Kapittel 1
Vedlegg
M

Bestemmelser vedrørende logger i Forsvarets personellregister (Hovedrulla)

BESTEMMELSER VEDRØRENDE LOGGER I FORSVARETS PERSONELLREGISTER

1-M 1 Innledning

Tilgang til personopplysninger i Forsvarets personellregister (Hovedrulla) gis etter autorisasjon med bakgrunn i tjenestelig behov.

For å forebygge og avdekke eventuell misbruk av autorisasjon for tilgang til og bruk av personopplysninger i registeret, er det etablert rutiner for ettersyn og evaluering av logger. Systemet loggfører fortløpende hvilken bruker som har gjort oppslag på personer i registeret og hvilken informasjon som er slått opp eller endret.

De overordnede logger skal sjekkes fortløpende og minimum kvartalsvis av den/de brukere som innehar roller som loggkontrollører. Mer detaljerte kontroller utføres dersom de overordnede logger gir mistanke om misbruk av autorisasjon. Det er bare autoriserte loggkontrollører som vil ha tilgang til de data som fremkommer av loggene.

Tilgang til personopplysninger i Forsvarets personellregister (Hovedrulla) gis etter tjenestelig behov, og all bruk av systemet logges.

1-M 2 Roller med ansvar for evaluering av logger

Sjef VPV eller den han bemyndiger er ansvarlig for å følge opp logger i personellregisteret for å hindre, samt avdekke misbruk av autorisasjon.

Rollen som loggkontrollør kan bare tildeles av VPV og skal bare innehas av personell tilsatt ved VPV eller Forsvarets personelltjenester (FPT).

Det utarbeides kvartalsvise rapporter vedrørende gjennomført kontroll. Rapport med resultat og forslag til tiltak fremlegges sjef VPV.

1-M 3 Rutiner for evaluering av logger

1-M 3.1 Beskrivelse av logger

1-M 3.1.1 Pålogging (all pålogging på registeret)

- ✓ Fødselsnummer til bruker
- ✓ Brukernavn
- ✓ Avdelingstilhørighet
- ✓ Tidspunkt for pålogging
- ✓ Tidspunkt for avlogging
- ✓ Applikasjon
- ✓ Operativsystembruker
- ✓ Servernavn
- ✓ PC-navn

1-M 3.1.2 Endrings- og innsynslogg (alle oppslag og endringer på data i registeret)

- ✓ Brukernavn
- ✓ Brukers avdelingstilhørighet
- ✓ Tidspunkt
- ✓ Fødselsnummer på person
- ✓ Navn på informasjonselement
- ✓ Komplett innhold før eventuell oppdatering
- ✓ Komplett innhold etter eventuell oppdatering

1-M 3.1.3 Personellmapper (dokumenter som er skannet)

- ✓ Fødselsnummer til bruker
- ✓ Brukernavn
- ✓ Brukers avdelingstilhørighet
- ✓ Tidspunkt for oppslag
- ✓ Fødselsnummer på person som slås opp
- ✓ Type personell mappe
- ✓ Eksakt hvilket dokument

1-M 3.1.4 Overføring av data fra Folkeregisteret til "Hovedrulla"

- ✓ Fødselsnummer til bruker som initierte overføringen
- ✓ Brukernavn
- ✓ Brukers avdelingstilhørighet
- ✓ Tidspunkt for første overføring
- ✓ Tidspunkt for siste oppdatering
- ✓ Angivelse av om også pårørende (dvs. mor og far) også ble overført (disse logges også vær for seg)

1-M 3.1.5 Oppslag i Folkeregisteret

- ✓ Brukernavn
- ✓ Fødselsnummer som slås opp
- ✓ Tidspunkt for oppslag
- ✓ Applikasjon

1-M 3.1.6 Eget rulleblad (Ansatte har innsyn i eget rulleblad gjennom Forsvarets Intranett)

- ✓ Brukernavn
- ✓ Fødselsnummer som slås opp
- ✓ Fødselsnummer på bruker som utførte oppslaget (disse to fødselsnumrene skal være like)
- ✓ Tidspunkt for oppslag

1-M 3.1.7 Kontroll av brukertilganger

1. All tildeling og endringer av tilganger logges i endringsloggen
2. Bruker må være sikkerhetsklarert eller autorisert av lokal sikkerhetsansvarlig for å kunne logge seg på
3. Brukertilgang termineres automatisk hvis sikkerhetsklarering inndras
4. Bruker kan ikke gi seg selv tilgang ei heller oppdatere noen opplysninger om seg selv

5. Egen rapport som gir oversikt over hva de ulike roller gir tilgang til
6. Oversikt over alle brukere med hvilke tilgang de har.
7. Eget skjermbilde som kontrollerer alle brukere og lister advarsler for brukere der tilgangen bør vurderes.

   Tilganger kan inndras direkte i dette skjermbildet. Følgende advarsler gis pr. bruker:

   - ✓ Brukers avdeling er nedlagt
   - ✓ Sikkerhetsklarering utløpt (til forskjell fra inndratt)
   - ✓ Autorisasjon fra lokal sikkerhetsansvarlig mangler
   - ✓ Ikke lenger i tjeneste
   - ✓ Ikke vært pålogget siste 6 måneder
   - ✓ Har rettigheter til å oppdatere alle personer
   - ✓ Har rettigheter til å se alle personer
   - ✓ Har brukertilgang knyttet til en annen avdeling enn sitt eget tjenesteforhold

1-M 3.2 Kontroll av endringer og oppslag av personopplysninger

Det skal kontrolleres om det finnes brukere som gjør oppslag på personer som ikke kan begrunnes i tjenestelig behov. Dette gjøres ved å benytte et loggregnskap der det listes opp brukere som har gjort oppslag på personer i andre avdelinger enn egen avdeling. Det listes opp brukere som har gjort oppslag på personer utenfor egen avdeling sortert på antall oppslag av den enkelte bruker. Brukere som har gjort oppslagene identifiseres med navn, ansattnummer og avdelingstilknytning. Personene det blir gjort oppslag på identifiseres på samme måte.

Det skal kontrolleres om det er personer det gjøres uforholdsmessig mange oppslag på i forhold til andre personer. Dette for å avdekke om det er personer som brukere fra flere avdelinger gjør oppslag på uten at det er tjenestelig behov for dette. Loggen sorterer data med bakgrunn i hvor mange oppslag som har blitt gjort på de aktuelle personene. Brukere som har gjort oppslagene identifiseres med navn, ansattnummer og avdelingstilknytning. Personene det blir gjort oppslag på identifiseres på samme måte.

Det skal kontrolleres om det finnes bilder av personer det gjøres uforholdsmessig mange oppslag på. Der det kommer frem av loggene at det finnes bilder av personer som hentes frem av mange brukere eller bildene har mange treff med oppslag gjort av samme person, skal det kontrolleres om det er sannsynlig tjenestemessig sammenheng mellom den bruker/de brukere som har gjort oppslaget og personen som er slått opp.

1-M 3.3 Evaluering av logger av bruk

1-M 3.3.1 Loggevaluering på personnivå (Rulleblad)

I de tilfeller det er personer som utpeker seg i den kontrollen som gjøres i loggregnskapet, skal forholdet kontrolleres nærmere. Dette gjøres i rullebladet til den enkelte person. Her vises alle oppslag på person, med hvilken bruker som har gjort oppslag på hvilken informasjon. Brukere som har gjort oppslagene identifiseres med navn, ansattnummer og avdelingstilknytning. Personene det blir gjort oppslag på identifiseres på samme måte. Denne funksjonaliteten omfatter også oppslag i skannet personellmappe.

1-M 3.3.2 Loggevaluering på brukernivå (Administrasjon og drift)

I de tilfeller det er brukere som utpeker seg i den kontrollen som gjøres i loggregnskapet, skal forholdet undersøkes nærmere. I logg som er knyttet til brukers konto vises alle oppslag gjort av bruker, med hvilke personer det har blitt gjort oppslag på, samt hvilken informasjon brukeren har slått opp. Brukeren som har gjort oppslagene identifiseres med navn, ansattnummer og

avdelingstilknytning. Personene det blir gjort oppslag på identifiseres på samme måte. Denne funksjonaliteten omfatter også oppslag i skannet personellmappe

1-M 3.3.3 Logg som kontrollerer oppslag i skjermbilder (Administrasjon og drift)

Kontroll for å vise oppslag pr skjermbilde, rapport og fanekort. Dette gjøres for å se alle brukere som har gjort oppslag på en gitt informasjon (for eksempel fanekort tjenesteuttalelser), og for å se hvilke personer oppslagene er gjort på. Brukere som har gjort oppslagene identifiseres med navn, ansattnummer og avdelingstilknytning. Personene det blir gjort oppslag på identifiseres på samme måte.

1-M 3.3.4 Endringslogg (Rulleblad)

Loggen viser alle endringer som er gjort på et rulleblad. Det vises både endringer som er gjort i P3 og endringer som er kommet via eksterne grensesnitt. Endringer som gjøres i P3 logges med brukernavn og fødselsnummer til bruker som har gjort endringen, mens en endring fra eksterne grensesnitt vil logges med brukernavn på en systembruker.

1-M 3.3.5 Logg for pålogging (Administrasjon og drift)

Fanekort i Vedlikehold brukere (AD101S) for Påloggінger, her vises alle påloggінger bruker har gjort, med hvilken Pc, citrix-server og FISBasis bruker.

1-M 4 Tiltak ved funn av uregelmessigheter

1-M 4.1 Bakgrunn for logging og autorisasjon

Håndtering av personopplysninger som er lagret i Hovedrulla, skal skje i samsvar med Lov om behandling av personopplysninger (Personopplysningsloven). Formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av opplysninger, og at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn. Tilgang til personopplysningene gis til brukere med bakgrunn i forutgående autorisasjon. Hvis det avdekkes at tilgang har blitt misbrukt kan dette få konsekvenser for den enkelte bruker av systemet.

Tilgang til personopplysninger i Forsvarets personellregister (Hovedrulla) gis etter autorisasjon og skal kun nyttes tjenestemessig.

1-M 4.2 Misbruk av autorisasjon

Ved autorisasjon for tilgang til Hovedrulla, signerer den enkelte bruker for de regler som gjelder med tanke på bruk av systemet, samt mulige konsekvenser ved eventuelt misbruk.

Hvis det under evaluering av logger avdekkes uregelmessigheter der det er rom for mistanke om uautorisert bruk, skal loggkontrollører vurdere om det først er nødvendig å følge opp logger på bruker over tid for å se om det er et mønster i bruk av systemet som er av uønsket art. Hvis mistanken som en følge av dette styrkes, skal forholdet først tas opp med den enkelte bruker, og deretter følges opp tjenestevei.

1-M 4.3 Konsekvenser ved misbruk

Dersom det avdekkes misbruk av tilgang til personopplysningene som er lagret i Hovedrulla, vil dette kunne få konsekvenser for den enkelte bruker/ansatt. Gjentatt eller alvorlig misbruk av tilgangsrettighetene vil kunne føre til at autorisasjon/tilgang inndras for kortere eller lengre tid.

Ved førstegangs avdekking av mulig uautorisert bruk vil loggkontrollør gjennom dialog med bruker søke å avdekke om bruken er uautorisert. Resultatet av denne dialogen logges.

Hvis bruken viser seg å være uautorisert, eller der det fremkommer et mønster som tyder på utstrakt misbruk skal det via tjenestevei tas kontakt med avdelingssjef, som tar opp forholdet med den enkelte bruker.

Gjentatt uautorisert bruk av tilgangsrettighetene og ved forhold av særlig graverende art vil føre til tap av autorisasjon.

Autorisasjon for tilgang til personopplysninger i Hovedrulla kan inndras av:

1. Lokal sjef
2. Sjef FPT
3. Sjef VPV