Informationssäkerhetspolicy för Linköpings universitet

Som en myndighet under regeringen har Linköpings universitet en skyldighet enligt Myndighetens för samhällsskydd och beredskap föreskrift om statliga myndigheters informationssäkerhet (MSBFS 2016:1) att bedriva ett systematiskt informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Denna policy beskriver universitetets viljeinriktning för informationssäkerhetsarbetet vid Linköpings universitet (LiU) och utgör grunden för universitetets ledningssystem för informationssäkerhet (LIS). Informationssäkerhetsarbetet vid LiU ska bedrivas med sin utgångspunkt i universitetets värdegrund, verksamhetens behov och förutsättningar, och en god förvaltningskultur.

Policyn operationaliseras av följande dokument:

- Ledningssystem för informationssäkerhet
- Uppdragsbeskrivning för informationssäkerhetssamordnaren
- Riktlinjer för informationssäkerhet
- Riktlinjer för personuppgiftsbehandling

Mål

Målet med informationssäkerhetsarbetet vid LiU är att säkerställa att informationstillgångar hanteras så att LiU:s, dess samarbetspartners, och enskilda individers intressen tillvaratas, särskilt med avseende på konfidentialitet, integritet, och tillgänglighet, samt att LiU följer gällande lagstiftning.

Strategi

Nyckeln till ett framgångsrikt och verksamhetsanpassat informationssäkerhetsarbete är att LiU upprätthåller mycket god egen kompetens inom IT- och informationssäkerhet, i synnerhet hos de personer och grupper som genom ledningssystem och riktlinjer för informationssäkerhet är utpekade att arbeta med informationssäkerhetsfrågor. Arbetet behöver vidare ständigt anpassas till förändringar i behov, förutsättningar, risker, och andra omständigheter.

Genom informationssäkerhetsarbetet ska LiU identifiera vilka informationstillgångar som finns vid universitetet, deras väsentlighet för verksamheten, och deras skyddsbehov utifrån den risk som LiU utsätts för. LiU ska även genom ett riskbaserat arbetssätt formulera riktlinjer för informationssäkerhet.

Riktlinjerna för informationssäkerhet ger ett konkret stöd för att reducera informationssäkerhetsriskerna till acceptabla nivåer, samt säkerställer efterlevnad av gällande lagstiftning. Effekt och efterlevnad av fastställda riktlinjer ska följas upp för att tillgodose universitetsledningens behov av information kring informationssäkerhet.

Genom att informationssäkerhetsarbetet är väl förankrat i verksamhetens behov och förutsättningar ska behovet av undantag från fastställd policy och riktlinjer minimeras. Undantag som ändå önskas måste först godkännas i enlighet med den ordning som beslutas av universitetsledningen, utifrån en värdering av den risk som de innebär för LiU som helhet.

Ansvar

Informationssäkerhet är en angelägenhet för hela LiU:s verksamhet. Ansvaret för informationssäkerhetsarbetet följer delegationsordningen och preciseras i de dokument som operationaliserar denna policy (Ledningssystem för informationssäkerhet, Uppdragsbeskrivning för informationssäkerhetssamordnaren, Riktlinjer för informationssäkerhet, samt Riktlinjer för personuppgiftsbehandling).

Varje anställd ansvarar för att följa universitetets riktlinjer för informationssäkerhet samt för att bedriva informationssäkerhetsarbete i enlighet med ledningssystemet för informationssäkerhet och riktlinjerna för informationssäkerhet.

Universitetsledningen fastställer genom rektor dels riktlinjer för informationssäkerhet och dels ett ledningssystem för informationssäkerhet som uppfyller de krav som ställs i den lagstiftning och annan reglering som universitetet lyder under. Riktlinjer och ledningssystem uppdateras regelbundet för att ständigt förbättra och effektivisera informationssäkerhetsarbetet. Universitetsledningen ska även genom rektor utse en informationssäkerhetssamordnare med ansvar att leda och samordna informationssäkerhetsarbetet.

Universitetsstyrelsen fastställer LiU:s informationssäkerhetspolicy. Policyn revideras med ett intervall av 3–5 år.

Definitioner

Informationssäkerhet	Bevarande av konfidentialitet, riktighet, och tillgänglighet hos information.
Informationstillgång	Information, och resurser som hanterar den, som är av värde för en organisation. Exempel på informationstillgångar är information, program, tjänster, fysiska tillgångar som datorer och datamedia, människor och deras kompetens, och immateriella tillgångar.
IT-säkerhet	IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet.
Konfidentialitet	Skydd mot obehörig insyn.
Ledningssystem för informationssäkerhet	Del av organisationens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla, och förbättra organisationens informationssäkerhet.
Riktighet	Skydd mot oönskad förändring.
Risk	En sammanvägning av sannolikheten för att en oönskad händelse ska inträffa, och de konsekvenser händelsen kan leda till.
Tillgänglighet	Åtkomst för behörig person vid rätt tillfälle.