



UPPSALA  
UNIVERSITET

Box 256  
SE-751 05 Uppsala

Besöksadress:  
S:t Olofsgatan 10 B

Handläggare:  
Veronika Berglund

Telefon:  
018-471 78 62

Telefax:  
018-471 17 08

[www.uu.se](http://www.uu.se)

[veronika.berglund@uadm.uu.se](mailto:veronika.berglund@uadm.uu.se)

Beredning med:  
Gunilla Liljeroth, Internrevisionschef  
Camilla Löw Lundin, bitr.  
akademiombudsman vid Juridiska  
avdelningen  
Magnus Hallberg, Universitetsjurist  
vid Juridiska avdelningen  
Christina Boman, Säkerhetschef  
Anna Clemensson,  
avdelningsdirektör vid  
Planeringsavdelningen  
Björn Gembert, bitr. kanslichef vid  
Kansliet för naturvetenskap och  
teknik  
Michael Thuné, Prefekt vid  
Institutionen för  
Informationsteknologi  
Mats Daniels, Studierektor vid  
Institutionen för  
Informationsteknologi

REMISSVAR

2015-09-08 UFV 2015/702

Justitiedepartementet

## **SOU 2015:23 Informations- och cybersäkerhet i Sverige Strategier och åtgärder för säker information i staten**

Uppsala universitet har anmodats lämna synpunkter på betänkandet "Informations- och cybersäkerhet i Sverige", SOU 215:23. Betänkandet innehåller dels ett förslag till ny förordning för statliga myndigheters informationssäkerhet, dels strategier för statens informationssäkerhet.

### **Sammanfattning**

Uppsala universitet tillstyrker betänkandets förslag till ny förordning samt följdändringar i andra lagrum, och bifaller i stort betänkandets förslag gällande strategier för statens informationssäkerhet; som inrättandet av ett myndighetsråd, samordning över den statliga sektorns informationssäkerhet, obligatorisk it-incidentrapportering, en nationell styrmodell för informationssäkerhet och säkrare kommunikation i staten.

### **Kommentarer och ändringsförslag**

#### **1. Författningsförslag (sid 27 ff)**

Uppsala universitet tillstyrker betänkandets förslag till ny förordning för statliga myndigheters informationssäkerhet i sin helhet. En sammanhållen och väl specificerad lagstiftning för informationssäkerhetsområdet underlättar på flera sätt universitetets interna arbete med informationssäkerhet.

Förslaget till ändring i säkerhetsskyddsförordningen ser universitetet som en logiskt följd av det utökade myndighetsansvaret gällande inrapportering av it-incidenter.

#### **9.2.1 En nationell styrmodell (sidan 211 ff)**

Uppsala universitet bifaller förslaget att skapa en samlad modell med gemensamma metoder, stöd, terminologi och regelverk och ser det som naturligt att MSB fortsätter sitt tidigare arbete inom området.

Eftersom styrmodellen ska baseras på både existerande krav i författningar och verksamheternas behov, vore det önskvärt med ytterligare information om hur sammanställningen av dessa

behov är tänkt att genomföras, samt om det är den befintliga modellen enligt förordningen om intern styrning och kontroll som avses med existerande krav.

### **9.2.5 Informationssäkerhet som en del av myndighetens revision (sid 230 ff)**

Uppsala universitet vill påpeka att internrevisionen redan omfattar hela verksamheten enligt internrevisionsförordningen, och det finns därför ingen anledning att föreslå att internrevisionens uppdrag ska utökas till att omfatta ”även informationssäkerhetsfrågorna”.

Vad gäller avsnittet *Förvaltningsmyndigheter under regeringen* (sid 235) så rekommenderar Uppsala universitet alternativ två, att en bestämmelse införs om att myndighetens ledning ansvarar för att upprätthålla säkerhet i sin informationshantering. Alternativt kan det redan existerande intygandet från ledningen avseende statusen på den interna kontrollen i myndigheten förtydligas på den här punkten.

Alternativ ett bedömer universitetet som mindre lämpligt med tanke på med nuvarande internrevisionsförordning och bemannings-/penningmässiga resurser för de flesta internrevisionsavdelningar i förvaltningsmyndigheter under regeringen. Att ålägga internrevisionen att årligen uttala sig om statusen på informationssäkerheten resulterar troligen i ett intygande med reservation varje år. Den riskbaserade ansats som ligger till grund för internrevisionen innebär att det inte nödvändigtvis innebär att informationssäkerheten granskas varje år. Ska så ske behövs betydligt utökade resurser. Dessutom skulle internrevisionsförordningen behöva kompletteras med en notering om att ett sådant årligt intygande ska lämnas. Internrevisionen i Sverige lämnar för närvarande inga intyg av den typen.

### **9.3.1 Kravställning vid upphandling (sid 236 ff)**

Förslag nummer 3, att myndigheter ska rapportera in vilken leverantör som valts vid användning av ramavtal, har en oklar praktisk verkan. Tanken att minska risken för stora störningar på samhället genom att minska koncentrationen av leverantörer av it-system är god, men hur ska den appliceras i praktiken? Att enbart rapportera in vilken leverantör som valts minskar i sig inte risken. Om ett antal myndigheter valt samma leverantör från ett ramavtal, ska det då finnas en maxgräns så att andra myndigheter inte längre har möjlighet att välja den leverantören, även om det är den som bäst uppfyller myndighetens krav? Universitetet konstaterar i övrigt att de ökade kraven på högre beställarkompetens vid upphandling troligen medför ett behov

både av viss kompetensutveckling bland upphandlarna och ett tätare samarbete internt på myndigheterna mellan de som ansvarar för upphandling och de som, enligt förordningen, ska leda och samordna arbetet med informationssäkerhet.

#### **9.4 Säkrare kommunikation i staten (sid 246 ff)**

Uppsala universitet bifaller förslaget samtliga tre delar för säkrare kommunikation i staten, d.v.s. anslutning till SGSI för relevanta myndigheter, utvecklandet av sensorteknik samt synkroniserad tidsskala i it-system.

#### **9.5.2 Obligatorisk it-incidentrapportering (sid 258 ff)**

Uppsala universitet kan se nyttoeffekter av en obligatorisk it-incidentrapportering till MSB.

Det är viktigt att det i det kommande regelverket tydligt framgår vad som räknas som en it-incident, hur rapportering ska ske, hur bedömningen av allvarlighetsgrader på it-incidenter ska göras och av vem (MSB eller myndigheten), hur inrapporterad information kommer att hanteras. Det vore också önskvärt med möjlighet till sekretessmarkering av känslig information.

En ytterligare fråga är i vilken fas av en it-incident som rapportering till MSB ska ske - direkt när incidenten identifierats som allvarlig, under arbetet med en pågående incident, eller efter avslutad incident.

Förslaget innebär för den enskilda myndigheten ett stort internt behov av tydliga regler och rutiner, liksom en förutbestämd ansvarsfördelning i händelse av en it-incident. Extra viktigt är detta vid stora myndigheter, speciellt universitet och högskolor där mycket av ansvaret ofta är delegerat från generaldirektör/motsvarande till chefer på olika områden.

#### **9.6.3 Översynen av bestämmelser om tvångsmedel i den digitala miljön**

Vad gäller den föreslagna översynen för att säkerställa förebyggande och utredande verksamhet i den digitala miljön anser Uppsala universitet det vara ett lovligt initiativ att göra en genomgripande och detaljerad analys över förutsättningar och möjligheter. Det är i sammanhanget viktigt att bland annat beakta medborgarnas personliga integritet, behovet av samarbeten över landsgränser och riskerna med infrastrukturella störningar, till exempel vid husrannsakan hos outsourcingföretag eller molntjänstföretag där hårdvara tas i beslag som kan tänkas betjäna fler än det kundföretag som husrannsakan gäller.



### **9.7 Internationella och regionala relationer (sid 266 ff)**

Uppsala universitet ser det som viktigt att betänkandets förslag om samordning och konsistens i ”samtliga internationella och regionala fora av relevans” inte gäller utbildning och forskning vad gäller universitet och högskolors vidkommande, och att det tydligt framgår att så är fallet.

Uppsala universitet är ett brett forskningsuniversitet med stark internationell ställning och uppgift att bedriva forskning och utbildning av högsta kvalitet och att på olika sätt samverka med samhället. Framgångsrik samverkan bygger på förtroende för universitetet som en oberoende och opartisk kunskapsorganisation och sker med utgångspunkt i universitetets vetenskapliga integritet.

### **9.8.1 Framtida övningsutveckling inom informations- och cybersäkerhetsområdet (sid 271 ff)**

Uppsala universitet ser utvecklingen av övningar inom området som positivt, med en förhoppning om att universitetet ges möjlighet att delta på övningar eller ta del av övningsmaterialet. Både simuleringsövningar och tekniska cybersäkerhetsövningar har nyttoaspekter för myndigheten som sådan likväl som för en del av universitetets utbildning och forskning.

### **9.8.2 Fördjupad dialog om kompetensförsörjning (sid 273 ff)**

Universitetet välkomnar en fördjupad dialog rörande kompetensutveckling, utbildning och forskning inom informationssäkerhetsområdet. Att kontinuerligt förnya kurs- och programutbud efter bland annat studenters efterfrågan och samhällets behov är en viktig del av universitetets mål och strategier. Vid diskussioner om forskningsbehov, resursbehov och kompetensuppbyggnad i de högre utbildningarna är det av största vikt att akademien involveras och att direktiven inte är alltför begränsande.

Beslut i detta ärende har fattats av undertecknad rektor i närvaro av ställföreträdande universitetsdirektören Per Abrahamsson, efter föredragning av bitr. säkerhetschefen Veronika Berglund. Närvarande därutöver var Uppsala studentkårs ordföranden Caisa Lycken.



Eva Åkesson



Veronika Berglund