Domstolsverkets författningssamling

ISSN 0347-5271
Ansvarig utgivare: Charlotte Driving

DOMSTOLSVERKET
SVERIGES DOMSTOLAR

DVFS 2021:1
Utkom från trycket
den 1 december 2021

Domstolsverkets föreskrifter om informationssäkerhet för gemensamma informationssystem

beslutade den 1 november 2021.

Domstolsverket föreskriver med stöd av 10 § förordningen (2007:1073) med instruktion för Domstolsverket följande.

Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om informationssäkerhet när det gäller informationssystem och enheter som direkt eller indirekt är anslutna till Sveriges Domstolars gemensamma nätverk Domnät.

Föreskrifterna gäller för de allmänna domstolarna, de allmänna förvaltningsdomstolarna, hyres- och arrendenämnderna, Rättshjälpsmyndigheten, Rättshjälpsnämnden och Domstolsverket, samt andra myndigheter som direkt eller indirekt är anslutna till Domnät enligt särskild överenskommelse.

Ledningssystem för informationssäkerhet

2 § Dessa föreskrifter kompletteras av Sveriges Domstolars ledningssystem för informationssäkerhet.

Definitioner

3 § I dessa föreskrifter avses med

Användare: Den som, genom anställning, uppdrag, praktik eller liknande vid en eller flera myndigheter inom Sveriges Domstolar, är berättigad åtkomst till informationssystem inom Sveriges Domstolar.

Centralt tillhandahållna informationssystem inom Sveriges Domstolar: Informationssystem, nätverk och infrastruktur som tillhandhålls och förvaltas centralt av Domstolsverket. Exempelvis Domnät, verksamhetsstöd, video- och telefonisystem och molntjänster.

Domnät: Sveriges Domstolars gemensamma nätverk som gör åtkomst möjlig till informationssystem inom Sveriges Domstolar och till internet.

E-identifiering och e-underskrift: Används för säker identifiering för åtkomst till informationssystem inom Sveriges Domstolar och för digital underskrift i vissa fall.

Enhet: Teknisk utrustning som används för åtkomst till informationssystem inom Sveriges Domstolar, t.ex. dator, mobil enhet och nätverksutrustning.

Information: Allt innehåll som behandlas digitalt och som rör en myndighets verksamhet.

Informationssystem inom Sveriges Domstolar: Applikationer, tjänster eller andra komponenter som hanterar information och som direkt eller indirekt är anslutna till Domnät. Ett informationssystem kan vara placerat vid Sveriges Domstolar eller hos en extern leverantör.

Informationssäkerhet: Bevarande av konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information.

Informationsägare: Den som har ägaransvaret för information som behandlas i ett eller flera informationssystem.

Molntjänst: Ett internetbaserat informationssystem som tillhandahåller datalagring, programkörning eller andra it-funktioner av extern leverantör.

Sveriges Domstolar: De allmänna domstolarna, de allmänna förvaltningsdomstolarna, hyres- och arrendenämnderna, Rättshjälpsmyndigheten, Rättshjälpsnämnden och Domstolsverket.

Systemägare: Den som har det övergripande ansvaret för ett informationssystem, nätverk eller infrastruktur, inkl. säkerhetsnivån i dessa system.

Säkerhetsskyddsklassificerade uppgifter: Uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), i den mening som avses i säkerhetsskyddslagen (2018:585).

Ansvarsfördelning

Domstolsverkets generaldirektör
4 § Domstolsverkets generaldirektör har det övergripande ansvaret för informationssäkerheten för centralt tillhandahållna informationssystem inom Sveriges Domstolar och är systemägare för dessa.

Myndighetschef
5 § Myndighetschefen vid respektive myndighet ansvarar för att informationssäkerheten upprätthålls vid myndigheten och ansvarar för att användarna vid respektive myndighet följer dessa föreskrifter.

Myndighetschefen är systemägare för egna informationssystem på myndigheten.

Myndighetschefen är informationsägare till myndighetens information.

6 § Myndighetschefen ansvarar för att Sveriges Domstolars ledningssystem för informationssäkerhet gällande e-identifiering och e-underskrift efterlevs.

Informationssäkerhetschef vid Domstolsverket
7 § Informationssäkerhetschefen har huvudansvar för det övergripande systematiska och riskbaserade informationssäkerhetsarbetet inom Sveriges Domstolar.

Användare
8 § Varje användare ansvarar för att informationssäkerheten upprätthålls genom att följa dessa föreskrifter.

Åtkomst, utbildning och ansvarsförbindelse

Åtkomst
9 § Endast den som har anställning, uppdrag, praktik eller liknande vid en eller flera myndigheter inom Sveriges Domstolar får ges åtkomst till Domnät och informationssystem inom Sveriges Domstolar.

10 § Myndighetschefen eller den myndighetschefen har delegerat uppgiften till ansvarar för att en användare endast har den åtkomst till informationssystem som användaren behöver för att kunna fullgöra sina arbetsuppgifter.

Utbildning
11 § Varje myndighet ska utbilda och informera samtliga användare om dessa föreskrifter, samt se till att de genomgår Domstolsverkets e-utbildning i informationssäkerhet i samband med att anställning, uppdrag, praktik eller liknande påbörjas och därefter årligen.

Ansvarsförbindelse
12 § Varje myndighet ska se till att samtliga nya användare undertecknar ansvarsförbindelse för användare av informationssystem inom Sveriges Domstolar efter genomgången e-utbildning.

Användarkrav

Användarens ansvar vid användning av enheter och informationssystem inom Sveriges Domstolar
13 § Endast enheter som är godkända av Domstolsverket får användas för åtkomst till Domnät och informationssystem inom Sveriges Domstolar.

14 § Endast programvaror som är godkända av Domstolsverket får laddas ned och installeras på enheter och i informationssystem inom Sveriges Domstolar.

15 § Endast molntjänster som är godkända av Domstolsverket får användas för hantering av information.

Generella användarkrav
16 § Inloggningsuppgifter och behörigheter är personliga och ska inte lånas ut eller på annat sätt göras åtkomliga för andra.

17 § Informationssystem och enheter är avsedda att användas i tjänsten. Privat användning av t.ex. Officepaketet, internet och e-post är tillåten i begränsad omfattning.

18 § En användare får inte stänga av, manipulera eller på annat sätt kringgå IT-säkerhetstjänster som finns på enheter och i informationssystemen. IT-säkerhetstjänster är t.ex. antivirusprogram, webbfilter och e-postfilter.

19 § Kontroll mot skadlig kod ska alltid göras i samband med att en enhet tar emot elektroniska filer från externa lagringsmedier, till exempel USB-minne eller externa lagringstjänster.

20 § En användare som upptäcker incidenter, fel eller brister som kan ha betydelse för informationssäkerheten inom Sveriges Domstolar, ska anmäla detta till närmaste chef vid myndigheten för vidare hantering.

Hantering av information
21 § Vid hantering av information via e-post ska de e-post-tjänster som Domstolsverket anvisar användas.

22 § En användare ska hantera känslig information på ett sådant sätt att risken för att obehöriga får del av den minimeras.

23 § Säkerhetsskyddsklassificerade uppgifter ska inte hanteras i informationssystem eller enheter som direkt eller indirekt är anslutna till Domnät, utan ska hanteras separat och i särskild ordning.

Hantering av enheter
24 § En användare ska hantera en enhet på ett sätt som minimerar risken för att obehöriga får tillgång till den. Om en användare lämnar en enhet utan uppsikt ska den vara låst.

25 § Vid förlust av en enhet ska detta snarast anmälas till driftsansvarig eller motsvarande funktion för vidare hantering och åtgärd.

Särskilt om mobilt arbete
26 § Vid mobilt arbete ska användaren se till att ingen obehörig kan ta del av information som visas på skärmen eller spelas upp från enheten.

27 § Det är inte tillåtet att använda lokal eller central administratörsbehörighet vid användande av Vera via fjärråtkomst. Lokal eller central administratörsbehörighet får endast användas i Sveriges Domstolars lokaler.

Kontrollåtgärder

28 § Vid misstanke om användning av informationssystem inom Sveriges Domstolar i strid med dessa föreskrifter ska ansvarig myndighetschef kontrollera användandet.

I förebyggande syfte har Domstolsverkets informationssäkerhetschef och myndighetscheferna inom Sveriges Domstolar rätt att kontrollera att dessa föreskrifter följs. Kontroll kan ske såväl av enskilda användare som generellt. Kontroll sker med hjälp av loggning eller andra tekniska verktyg.

---

1. Dessa föreskrifter träder i kraft den 1 januari 2022.

2. Genom dessa föreskrifter upphävs Domstolsverkets föreskrifter (DVFS 2015:5) om informationssäkerhet för gemensamma IT-system.

DOMSTOLSVERKET

Thomas Rolén

Marita Stjernmira