å utvise stor forsiktig med å klikke på linker fra ukjente kilder og eposter som mottas fra ukjente.

2.8 Bruk av bilde og video fra tjenesten i Forsvaret

De fleste tjenestegjørende og tilsatte i Forsvaret bærer med seg en mobiltelefon eller nettbrett med kamera, muligheter til opptak og internett-tilgang. For å unngå kompromittering av informasjon er det viktig å kjenne til lover og regler som gjelder for bilde- og videobruk. For eksempel:

a) Det er lovregulert å gjøre opptak av eller på annen måte bruke informasjon som gjelder bestemte angitte områder samt offentliggjøring av informasjon om militære anlegg, områder og aktivitet[9].

b) Det kan medføre straffeansvar å offentliggjøre statshemmeligheter som for eksempel gjelder forsvars-, sikkerhets- og beredskapsmessige forhold[10].

c) Det er ikke tillatt å ta bilder eller film av skjermingsverdig informasjon med et kamera som ikke er godkjent for dette[11], eller publisere bilder eller film av sikkerhetsgradert eller taushetsbelagt informasjon[12]. Det kan være forsvarets materiell, personell, aktivitet mm. Er du i tvil om noe er skjermingsverdig informasjon eller ikke, bør du ikke publisere noe før du har rådført deg med avdelingens sikkerhetsorganisasjon. Det er straffbart å publisere informasjon som er sikkerhetsgradert[13].

Forsvarets kommunikasjonsvirksomhet har regelverk som regulerer deres tjeneste[14]. De publiserer informasjon internt i Forsvaret og eksternt via offentlige kanaler. Informasjonen er på forhånd sikkerhetsvurdert og godkjent for publisering.

---

[9] Lov 21 juni 2017 nr. 88 om informasjon om bestemt angitte områder, skjermingsverdige objekter og bunnforhold

[10] Jfr. Lov 20 mai 2005 nr. 28 (straffeloven) § 123, § 124 og § 125

[11] Jfr. Lov om nasjonal sikkerhet av 1. juni 2018 nr 24 (sikkerhetsloven) § 6-3

[12] Sikkerhetsloven § § 5-4

[13] Sikkerhetsloven § § 11-4, jfr. § 5-4

[14] Jfr. Direktiv for kommunikasjonsvirksomhet av 2013-05-01

2.9 Oppretting av profiler og grupper

Ved oppretting av profiler og grupper på sosiale medier gjelder følgende:

a) Ingen profiler, grupper eller sider som gir uttrykk for at de representerer en avdeling eller enhet i Forsvaret skal opprettes uten først å kontakte Forsvarets mediesenter (FMS) på desk@mil.no[15]. FMS har fagansvaret for Forsvarets digitale nærvær[16].

b) Private profiler opprettes på eget ansvar så lenge du følger gjeldende lover og regler.

2.10 Roller

Det er viktig å være bevisst hvem du representerer på sosiale medier. Tilsatte i Forsvaret har en lojalitetsplikt til arbeidsgiver[17]. For vernepliktige og andre som ikke er tilsatt i Forsvaret kan dette falle innunder militær tjenesteplikt[18].

Selv om du opptrer som privatperson, kan meninger og ytringer oppfattes som at du representerer Forsvaret. Du bør derfor være tydelig på om meninger er personlige eller om du uttaler deg på vegne av Forsvaret eller en avdeling i Forsvaret. Det du legger ut i et nettsamfunn eller skriver i en blogg må vurderes på samme måte som om du ville sagt det samme ansikt til ansikt.

Om du har en rolle eller stilling i Forsvaret som er mer offentlig, for eksempel ledere, kommunikasjonsrådgivere eller pressekontakter, kan det være vanskelig å fremstå som en privatperson på sosiale medier. Vær tydelig på hvilken rolle du har når du uttaler deg.

For å tydeliggjøre at du uttaler deg som privatperson, kan du ta inn en ansvarsfraskrivelse ("disclaimer"). Eksempel: *"Dette er en privat (blogg eller annet). Meningene fremført her er mine personlige oppfatninger. Jeg er ikke ansvarlig for innhold på andre nettsteder som det lenkes."*

Hvis du blir kontaktet av media eller skal fremstå med en offentlig profil er det egne retningslinjer for dette[19]. Ta kontakt med din avdeling for avklaring og rådføring. Forsvaret har egne talspersoner som kan bistå[20]. Det er vanlig presseskikk å få sitatsjekket innholdet før en eventuell publisering, men du må selv sørge for å gjøre en avtale om dette på forhånd[21].

2.11 Generelle råd og anbefalinger

Generelle råd og anbefalinger ved bruk av sosiale medier:

a) Etabler og vedlikehold kontakt på sosiale medier kun med mennesker du stoler på.

b) Bruk aktivt de sikkerhetsinnstillingene som er tilgjengelige på de tjenestene du bruker, som for eksempel personverninnstillinger.

c) Etabler gjerne en felles policy i familien, slik at det er en enighet om hva slags informasjon som er greit å dele med andre. Som tilsatt eller tjenestegjørende i Forsvaret kan du og dine nærmeste være mer utsatt for uønsket tilnærming.

d) Informasjon om gjennomføring av operasjoner, for eksempel planer, ordrer, tider, plasser, stridsteknikk, utrustning og våpen, er sannsynligvis sikkerhetsgradert informasjon. Det anbefales ikke å legge ut informasjon om rotasjoner og tidspunkter for leave.

e) Vær kritisk til lenker du får tilgang til gjennom ulike tjenester. Disse kan inneholde skadevare som installeres på maskinen din og deretter spres til dine kontakter.

f) Ikke last ned applikasjoner fra ukjente eller useriøse tilbydere, da disse ofte inneholder skadevare.

---

[15] Jfr. Direktiv for kommunikasjonsvirksomhet av 2013-05-01 pkt. 5.2.2

[16] Jfr. Direktiv for kommunikasjonsvirksomhet av 2013-05-01 pkt. 5.2.2 og Bestemmelser for Forsvarets tilknytning til og bruk av internett av 2012-11-01

[17] Se Etiske retningslinjer for statstjenesten pkt. 2. Se www.regjeringen.no

[18] Jfr. Militær straffelov § 77 og Disiplinærloven § 1.

[19] Jfr. Direktiv for kommunikasjonsvirksomhet av 2013-05-01 pkt. 5.6

[20] Jfr. Direktiv for kommunikasjonsvirksomhet av 2013-05-01 pkt. 5.6

[21] Jfr. «Vær varsom-plakaten» for god presseskikk pkt 3.3. Se www.presse.no

g) Informasjon som du tror er beskyttet, kan bli offentlig på grunn av nettverkets allmenne vilkår. Vilkårene kan også endres uten at du blir gjort oppmerksom på det. Vær også klar over at din informasjon kan bli delt eller solgt videre til tredjepart.

h) Anse alt du deler på internett som tilgengelig for alle med internett-tilgang. Vurder om du ville publisert den samme informasjonen på andre måter, for eksempel ansikt til ansikt.

i) Du bør vurdere behovet for å publisere at du jobber eller tjenestegjør i Forsvaret og eventuelt hva du jobber med.

j) Informasjon om avdelingstilhørighet og arbeidsoppgaver bør ikke publiseres uten at dette er godkjent av avdelingssjef.

k) Tjenesterelaterte bilder bør ikke publiseres uten at dette er godkjent av avdelingens sikkerhetsleder eller sikkerhetskontakt(ASL/ASK) eller avdelingssjef, da bildene kan inneholde skjermingsverdig informasjon. Dette gjelder også ved hendelser eller ulykker i tjenesten. Forsvaret har egne offentlige kommunikasjonslinjer som håndterer slik informasjon.

l) Tjenestegjør du i internasjonale operasjoner bør du ikke legge ut informasjon om dette på sosiale medier. Det gjelder også familiemedlemmer. Dette er av hensyn til din egen og andres sikkerhet.

m) Bilder eller film av privat karakter som viser flere tilsatte eller tjenestegjørende i Forsvaret, skal som nevnt i pkt. 2.4.4 ikke publiseres på nett uten at de som er på bildet eller opptaket har samtykket til dette. Unntaket er om det er store folkemengder, som for eksempel et 17. mai-tog.

n) Ved den minste tvil bør du ikke publisere informasjonen.

3 Ansvar

Den enkelte er ansvarlig for egne handlinger på sosiale medier.

Enhver avdelingssjef i Forsvaret har ansvar for at denne policy er kjent i avdelingen, og at det er etablert gode holdninger til bruk av sosiale medier. Det anbefales rutinemessig å ta med et punkt om bruk av sosiale medier i for eksempel avdelingens stående ordre, øvelsesordre og eventuelt i ordren til hvert enkelt oppdrag.

4 Risikovurdering

Sikkerhetsgradert informasjon skal ikke publiseres på sosiale medier. Det er den som tilvirker informasjonen som vurderer hvilken sikkerhetsgradering informasjonen har[22]. En mengde av lavere sikkerhetsgradert informasjon, eller en mengde med ugradert informasjon, kan samlet ha en høyere sikkerhetsgradering.

Trusselen Forsvaret og Forsvarets personell står ovenfor vil endre seg. Det er viktig å kjenne til trusselen for å kunne vite hvordan den kan forebygges og på hvilken måte vi alle kan bidra til å redusere sårbarheter og sikkerhetstruende hendelser. Vurdering av risiko ved bruk av sosiale medier bør gjennomføres før publisering av informasjon, uansett om det er i regi av Forsvaret eller som privatperson.

5 Kontakt

Følgende kan kontaktes for spørsmål eller avklaringer:

a) Avdelingens sikkerhetsleder
b) Nærmeste linjeleder
c) Forsvarets sikkerhetsavdeling via FSA Kontakt (postboks)

[22] Sikkerhetsloven § 5-3

6 Rapportering

Ved kritikkverdige forhold på sosiale medier kan det rapporteres som nevnt i pkt. 5. Sikkerhetstruende hendelser skal rapporteres iht. Bestemmelse om sikkerhetsrapportering.

7 Ikrafttredelse

Policy for bruk av sosiale medier i Forsvaret trer i kraft 2020-05-20. Samtidig settes Policy for bruk av sosiale medier av 2017-10-15 ut av kraft.