

Reviderad Informationssäkerhetspolicy

Bakgrund

I enlighet med de av Högskolestyrelsen beslutade IT-riktlinjerna (junisammanträdet 2005) tog en arbetsgrupp under hösten 2005 fram ett förslag till ett övergripande policydokument. Förslaget förankrades inom Högskolan och beslutades därefter av rektor att gälla. Informationssäkerhetspolicyn avser tiden fram till 2008-12-31. Det är nu dags att säkerställa en gällande policy för tiden 2009-2011.

IT- och campuschefen har därför med stöd av några medarbetare reviderat policyn. Några få marginella anpassningar har införts. IT-strategigruppen har ställt sig bakom revisionen.

Beslut

Efter föredragning av IT- och campuschefen, Lars Nord, beslutar jag härmed att den reviderade informationssäkerhetspolicyn ska gälla för tiden 2009-2011.



Leif Larsson

Sändlista: Chefsgruppen, FUN, LUN, Informationsavdelningen, SACO, ST, Studentkåren

Informationssäkerhetspolicy för Högskolan i Skövde

Innehåll

| | |
|---|----------|
| Informationssäkerhetspolicy för Högskolan i Skövde | 3 |
| 1. Definition och avgränsning | 3 |
| 2. Syfte | 3 |
| 3. Tillhörande dokument | 3 |
| 4. Mål | 3 |
| 5. Ansvar | 4 |
| 5.1 Övergripande ansvar | 4 |
| 5.2 Institutionens och avdelningens ansvar | 4 |
| 5.3 Användarnas ansvar | 4 |
| 6. Information och utbildning | 4 |
| 7. Utveckling och upphandling | 5 |
| 8. Extern drift och tjänst | 5 |
| 9. Extern användning av Högskolans IT-resurser | 5 |
| 10. Genomförande | 5 |
| 11. Regelbrott och påföljder | 5 |
| 12. Informationssäkerhetspolicyns giltighet | 5 |

Utgåvehistorik för dokumentet

| Utgåva | Datum | Kommentar |
|--------|------------|--|
| P1.0-1 | 2005-12-12 | Första remissutgåva |
| P1.0-2 | 2005-12-19 | Punkt 4, 5.2 samt 10 justerade |
| 1.0 | 2006-01-30 | Punkt 5.1 kompletterad |
| 1.1 | 2008-11-11 | Inledning justerad samt punkt 12 |
| 1.2 | 2008-11-12 | Remiss till IT-strategigruppen |
| 1.3 | 2008-11-21 | IT-strategigruppen ställer sig bakom förslaget |
| 2.0 | 2008-12-04 | Beslutad av rektor |

Informationssäkerhetspolicy för Högskolan i Skövde

Under hösten 2005 tog en arbetsgrupp fram ett förslag till informationssäkerhetspolicy för tiden 2005-2008. Förslaget förankrades inom Högskolan och beslutades av rektor att gälla. Detta dokument har nu reviderats och ska gälla fram till 2011-12-31.

Informationssäkerhetspolicyen utgör ett komplement till Högskolans IT-strategi som anger inriktningen för den totala informationsbehandlingen.

Övriga styrande dokument är Vervas föreskrift (VERVAFS 2007:2) om statliga myndigheters arbete med elektroniskt informationsutbyte. I denna föreskrift sägs att myndigheten skall bedriva sitt säkerhetsarbete enl. följande etablerade svenska standarder

- Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001: 2006)
- Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005)

1. Definition och avgränsning

Denna policy avser säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet, tillgänglighet samt spårbarhet. Informationssäkerhet innefattar såväl IT-säkerhet som säkerhet i administrativa rutiner. Det bör noteras att policyen inte har någonting med informationsinnehållet att göra utan hanterar endast skydd av informationen.

2. Syfte

Informationssäkerheten på Högskolan ska skydda informationstillgångarna, så att störningar i IT-system inte orsakar omfattande skada eller kostnader för Högskolan, anställda, studerande och andra berörda.

3. Tillhörande dokument

Som ett komplement till den övergripande informationssäkerhetspolicyen och riktlinjerna kommer dokument att finnas i form av anvisningar och instruktioner på en mer detaljerad nivå för vissa specifika områden. Dessa dokument beskriver tillsammans alla säkerhetsåtgärder som syftar till att förebygga och minimera oönskade konsekvenser av olika händelser inom IT-området.

4. Mål

Informationssäkerhet vid Högskolan ska säkerställa att information som överförs, lagras eller behandlas i IT-system, skyddas mot

- obehörig eller otillåten åtkomst eller kopiering.
- oavsiktlig, obehörig eller otillåten förändring eller förstöring

Informationssäkerheten vid Högskolan ska också säkerställa att IT-system skyddas mot

- intrång och otillåten användning
- stöld eller skadegörelse
- funktionsstörning.

Dessutom ska informationssäkerhetsarbetet på Högskolan säkerställa arbetsrutiner avseende informationssäkerhet för anställda och studenter genom att tillgodose utbildning och information så att informationssäkerhet kan uppnås.

Säkerhetsnivåer och skyddsåtgärder för informationssäkerheten vid Högskolan ska utformas så, att målen för informationssäkerheten uppnås till rimliga kostnader, och utan att den dagliga verksamheten försvåras mer än nödvändigt.

Val och utformning av säkerhetsnivåer och skyddsåtgärder ska grunda sig på aktuell eller förväntad hotbild, och på konsekvenserna av störningar för Högskolan eller för anställda, studerande och allmänheten.

Hänsyn ska tas till såväl direkta som indirekta konsekvenser. Bedömningar av hotbild och konsekvenser av störningar ska göras regelbundet och systematiskt.

5. Ansvar

5.1 Övergripande ansvar

Högskolestyrelsen och rektor är ytterst ansvariga för Högskolans informationssäkerhet. För centrala och gemensamma system ska särskild systemägare utses av rektor eller den rektor utser. Systemägaren ansvarar för informationssäkerheten i respektive system eller resurs.

5.2 Institutionens och avdelningens ansvar

Prefekt, avdelningsschef eller motsvarande har ansvaret för informationssäkerheten vid respektive institution och avdelning.

Central IT-organisation utgör ett kompetenscentrum i informationssäkerhetsfrågor och ska ge råd och stöd till institutioner och avdelningar i deras säkerhetsarbete.

5.3 Användarnas ansvar

Alla användare ska underteckna särskild ansvarsförbindelse som tydliggör deras ansvar. Anställda och studenter ansvarar för säkerheten i sitt användande av Högskolans IT-system och att gällande policy och riktlinjer för informationssäkerhet tillämpas.

6. Information och utbildning

Kunskaper och säkerhetsmedvetande är helt avgörande för informationssäkerheten. Information och utbildning inom säkerhetsområdet ska ske fortlöpande och vid all nyanställning.

7. Utveckling och upphandling

Vid utveckling och upphandling av IT-system och tjänster ska alltid säkerhetsaspekten utredas och beaktas. Krav på informationssäkerhet ska dokumenteras och vara en del av kravspecifikationen och avtalet där det är tillämpligt.

8. Extern drift och tjänst

Om en annan part utför tjänst eller uppdrag åt högskolan där IT-tjänster eller IT-system utgör en viktig del, ska Högskolan genom avtal försäkra sig om att parten upprätthåller en informationssäkerhet som motsvarar högskolans krav.

9. Extern användning av Högskolans IT-resurser

Om en annan part får tillgång till eller kan utnyttja Högskolans IT-resurser, ska Högskolan genom avtal försäkra sig om att nyttjandet sker i enlighet med Högskolans regler och riktlinjer, och att parten upprätthåller en informationssäkerhet som motsvarar Högskolans krav.

10. Genomförande

För att nå de uppsatta målen ska resurser avdelas för att systematiskt genomföra:

- riskbedömning och konsekvensanalys
- riktlinjer och handlingsplan
- informationssäkerhetshöjande åtgärder
- utbildning och information

En plan för säkerhetsarbetet inom varje institution och avdelning ska upprättas och regelbundet revideras. Planen ska innehålla en beskrivning av säkerhetsläget samt planerade åtgärder för att åstadkomma rätt säkerhetsnivå. Resultatet redovisas till rektor tillsammans med förslag till budget. Rektor beslutar om planen, genomförande och budget.

11. Regelbrott och påföljder

Brott mot informationssäkerhetsregler kan medföra avstängning från IT-system genom beslut av prefekt /avdelningschef enligt anvisningar som rektor meddelar. Allvarligare fall av missbruk eller andra liknande regelbrott ska anmälas till personalansvarsnämnden när det gäller anställda och till disciplinnämnden för studenter när frågan berör studerande. Misstankar om brottslig verksamhet ska polisanmälas. Sådan anmälan ska ske genom rektors försorg.

12. Informationssäkerhetspolicyns giltighet

Detta dokument gäller till 2011-12-31, men kan vid behov revideras. IT- och campuschefen är ansvarig för att så sker.