Stockholms dramatiska högskola
Box 27095
102 51 Stockholm

Datum 2012-01-27
Dnr 32-2011-0247

Informationssäkerhet vid Stockholms dramatiska högskola 2011

Riksrevisionen har som ett led i den årliga revisionen av Stockholms dramatiska högskola (StDH) 2011, granskat den interna styrningen och kontrollen i informationssäkerheten vid högskolan.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa styrelsen vid StDH uppmärksamhet på i denna revisionsrapport.

Riksrevisionen önskar information senast 2012-03-02 med anledning av våra iakttagelser i denna rapport.

Iakttagelser och rekommendationer

Det ökande elektroniska informationsutbytet i samhället ställer krav på att myndigheterna i sitt arbete med att upprätthålla säkerhet i sin informationshantering tillämpar ett ledningssystem för informationssäkerhet (LIS). Begreppet informationssäkerhet är ett vidare begrepp än IT-säkerhet och fokuserar på informationens säkerhet snarare än IT-systemens säkerhet. Myndigheternas arbete med informationssäkerhet och deras tillämpning av standarder i sådant arbete, framgår närmast av Myndigheten för samhällskydd och beredskaps (MSB) föreskrifter och allmänna råd (MSBFS 2009:10).

En myndighets arbete med att upprätthålla säkerhet i sin informationshantering och tillämpa ett ledningssystem för informationssäkerhet (4 § MSB:s föreskrifter) innebär att:

1. Upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet.
2. Utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet.
3. Klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet,
4. Utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt besluta om åtgärder för myndighetens informationssäkerhet,
5. Dokumentera granskningar och säkerhetsåtgärder av större betydelse som har vidtagits.

Myndighetens ledning ska även löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på myndigheten (5§ MSB:s föreskrifter).
Vidare ska en myndighets arbete med informationssäkerhet bedrivas i former enligt etablerade svenska standarder (6 § MSB:s föreskrifter).

Vid Riksrevisionens granskning framkom att StDH i sin informationshantering inte tillämpar ett ledningssystem för informationssäkerhet, på det sätt som framgår av MSB:s föreskrifter och allmänna råd.
Vid granskningen noterades bl.a. att StDH

- saknade en informationssäkerhetspolicy och andra styrande dokument för myndighetens informationssäkerhet. Vid högskolan finns interna riktlinjer för användning av högskolans It-resurser, en It-manual samt för hantering av handlingar på StDH.
- inte hade utsett en eller flera personer som har ansvar för att leda och samordna arbetet för informationssäkerheten.
- inte har upprättat risk- och sårbarhetsanalyser för att avgöra hur risker ska hanteras, samt beslutat om åtgärder för högskolans informationssäkerhet.

Vid granskningen har Riksrevisionen inte noterat några incidenter föranledda av att StDH inte tillämpar ett ledningssystem för informationssäkerhet.

StDH har efter granskningen inlett ett arbete med att införa ett ledningssystem för informationssäkerhet och har numera utarbetat ett utkast till informationssäkerhetspolicy samt utsett en ansvarig person för informationssäkerheten vid högskolan.

Information är en av de viktigaste tillgångarna vid StDH, t.ex. i studiedokumentationssystemet. Informationssäkerhet är även en viktig del i skyddet av den personliga integriteten för anställda och studenter vid StDH. Oavsett vilken form informationen har och på vilket sätt den överförs eller lagras, måste den alltid ha godtagbart skydd. Brister i informationssäkerheten medför att tillförlitligheten i myndighetens interna kontroll försvagas och att det finns risker för informationens riktighet, sekretess, tillgänglighet och spårbarhet.

Av 2 kap. 2 § i högskoleförordningen framgår att det är styrelsens ansvar att säkerställa att det vid högskolan finns en intern styrning och kontroll som fungerar på ett betryggande sätt. För att en god intern styrning och kontroll ska anses föreligga vid en myndighet förutsätts bl.a. en god informationssäkerhet.

Riksrevisionen *rekommenderar* att Stockholms dramatiska högskola inför ett ledningssystem för informationssäkerhet vid högskolan i enlighet med MSB:s föreskrifter och allmänna råd.

Ansvarig revisor Claes Backman har beslutat i detta ärende. Uppdragsledare Britt Huldén Ljusnemo har varit föredragande.

Claes Backman

Britt Huldén Ljusnemo

Kopia för kännedom:
Regeringen