Domstolsverkets författningssamling

ISSN 0347-5271
Ansvarig utgivare: Anna Hjort Ööpik

DOMSTOLSVERKET
SVERIGES DOMSTOLAR

DVFS 2015:5
Utkom från trycket
den 25 november 2015

Domstolsverkets föreskrifter om informationssäkerhet för gemensamma IT-system

beslutade den 15 oktober 2015

Domstolsverket meddelar med stöd av 10 § förordning (2007:1073) med instruktion för Domstolsverket följande föreskrifter om informationssäkerhet för gemensamma IT-system.

Tillämpningsområde

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

Ledningssystem för informationssäkerhet

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

Definitioner

3 § I dessa föreskrifter avses med

Myndighet: En myndighet inom Sveriges Domstolar.

Systemägare: Den som har det överordnade ansvaret för administration och drift av ett IT-system. Domstolsverkets generaldirektör är systemägare för centralt tillhandahållna IT-system inom Sveriges Domstolar. I de fall en myndighet har egna IT-system anslutna till Domnät är respektive myndig-

hetschef systemägare. Systemägaransvaret kan delegeras till annan vid myndigheten.

Användare: En person som, genom anställning, uppdrag, praktik eller liknande vid en eller flera myndigheter inom Sveriges Domstolar, är berättigad åtkomst till nätverket Domnät och dess IT-system.

Domnät: Sveriges Domstolars gemensamma nätverk för datakommunikation som gör nätverksåtkomst möjlig till t.ex. gemensamma verksamhetsstöd och internet.

IT-system: Teknisk utrustning som, oavsett om den är införskaffad av en myndighet eller tillhandahålls av en extern leverantör, är ansluten till nätverket Domnät och som används t.ex. för att lagra och behandla information centralt.

Enhet: Teknisk utrustning som är ansluten till nätverket Domnät, t.ex. PC-dator, mobiltelefon och nätverksutrustning.

Information: Allt innehåll som finns på elektroniska lagringsmedier och som rör en myndighets verksamhet.

Känslig information: Sådan verksamhetsinformation som, om obehörig kan ta del av, förändra eller radera den, kan innebära risk för skada för en enskild eller en myndighet. Känslig information är t.ex. information i ett verksamhetsregister som direkt visar att en enskild förekommer i registret, information som är sekretessbelagd och information om en enskilds eller en myndighets ekonomiska förhållanden.

Molntjänst: Ett IT-system för att lagra och upprätthålla verksamhetsinformation tillhandahållen och placerad hos en tredjepartsleverantör. Verksamhetsinformationen görs tillgänglig via internet.

Åtkomst: Möjlighet för en användare att få tillgång till nätverket Domnät, IT-system eller enheter.

Ansvarsfördelning

Domstolsverkets generaldirektör

4 § Domstolsverkets generaldirektör har det övergripande ansvaret för informationssäkerheten inom Sveriges Domstolar.

Myndighetschefen

5 § Myndighetschefen vid respektive myndighet ansvarar för att informationssäkerheten upprätthålls vid myndigheten bl.a. genom att se till att dessa föreskrifter följs.

Informationssäkerhetschefen vid Domstolsverket

6 § Informationssäkerhetschefen ansvarar för att ett systematiskt informationssäkerhetsarbete bedrivs inom Sveriges Domstolar.

Systemägare

7 § En systemägare av ett IT-system har det övergripande ansvaret för informationssäkerheten inom IT-systemet.

Användare

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

Åtkomst till och hantering av nätverket Domnät, IT-system och enheter

Åtkomst

9 § Endast den som har anställning, uppdrag, praktik eller liknande vid en eller flera myndigheter inom Sveriges Domstolar får medges åtkomst till nätverket Domnät och till nätet direkt eller indirekt anslutna IT-system och enheter.

10 § Myndighetschefen eller den myndighetschefen har delegerat uppgiften till ansvarar för att användaren endast har den åtkomst till IT-system som användaren behöver för att kunna fullgöra sina arbetsuppgifter.

Generella användarkrav

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

12 § En användare ska hantera lösenordsuppgifter så att de inte blir kända för andra. Om så ändå skulle ske ska användaren utan dröjsmål ändra lösenordet.

13 § Vid hantering av arbetsrelaterad e-post ska de e-posttjänster som Domstolsverket har anvisat användas. Andra e-posttjänster får endast användas om tillgången till de anvisade e-posttjänsterna saknas och det i övrigt bedöms lämpligt.

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

15 § En användare som upptäcker incidenter, fel eller brister, som kan ha betydelse för informationssäkerheten inom Sveriges Domstolar, ska anmäla detta till drifts- eller teknikansvarig vid myndigheten. Anmälan ska därefter vidarebefordras till informationssäkerhetschefen vid Domstolsverket.

Utbildning

16 § Varje myndighet ska utbilda och informera användare om dessa föreskrifter i samband med att arbetet påbörjas. Varje myndighet ska se till att samtliga användare undertecknar ansvarsförbindelse för datoranvändare vid Sveriges Domstolar och genomgår Domstolsverkets e-utbildning inom informationssäkerhet.

Hantering av IT-system och enheter

Hantering av enheter

17 § En användare ska hantera en enhet på ett sätt som minimerar risken för att obehöriga får tillgång till den, t.ex. att den stjäls eller går förlorad.

Om en användare lämnar en enhet ska åtkomsten begränsas genom låsning.

18 § Vid förlust av enhet, t.ex. PC-dator eller mobiltelefon, ska detta snarast anmälas till Domstolsverkets support.

19 § En användare som är uppkopplad utanför Domnät (vid fjärråtkomst) ska se till att ingen obehörig kan ta del av känslig information som visas på skärmen eller spelas upp från enheten.

20 § 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.

Användning av programvaror och IT-system m.m.

21 § En användare ansvarar för att de programvaror som användaren laddar ned och installerar i IT-system och enheter är godkända av Domstolsverket.

22 § En användare ansvarar för att den utrustning som användaren ansluter till nätverket Domnät är godkänd av Domstolsverket.

23 § En användare får inte stänga av, manipulera eller på annat sätt kringgå IT-säkerhetstjänster i IT-system och enheter som direkt eller indirekt är anslutna till nätverket Domnät. IT-säkerhetstjänster är t.ex. antivirusprogram, webbfilter och e-postfilter.

24 § I samband med att en enhet tar emot externa elektroniska filer, t.ex. via USB-minne eller extern lagringstjänst, ska en användare alltid utföra kontroll mot skadlig kod, t.ex. datorvirus.

Ansvar för säkerhetsåtgärder

25 § Varje myndighet ansvarar för att IT-system som ska användas inom Sveriges Domstolar genomgår en riskanalys för att identifiera behov av säkerhetsåtgärder. Sveriges Domstolars ledningssystem för informationssäkerhet (LIS) ska ligga till grund vid val av säkerhetsåtgärder.

26 § Varje myndighet ansvarar för att enheter som ska användas för att lagra och behandla känslig information, är krypterade på det sätt som Domstolsverket anvisat.

27 § Varje myndighet ansvarar för att externa molntjänster som innehåller myndighetsinformation är godkända av Domstolsverket.

Kontrollåtgärder

28 § Vid misstanke om användning av gemensamma IT-system 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.

Dessa föreskrifter träder i kraft den 1 januari 2016. Genom föreskrifterna upphävs Domstolsverkets föreskrifter (DVFS 2012:1) om informationssäkerhet för gemensamma IT-system.

DOMSTOLSVERKET

Martin Holmgren

Håkan Sonesson