



Vår referens: Karolina Arneson

**KANSLIBESLUT**

Diariernr: 10-576/09

Beteckning: ITincid

Beslutsdatum: 2009-05-07

**Beslutsinstans:**

Förvaltningen

**Beslut fattat av:**

Marianne Wiktorin,  
förvaltningschef

**Föredragande:**

Mona Åkerman, IT-chef

**Övriga närvarande:**

**Delges för åtgärd:**

II-avdelningen,  
Förvaltningsråd,  
Ledningsgrupp

**Delges för kännedom:**

---

**Ärende:**

*Riktlinjer för hantering av allvarliga IT-incidenter*

Vid ledningsgruppens möte 2009-02-27 aktualiserades behovet av riktlinjer för hantering av allvarliga IT-incidenter. Bifogade riktlinjer har utarbetats av Maivor Halén, bibliotekschef, Mona Åkerman, IT-chef och Marianne Wiktorin, förvaltningschef.

**Beslut:**

Bifogade riktlinjer antas och gäller fr o m beslutsdatum.

Marianne Wiktorin

## Riktlinjer för hantering av allvarliga IT-incidenter

Högskolan har antagit en policy för elektronisk informationssäkerhet som syftar till att tillförsäkra riktighet, tillgänglighet, sekretess och spårbarhet i elektronisk information. Det operativa och samordnande ansvaret för den elektroniska informationssäkerheten har IT-chefen, som utsetts till informationssäkerhetschef. Ansvaret i övrigt följer Högskolans delegationsordning och det övergripande ansvaret har rektor och högskolestyrelse (Dnr 10-818/08, kanslibeslut RÄ:27).

Nedanstående riktlinjer tydliggör rutiner som syftar till att motverka verksamhetsstörningar vid allvarliga IT-incidenter.

### Vid en allvarlig IT-incident skall följande snarast utföras:

1. Sätt stopp för händelsen snarast och minimera skadan
2. Larma ansvariga om incidenten
3. Sprida information till alla berörda
4. Dokumentera vad som sker
5. Samla in konsekvensanalyser
6. Förebyggande åtgärder för att incidenten inte skall upprepas
7. Återrapportera till verksamheten och ledningen

### 1. Sätt stopp för händelsen snarast och minimera skadan

IT-chefen ansvarar för att IT-personalen agerar skyndsamt vid inträffade IT-incidenter för att avhjälpa eller lindra effekterna av det inträffade.

De nyckelpersoner inom IT-personalen som kan avhjälpa problemet och minimera skadan skall snarast inkallas.

### 2. Larma ansvariga om incidenten

IT-chefen ansvarar för att sprida korrekt, aktuell information och samordna nödvändiga åtgärder. Så snart en allvarlig IT-incident inträffar skall en kort och enkel rapport skickas till rektor, chefsgrupp samt IT-ansvariga på institutioner och avdelningar (nedan kallas dessa samlat för nyckelgrupper). Informationen sänds i första hand per SMS, alternativt per telefon eller genom direkt kontakt.

### 3. Sprida information till alla berörda

Ovan nämnda nyckelgrupper har ansvaret för att informationen om incidenten skyndsamt vidare sprids i den egna organisationen och till externt berörda. Informationen sänds i särskild ordning via tillgängliga kanaler, i första hand per SMS, e-post, telefon, fax och intern-TV.

#### **4. Dokumentera vad som sker**

IT-incidenter kan ofta avhjälpas av IT-avdelningen. De bör dock alltid dokumenteras, för att man skall kunna analysera vad som hänt och förebygga att det händer igen. IT-chefen har ett ansvar för denna dokumentation, som skall inkludera hur problemet upptäcktes och alla vidtagna åtgärder i kronologisk ordning.

Följande frågor skall besvaras i rapporten: VAD, VAR, NÄR, VEM, HUR och VARFÖR.

#### **5. Samla in konsekvensanalyser**

Ovan nämnda nyckelgrupper ansvarar för att konsekvensanalyser, som beskriver vilka störningar som IT-incidenten orsakat, sammanställas vid berörda institutioner och avdelningar. Dessa sänds till IT-chef och förvaltningschef och användas som underlag i arbetet med att följa upp och utreda det inträffade.

#### **6. Förebyggande åtgärder för att incidenten inte skall upprepas**

För att undvika och hantera IT-incidenter är det viktigt med förebyggande åtgärder och att dra nytta av kunskapen från tidigare incidenter. Efter varje IT-incident bör berörda dokument, t ex systemförvaltningsplaner för IT-system, gås igenom och vid behov justeras av ansvariga.

#### **7. Återrapportera till verksamheten och ledningen**

När hela händelsen är dokumenterad från start till slut, skall en analys göras över förloppet. Återrapportering skall göras till rektor, chefsgrupp samt IT-ansvariga på institutioner och avdelningar. I återrapporteringen bör ett förslag ingå, som specificerar nödvändiga åtgärder och om möjligt uppskattade kostnader för dessa. Information om rapporten görs tillgänglig för all personal via intranätet.