Åklagarmyndighetens författningssamling

ÅKLAGARMYNDIGHETEN

ÅFS 2014:7

Publiceringsdatum:
30 september 2014

Åklagarmyndighetens föreskrifter om IT-säkerhet inom åklagarväsendet;

beslutade den 29 september 2014.

Åklagarmyndigheten föreskriver med stöd av 1 b § åklagarförordningen (2004:1265) följande.

1 § Rikspolisstyrelsen har med stöd av 43 och 44 §§ säkerhetsskyddsförordningen (1996:633) meddelat föreskrifter och allmänna råd om säkerhetsskydd (RPSFS 2010:3, FAP 244-1) som gäller även för åklagarväsendet.

2 § För Ekobrottsmyndighetens verksamhet gäller dessa föreskrifter endast i fråga om åklagarväsendets gemensamma IT-infrastruktur.

3 § I dessa föreskrifter avses med

myndighetschef: riksåklagaren och chefen för Ekobrottsmyndigheten,

områdeschef: chef för åklagarområde inom Åklagarmyndigheten samt chefen för den nationella åklagaravdelningen samt verksamhetschefen vid Ekobrottsmyndigheten

chef för åklagarkammare: chef för åklagarkammare eller riksenhet inom Åklagarmyndigheten och ekobrottskammare inom Ekobrottsmyndigheten

enhetschef: chef för avdelning och enhet vid Åklagarmyndighetens huvudkontor och Ekobrottsmyndighetens huvudkontor, chef för utvecklingscentrum samt chef för polisoperativ enhet inom Ekobrottsmyndigheten,

personal inom åklagarväsendet: anställd personal vid Åklagarmyndigheten och Ekobrottsmyndigheten, poliser som tjänstgör vid Ekobrottsmyndigheten samt uppdragstagare vid respektive myndighet,

datamedia: media som kan lagra data såsom hårddisk, band, CD, DVD och elektroniskt minne,

IT-system: ett informationsbehandlingssystem som baseras på informationsteknik, såsom datorkommunikations- eller datorsystem,

IT-utrustning: materiel såsom datorer, mobila enheter, datamedia, kablage eller nätverksutrustning som anskaffats för tjänstebruk inom åklagarväsendet,

åklagarväsendets gemensamma IT-infrastruktur: åklagarväsendets gemensamma nätverk för datakommunikation samt de godkända programvaror och IT-utrustningar som är anslutna till detta nätverk,

behörighet: tilldelad åtkomsträttighet till IT-system,

behörighetsprofil: beskrivning av en behörig användares samlade rättigheter i ett IT-system,

behörighetsadministratör: person som ansvarar för inregistrering och avregistrering av behörigheter i IT-system.

Ledning m.m.

4 § Myndighetschefen har det övergripande ansvaret för säkerheten i samband med all informationsbehandling vid myndigheten. Myndighetschef får delegera sådant ansvar till områdeschef, chef för åklagarkammare och enhetschef eller annan befattningshavare enligt myndighetschefens bestämmande.

5 § För IT-säkerhetsarbetet inom åklagarväsendet ska finnas en IT-säkerhetschef och en ersättare för denne. För IT-säkerhetschefen ska finnas en särskild instruktion. IT-säkerhetschefen utses av riksåklagaren.

Vid Ekobrottsmyndigheten ska finnas en IT-säkerhetsansvarig som biträder myndighetens chef och IT-säkerhetschefen i IT-säkerhetsarbetet i åklagarväsendets gemensamma IT-infrastruktur. IT-säkerhetsansvarig utses av chefen för Ekobrottsmyndigheten.

6 § För centrala eller gemensamma system och resurser ska särskilda verksamhetsansvariga finnas utsedda. Verksamhetsansvaret för system ska vara reglerat vid respektive myndighet i arbetsordningen. IT-säkerhetschefen ansvarar dock för att IT-säkerheten i systemet eller resursen följer lagar, gällande styrdokument samt de IT-säkerhetskrav och andra beslut som fattas av IT-säkerhetschefen**.**

7 § Varje användare av åklagarväsendets IT-system ansvarar för att säkerheten upprätthålls genom att följa regler och instruktioner samt anmäla iakttagna incidenter, fel och brister**.**

8 § IT-utrustning ska förvaras på ett sådant sätt att obehöriga inte kan få tillgång till utrustningen, till i utrustningen lagrade uppgifter eller via utrustningen få tillgång till uppgifter lagrade i annan IT-utrustning**.**

9 § Dataserver, kommunikationsutrustning och krypteringsutrustning ska förvaras i särskilt skyddat utrymme. Myndighetschef, IT-direktör,

IT-chef, områdeschef, chef för åklagarkammare, IT-ansvarig och IT-samordnare vid myndighet och IT-administratör vid kammare eller enhet samt deras ersättare eller annan person som av myndighetschef eller IT-säkerhetschef fått särskilt tillstånd har tillgång till sådant skyddat utrymme. Tillträdesbehörighet till särskilt skyddat utrymme vid Ekobrottsmyndigheten beslutas av chefen för Ekobrottsmyndigheten. Sådant beslut får delegeras till IT-ansvarig, verksamhetsskyddschef samt deras ersättare**.**

Behörighet m.m.

10 § Myndighetschef beslutar om behörighet, upphörande av behörighet, behörighetsprofil och ändring av behörighetsprofil. Sådant beslut får delegeras till IT-direktör, områdeschef, chef för åklagarkammare och enhetschef.

Beslut verkställs av utsedd behörighetsadministratör. Beslut och verkställighet av beslut ska skriftligen dokumenteras.

11 § Endast personal inom åklagarväsendet har rätt att använda åklagarväsendets IT-utrustningar självständigt. Vad som nu sagts gäller inte för terminal som tillhandahålls för allmänheten.

IT-säkerhetschefen och IT-säkerhetsansvarig vid Ekobrottsmyndigheten får medge undantag från vad som sägs i första stycket.

12 § IT-utrustning tillhörande åklagarväsendet syftar till att användas i samband med tjänsteutövning. Tjänsteman har, oberoende av tilldelad behörighet och behörighetsprofil, rätt att ta del av information från åklagarväsendets IT-system endast i den utsträckning som krävs för vederbörandes tjänsteutövning.

IT-säkerhetschefen och IT-säkerhetsansvarig vid Ekobrottsmyndigheten får medge undantag från vad som sägs i första stycket.

Säkerhet m.m.

13 § Endast åklagarväsendets och andra RIF-myndigheters datamedia får användas i åklagarväsendets IT-utrustningar. Med RIF-myndigheter avses de myndigheter som ingår i rättsväsendets informationsförsörjning enligt beslut av regeringen. Åklagarväsendets datamedia får inte användas i andra än åklagarväsendets IT-utrustningar, med undantag för andra RIF-myndigheters IT-utrustning. Undantag gäller även för s.k. hemdatorer som anskaffats av åklagarväsendet samt för privata datorer som den anställde disponerar under förutsättning att sådan har aktiverad brandvägg och uppdaterat virusskydd. Den anställde får dock inte lagra arbetsinformation på en sådan dator om informationen omfattas av sekretess.

IT-säkerhetschefen och IT-säkerhetsansvarig vid Ekobrottsmyndigheten får medge undantag från vad som sägs i första stycket.

14 § Endast åklagarväsendets programvaror får användas i system som är anslutna till åklagarväsendets gemensamma IT-infrastruktur. Endast åklagarväsendets IT-utrustningar får användas i system som är anslutna till åklagarväsendets gemensamma IT-infrastruktur, med undantag för vad som sägs i 13 §. Det är tillåtet att sammankoppla åklagarväsendets IT-utrustning med annan myndighets projektor och vice versa, under förutsättning att separat programvara inte installeras.

IT-säkerhetschefen får medge undantag från vad som sägs i första stycket.

15 § Hemliga uppgifter lagrade på datamedia ska hanteras på samma sätt som hemliga handlingar i enlighet med FAP 244-1. Detsamma gäller datamedia som innehållit hemlig uppgift.

16 § Utbyte av fast monterat datamedia får inte ske utan tillstånd av IT-säkerhetschefen eller IT-ansvarig vid Ekobrottsmyndigheten. IT-säkerhetschefen respektive IT-säkerhetsansvarig vid Ekobrottsmyndigheten ska lämna erforderliga anvisningar hur arbetet får utföras och hur det demonterade datamediet ska hanteras**.**

17 § Externa uppkopplingar mot åklagarväsendets gemensamma IT-infrastruktur får inte ske utan tillstånd av IT-säkerhetschefen.

Sådan uppkoppling och tillstånd som avses i första stycket ska dokumenteras.

18 § IT-säkerhetschef respektive IT-säkerhetsansvarig ansvarar för att kontroll och uppföljning fortlöpande sker av IT-säkerheten i enskilda system med tillhörande rutiner samt att personalen får utbildning i IT-säkerhet**.**

19 § Åklagarmyndighetens IT-säkerhetschef beslutar vilka datautrustningar och programvaror som får användas i system som är anslutna till åklagarväsendets gemensamma IT-infrastruktur**.**

20 § IT-säkerhetschefen beslutar om begränsningar i rätten att sända och ta emot e-post som innehåller vissa typer av bilagor samt begränsningar för extern åtkomst till åklagarväsendets e-postsystem, om det behövs för att säkerställa driften av e-postsystemet eller för att upprätthålla en godtagbar säkerhetsnivå på IT-säkerheten i åklagarväsendets gemensamma IT-infrastruktur**.**

21 § Personal inom åklagarväsendet som misstänker försök till dataintrång, förekomst av datavirus eller annat hot mot informationssystem eller brist däri, ska omgående rapportera detta till åklagarmyndighetens IT-enhet, som ska vidarebefordra rapporten till IT-säkerhetschefen. Detsamma gäller rapportering av generella hot mot samhällets informationssystem och som skulle kunna utgöra ett hot även mot åklagarväsendets informationssystem. Ekobrottsmyndighetens personal ska rapportera till Ekobrottsmyndighetens IT-funktion, som i sin tur rapporterar till Åklagarmyndighetens IT-enhet**.**

Övrigt

22 § Finner IT-säkerhetschefen vid inspektion eller på annat sätt allvarliga brister i IT-säkerheten får han fatta de beslut som behövs för att avhjälpa bristen.

Bedömer IT-säkerhetschefen det vara nödvändigt för att upprätthålla en godtagbar säkerhetsnivå får IT-säkerhetschefen stoppa användningen av IT-utrustningen helt eller delvis.

Fattar IT-säkerhetschefen sådant beslut, som föreskrivs i första eller andra stycket, ska han utan dröjsmål underrätta riksåklagaren samt chefen för Ekobrottsmyndigheten och IT-säkerhetsansvarig vid Ekobrottsmyndigheten.

Vad som sagts om IT-säkerhetschefen i första och andra stycket gäller även för IT-säkerhetsansvarig vid Ekobrottsmyndigheten såvitt gäller brister i IT-säkerheten och användningen av IT-utrustning vid Ekobrottsmyndigheten. Fattar IT-säkerhetsansvarig ett sådant beslut ska även IT-säkerhetschefen utan dröjsmål underrättas.

Denna författning träder i kraft den 1 oktober 2014. Samtidigt upphör ÅFS 2006:1 att gälla.

ANDERS PERKLEV

Anders Thoursie
(IT-avdelningen)