

# Åklagarmyndighetens författningssamling



## Åklagarmyndighetens föreskrifter om it-säkerhet inom åklagarväsendet

ÅFS 2023:5

Publicerade den 31  
augusti 2023

Utfärdade den 30 augusti 2023

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

**1 §** För Ekobrottsmyndighetens verksamhet gäller dessa föreskrifter endast i fråga om åklagarväsendets gemensamma it-infrastruktur.

**2 §** I dessa föreskrifter avses med

*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, USB och annat 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*: Åklagarmyndighetens it-infrastruktur, vilken används som gemensam it-infrastruktur i åklagarväsendet, och de godkända system, programvaror och it-utrustningar som är anslutna till denna it-infrastruktur,

*behörighet*: tilldelad åtkomsträttighet till it-system, resurser eller filer.

### Ledning m.m.

**3 §** För it-säkerhetsarbetet inom åklagarväsendets gemensamma it-infrastruktur ska det finnas en it-säkerhetschef och en ersättare som it-säkerhetschefen utser. It-säkerhetschefen utses av riksåklagaren.

**4 §** För centrala eller gemensamma system och resurser ska särskilda verksamhetsansvariga finnas utsedda. Den som är verksamhetsansvarig för ett system är ansvarig för funktionella krav på systemet.

Åklagarmyndighetens it-direktör är ansvarig för icke-funktionella krav på centrala eller gemensamma system och resurser och för det fall någon verksamhetsansvarig inte utsetts även för funktionella krav.

**5 §** Åklagarväsendets gemensamma it-infrastruktur är avsedd att utgöra ett stöd för åklagarverksamhet och får bara användas för de ändamål som Åklagarmyndigheten fastställt.

**6 §** It-säkerhetschefen ansvarar för att system eller andra it-resurser i den gemensamma it-infrastrukturen följer lagar, styrdokument och beslut för it-säkerheten.

**7 §** Varje användare av åklagarväsendets gemensamma it-infrastruktur 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. Centrala serverhallar och lokala serverrum utgör sådana utrymmen som ska vara särskilt skyddade. Tillträdesbehörighet till centrala serverhallar och lokala serverrum vid Åklagarmyndigheten beslutas av riksåklagaren eller den som riksåklagaren delegerat detta till.

Tillträdesbehörighet till särskilt skyddat utrymme vid Ekobrottsmyndigheten beslutas av generaldirektören vid Ekobrottsmyndigheten eller den som generaldirektören delegerat detta till.

### **Behörighet m.m.**

**10 §** Åklagarmyndighetens it-direktör ska besluta om behörighetsmodeller för infrastrukturen och samtliga it-system som tillhandahålls i åklagarväsendets gemensamma it-infrastruktur. Av modellen ska framgå roller, typer av behörigheter och beslutsstruktur för respektive behörighet och system.

Tilldelning och borttagande av behörigheter verkställs av Åklagarmyndighetens centrala behörighetsadministration. Verkställande får endast ske om begäran gjorts av behörig person. Beslut ska dokumenteras skriftligen.

För verkställande av behörighetsbeslut ska det finnas ett av it-direktören fastställt beslut om vilka befattningar som har tilldelats roller som har rätt att fatta beslut om tilldelning och upphörande av de behörigheter som framgår av respektive behörighetsmodell.

I de fall en behörighetsmodell ännu inte har fastställts för ett it-system får Åklagarmyndighetens it-direktör besluta om en tillfällig behörighetsmodell och rutiner för tilldelning av behörigheter inom den tillfälliga behörighetsmodellen.

**11 §** Endast personal inom åklagarväsendet har rätt att självständigt använda it-utrustning som ingår i eller är anslutna till åklagarväsendets gemensamma it-infrastruktur. Detta gäller inte för anställda vid externa tillsynsorgan som har att utöva tillsyn över verksamheten i åklagarväsendet och har rätt att ta del av uppgifter.

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

**12 §** Behörighet till Åklagarmyndighetens system för diarieföring och handläggning av brottmål får enbart beslutas för, tilldelas till och innehas av den som inte samtidigt innehar behörighet eller åtkomst till annan myndighets motsvarande system för utredning av brottmål om det systemet kommunicerar med Åklagarmyndighetens system för diarieföring och handläggning av brottmål.

Första stycket gäller inte den som har anställning som registrator, administratör, it-samordnare, beslagshandläggare, arkivarie eller verksamhetsutvecklare vid Ekobrottsmyndigheten och som har samtidig tillgång till den begränsade version av Polismyndighetens Durtvå som används vid Ekobrottsmyndigheten.

**13 §** It-utrustning och it-system tillhörande åklagarväsendet syftar till att användas i samband med tjänsteutövning. Personal inom åklagarväsendet eller anställda vid externa tillsynsorgan som har att utöva tillsyn över verksamheten i åklagarväsendet 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 får medge undantag från vad som sägs i första stycket.

### **Säkerhet m.m.**

**14 §** I Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsknydd finns bestämmelser om behandling av säkerhetsknyddsklassificerade uppgifter och handlingar samt behandling av dessa i informationssystem och lagringsmedium.

**15 §** Endast programvaror som godkänts av Åklagarmyndigheten får användas i system som är anslutna till åklagarväsendets gemensamma it-infrastruktur. Endast it-utrustning som godkänts av Åklagar-

myndigheten får användas i system som är anslutna till åklagarväsendets gemensamma it-infrastruktur.

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

**16 §** Endast åklagarväsendets och andra RD-myndigheters godkända och säkerhetskontrollerade datamedia får användas i it-utrustning som ingår i eller är anslutna till åklagarväsendets gemensamma it-infrastruktur. Med RD-myndigheter avses de myndigheter som ingår i Rättsväsendets digitalisering enligt beslut av regeringen.

Annan datamedia får användas i it-utrustning som ingår i eller är anslutna till åklagarväsendets gemensamma it-infrastruktur endast efter särskild säkerhetskontroll. Detsamma gäller i de fall åklagarväsendets datamedia har använts i annans it-utrustning.

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

**17 §** Det är tillåtet att sammankoppla it-utrustning som ingår i åklagarväsendets gemensamma it-infrastruktur med annan myndighets projektor eller bildskärm och vice versa, under förutsättning att separat programvara inte installeras.

**18 §** It-säkerhetschefen beslutar vilka it-utrustningar och programvaror som är godkända och därmed får användas i system som är anslutna till åklagarväsendets gemensamma it-infrastruktur.

Utbyte av fast monterat datamedia får inte ske utan tillstånd av it-säkerhetschefen.

It-säkerhetschefen får medge undantag från vad som sägs i andra stycket.

**19 §** Externa uppkopplingar eller anslutningar till eller ifrån åklagarväsendets gemensamma it-infrastruktur får inte ske utan tillstånd av it-säkerhetschefen.

**20 §** It-säkerhetschefen ansvarar för att kontroll och uppföljning fortlöpande sker av it-säkerheten i åklagarväsendets gemensamma it-infrastruktur. It-säkerhetschefen ska också kontrollera att it-infrastrukturen endast används för fastställda ändamål.

**21 §** Personal inom åklagarväsendet som misstänker försök till dataintrång, förekomst av skadlig kod eller annat hot mot åklagarväsendets gemensamma it-infrastruktur, ska omgående rapportera detta till it-säkerhetschefen via Åklagarmyndighetens supportfunktion.

**22 §** Om it-säkerhetschefen bedömer att det kan föreligga ett hot mot it-säkerheten i den gemensamma it-infrastrukturen ska en fördjupad kontroll genomföras.

**23 §** It-säkerhetschefen får besluta om begränsningar i möjligheten att sända eller ta emot e-post som är av vissa format eller innehåller vissa typer av bilagor om det behövs för att säkerställa driften av e-postsystemet eller om det behövs för att upprätthålla en godtagbar nivå på it-säkerheten i åklagarväsendets gemensamma it-infrastruktur.

### **Övrigt**

**24 §** It-säkerhetschefen får helt eller delvis stoppa användning av utrustning, system eller behörighet, om det bedöms nödvändigt för att upprätthålla en godtagbar säkerhetsnivå i åklagarväsendets gemensamma it-infrastruktur. It-säkerhetschefen får även i övrigt fatta de beslut som behövs för att avhjälpa it-säkerhetsbrister.

Fattar it-säkerhetschefen ett sådant beslut såvitt avser allvarliga brister, ska denne utan dröjsmål underrätta riksåklagaren samt i tillämpliga fall även generaldirektören vid Ekobrottsmyndigheten.

---

Denna författning träder i kraft den 15 september 2023. Samtidigt upphör ÅFS 2014:7 att gälla.

PETRA LUNDH

Anders Thoursie  
(It-avdelningen)