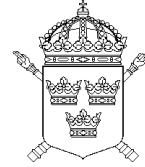


# Åklagarmyndighetens författningssamling



## Åklagarmyndighetens föreskrifter om IT-säkerhet inom åklagarväsendet;

ÅFS 2006:1

Utkom från trycket  
den 8 maj 2006

beslutade den 8 maj 2006.

Åklagarmyndigheten föreskriver med stöd av 3 § förordningen (2004:1266) med instruktion för Åklagarmyndigheten följande.

**1 §** Rikspolisstyrelsens (RPS) föreskrifter och allmänna råd om säkerhetsskydd (RPSFS 2004:11, FAP 244-1) beslutade den 2 december 2004 skall i tillämpliga delar gälla för åklagarväsendet.

**2 §** I dessa föreskrifter avses med:

**myndighetschef:** chefen för Åklagarmyndigheten och chefen för Ekobrottsmyndigheten,

**chef för åklagarkammare:** chef för åklagarkammare inom Åklagarmyndigheten och Ekobrottsmyndigheten,

**enhetschef:** chef för avdelning och enhet vid Riksåklagarens kansli och Ekobrottsmyndighetens stab, chef för utvecklingscentrum, chef för riksenhet inom Åklagarmyndigheten samt chef för polisoperativ enhet och operativ serviceenhet inom Ekobrottsmyndigheten,

**personal inom åklagarväsendet:** anställd personal vid Åklagarmyndigheten och Ekobrottsmyndigheten samt poliser som tjänstgör vid Ekobrottsmyndigheten.

**datamedia:** Utrustning som kan lagra data såsom hårddisk, band, flexskivor, CD, DVD och elektroniskt minne,

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

**IT-utrustning:** materiel såsom datorer, 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.**

3 § Myndighetschefen har det övergripande ansvaret för säkerheten i samband med all informationsbehandling vid myndigheten. Myndighetschef får delegera sådant ansvar till chef för åklagarkammare och enhetschef.

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

Vid Ekobrottsmyndigheten får finnas en IT-säkerhetsansvarig som biträder myndighetens chef och IT-säkerhetschefen i IT-säkerhetsarbetet. IT-säkerhetsansvarig utses av myndighetschefen.

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

6 § IT-utrustning skall 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.

7 § Dataserver, kommunikationsutrustning och krypteringsutrustning skall förvaras i särskilt skyddat utrymme. Myndighetschef, 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 fått särskilt tillstånd har tillgång sådant skyddat utrymme.

### **Behörighet m.m.**

8 § Myndighetschef beslutar om behörighet, upphörande av behörighet, behörighetsprofil och ändring av behörighetsprofil. Sådant beslut får delegeras till chef för åklagarkammare och enhetschef.

Beslut verkställs av utsedd behörighetsadministratör. Beslut och verkställigheten av beslut skall skriftligen dokumenteras.

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

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

**10 §** IT-utrustning tillhörande åklagarväsendet får endast 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.

### **Säkerhet m.m.**

**11 §** Endast åklagarväsendets datamedia får användas i åklagarväsendets IT-utrustningar.

Åklagarväsendets datamedia får inte användas i andra än åklagarväsendets IT-utrustningar. Undantag gäller för s.k. hemdatorer som anskaffats av åklagarväsendet samt för privata datorer som den anställde disponerar. Den anställde får dock inte lagra arbetsinformation på en sådan dator om informationen omfattas av sekretess.

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

**12 §** Endast åklagarväsendets IT-utrustningar och programvaror får användas i system som är anslutna till åklagarväsendets gemensamma IT-infrastruktur.

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

**13 §** Hemliga uppgifter lagrade på datamedia skall hanteras på samma sätt som hemliga handlingar. Detsamma gäller datamedia som innehållit hemlig uppgift.

**14 §** Myndighetschef, chef för åklagarkammare samt enhetschef eller den de utser ansvarar för att datamedia till vilket allmänheten har tillgång inte innehåller hemlig uppgift.

**15 §** Utbyte av fast monterat datamedia får inte ske utan tillstånd av IT-säkerhetschefen. IT-säkerhetschefen skall lämna erforderliga anvisningar hur arbetet får utföras och hur det demonterade datamediet skall hanteras.

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

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

**17 §** Myndighetschefen ansvarar för att kontroll och uppföljning fort-löpande sker av IT-säkerheten i enskilda system med tillhörande manu-ella rutiner samt att personalen får utbildning i IT-säkerhet.

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

**19 §** Personal inom åklagarväsendet som misstänker försök till data-intrång, förekomst av datavirus eller annat hot mot informationssystem eller brist däri, skall omgående rapportera detta till åklagarmyndig-hetens IT-enhet, som skall vidarebefordra rapporten till IT-säkerhets-chefen. Detsamma gäller rapportering av generella hot mot samhällets informationssystem och som skulle kunna utgöra ett hot även mot åkla-garväsendets informationssystem.

### **Övrigt**

**20 §** Finner IT-säkerhetschefen vid inspektion eller på annat sätt all-varliga 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, skall han utan dröjsmål underrätta riksåklagaren och myndighetens chef.

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 användning av IT-utrustning vid Ekobrotts-myndigheten. Fattar IT-säkerhetsansvarig ett sådant beslut skall även IT-säkerhetschefen utan dröjsmål underrättas.

---

Denna författning träder i kraft den 8 maj 2006. Den ersätter ÅFS 2005:22.

FREDRIK WERSÄLL

/Bertil Metzger  
(Administrativa avdelningen)