Linnéuniversitetet
Kalmar Växjö

Rektorsbeslut nr: 91
Datum: 2012-04-16
Dnr: LNU 2012/128

Informationssäkerhetspolicy för Linnéuniversitetet

Föredragning
Strategiska IT-rådet har på uppdrag av tf universitetsdirektör Per Brolin utarbetat förslag till Informationssäkerhetspolicy för Linnéuniversitetet. En arbetsgrupp bestående av personer från IT-rådet, IT-avdelningen samt Informatikämnet utsågs av IT-rådet för att arbeta fram förslag till informationssäkerhetspolicy samt tillhörande styrdokument. Gruppens arbete har kontinuerligt avrapporterats och slutredovisats till universitetsdirektören och personer verksamma inom rektors kansli.

Rektor föreslås fastställa förslag till informationssäkerhetspolicy för Linnéuniversitetet.

Handläggningen har godkänts av universitetsdirektör Per Brolin.

Beslut

Rektor beslutar

att fastställa dokumentet *Informationssäkerhetspolicy* enligt förslag.

Beslut i detta ärende har fattats av rektor Stephen Hwang efter skriftlig föredragning av handläggare Peter Knutsson, nämndskansliet i närvaro av universitetsdirektör Per Brolin, prorektor Lena Fritzén, studentrepresentanten Dennis Persson och sekreterare Sofia Svensson.

Stephen Hwang
rektor

Sofia Svensson
sekreterare

Linnéuniversitetet
Kalmar Växjö

Dnr: 2012/128

Policydokument

Informationssäkerhetspolicy

Beslutat av
Rektor

Gäller från
2012-04-16

Inledning

Styrelsen är ansvarig för att det finns ett informationssäkerhetsarbete (LIS, Ledningssystem för informationssäkerhet) varav denna policy är det övergripande styrdokumentet.

Informationssäkerhet som begrepp omfattar skydd av information både när den hanteras manuellt av människor och när den behandlas med hjälp av IT.

Medborgare och företag måste känna tillit till myndighetens sätt att hantera information.

Bakgrund

Ett systematiskt arbete med informationssäkerhet krävs av myndigheter enligt föreskrift (MSBFS 2009:10, § 3-6) "Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet". Enlig dessa ska myndigheten:

- Upprätta en informationssäkerhetspolicy och andra styrande dokument,
- Utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet,
- Klassificera sin information med utgångspunkt i krav på konfidentialitet, tillförlitlighet och tillgänglighet,
- Utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras,
- Dokumentera granskningar och säkerhetsåtgärder av större betydelse som har vidtagits,
- Minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet,
- Arbeta enligt standarder som: ledningssystem för informationssäkerhet, (SS-ISO/IEC 27001: 2006 fastställd 2006-01-19) och riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005 fastställd 2005-08-12).

Övergripande ledningssystem

Ledningssystem för informationssäkerhet (LIS) är ett av flera system inom universitetet. Det är därför viktigt att LIS-arbetet samordnas med övrigt ledningsarbete.

Informationssäkerheten är beroende av universitetets övriga säkerhetsarbete. Säkerhetsarbetet skall ur alla aspekter samordnas i så hög grad som möjligt och utgöra en del av processen "intern styrning och kontroll" (ISK).

Syfte med Informationssäkerhetspolicyn

Informationssäkerhetspolicyn ska:

- Ange ramar för organisationen, ledning och beslutfattande inom informationssäkerhet,
- Fastställa vilka styrdokument som ska finnas och som är av särskild betydelse för universitetet.

Informationssäkerhetspolicyn omfattar hela myndighetens arbete med informationssäkerhet. Eventuella undantag regleras i för ändamålet framtagna styrdokument.

Mål för informationssäkerhet

Informationssäkerhetsarbetets målsättningar är:

- Tillförlitlighet, information och system ska befinna sig i förväntat och korrekt tillstånd,
- Tillgänglighet, information och system ska vara tillgängliga för behöriga användare,
- Konfidentialitet, endast behöriga användare ska ha tillgång till information och system.

Övergripande principer

Informationssäkerhetspolicyn beslutas av rektor.

Ansvarig för att informationssäkerhetspolicyn är känd, efterlevs, följs upp och revideras är informationssäkerhetsansvarig.

Inom myndighetens organisatoriska enheter kan det vid behov även utses lokala informationssäkerhetsansvariga.

Alla anställda omfattas av informationssäkerhetspolicyn och ska verka för att myndigheten når uppsatta mål.

Som komplement till denna policy finns det/ska det arbetas fram styrdokument som beskriver nedan angivna områden på en mer detaljerad nivå.

Det åligger universitetsstyrelsen att kontinuerligt följa upp arbetet med informationssäkerhet. Det ska därför finnas styrdokument för hur rapportering och uppföljning sker mellan verksamheterna, universitetsledningen och styrelsen.

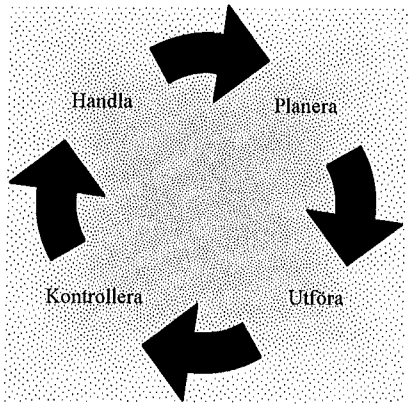
Ledningen ska dock minst en gång per år följa upp och utvärdera informationssäkerheten.

Styrdokument

Informationssäkerhetsarbetet preciseras i ett antal universitetsövergripande styrdokument. De universitetsövergripande reglerna kan behöva kompletteras med verksamhetsspecifika styrdokument. Styrdokumenten utarbetas med stöd av standarder som SS-ISO/IEC 27001:27005 eller motsvarande.

Styrdokument ska finnas för följande områden:

- Informationsklassificering,
- Organisation, roller och ansvarsförhållanden,
- Riskhantering av information,
- Incidenthanterings- och kontinuitetsorganisation,
- Omfattningar och begräsningar av säkerhetsarbetet,
- Säkerhetsarbete för olika typer av resurser, vilket innebär en riktlinje per resurs eller grupp av resurser,
- Rapportering och uppföljning.



PDCA modell, Figur 1

Styrdokumenten ska regelbundet revideras för att säkerställa att uppställda krav på informationssäkerhetsarbetet uppfylls. Den ISO–standard som förekommer inom informationssäkerhet är PDCA (Planera, Utföra, Kontrollera, Handla), se figur 1 ovan.