

Beslut om Informationssäkerhetspolicy

Beslut

Universitetsstyrelsen beslutar att "Informationssäkerhetspolicy" ska träda i kraft i enlighet med de ikraftträdandebestämmelser som anges i styrdokumentet (se bilaga).

Detta beslut ersätter tidigare beslut om informationssäkerhetspolicy för Linköpings universitet (LiU), dnr LiU-2018-02237, som fastställdes den 5 december 2018.

Beslutet ska föras in i LiU:s regelsamling.

Skäl till beslut

Styrelsen för LiU antog 2018 en informationssäkerhetspolicy för lärosätet, i enlighet med kraven som då ställdes av Myndigheten för samhällsskydd och beredskap (MSB), med ett uttalat mål att revidera policyn med ett intervall om tre till fem år. Sedan policyn antogs har förutsättningarna för den förändrats, vilket också aktualiserar en uppdatering.

MSB har utkommit med nya föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter, som ersätter de tidigare föreskrifterna och allmänna råden (MSBFS 2016:1) om statliga myndigheters informationssäkerhet till vilken den tidigare policyn var avpassad. De nya föreskrifterna framhäver tydligare att myndigheterna ska ta stöd av standarderna ISO 27001 och 27002 samt att tillräckliga resurser ska avsättas till arbetet. I de upphävda föreskrifterna angavs enbart att den standarden skulle beaktas. Vidare har flera organisationer som universitetet samarbetar med uttryckt förväntningar gränsande till krav på att informationssäkerhetsarbetet ska bedrivas i enlighet med standarden ISO 27001.

För att uppfylla formkraven för en informationssäkerhetspolicy enligt ISO 27001 har följande införts:

- En definition av informationssäkerhet.
- Ett ramverk för att sätta informationssäkerhetsmål.
- Ett åtagande att ständigt förbättra ledningssystemet för informationssäkerhet.

Därutöver har policyn ändrats så att det systematiska informationssäkerhetsarbetet ska bedrivas med stöd av standarderna ISO 27001 och 27002 eller motsvarande för

att reflektera motsvarande förändring i MSB:s föreskrifter.

Slutligen har hänvisningarna till MSB:s föreskrifter uppdaterats och riktlinjerna för personuppgiftsbehandling tagits bort från listan över operationaliserande dokument, då de har upphävts och ersatts med en vägledning.

Handläggningen av beslutet

Beslut i detta ärende har fattats av universitetsstyrelsen vid dess sammanträde denna dag efter föredragning av digitaliseringsdirektören Joakim Nejdeby och enhetschefen för IT-infrastrukturenheten David Byers. I beslutet har deltagit ordföranden Susanne Thedéen, universitetets rektor Jan-Ingvar Jönsson och övriga ledamöterna Filippa Alesand Lundin, Dilsa Demirbag-Sten, Michael Felsberg, Markus Heilig, Hans Holmström, Magnus Höij, Linus Karlsson, Betty Malmberg, Staffan Sarbäck, Stig Slørdahl, Ulrika Unell, Elin Wihlborg och Anna Wikström. Vidare har närvarat prorektor Karin Axelsson, tillförordnande universitetsdirektören Per-Olof Brehmer, personalföreträdarna Eva-Lisa Granath och Maria Hugo-Lindén, tillträdande studentledamoten Eira Movin, doktoranden Magdalena Nejld samt styrelsens sekreterare Linda Strandlund.

Vid beredningen av ärendet har enhetschefen för IT-infrastrukturenheten David Byers och systemarkitekten Johannes Hassmund deltagit. Ärendet har varit föremål för samverkan med de fackliga organisationerna i centrala samverkansgruppen (CSG).

Redaktionen för regelsamlingen har granskat beslutets form.

Susanne Thedéen

Joakim Nejdeby

Informationssäkerhetspolicy

1 Bakgrund

Som en myndighet under regeringen har Linköpings universitet (LiU) en skyldighet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter att bedriva ett systematiskt informationssäkerhetsarbete med stöd av standarderna ISO 27001 och 27002 eller motsvarande. Denna policy beskriver universitetets viljeinriktning för informationssäkerhetsarbetet vid 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, samt en god förvaltningskultur.

Policyn operationaliseras av följande dokument:

- Ledningssystem för informationssäkerhet
- Riktlinjer för informationssäkerhet.

2 Informationssäkerhet

Med informationssäkerhet menas bevarandet av informationens konfidentialitet, riktighet och tillgänglighet. Det är ett vitt begrepp som omfattar såväl fysisk som elektronisk hantering, alla typer av information samt skyddsbehov till följd av såväl interna och externa krav som antagonistiska och slumpartade hot.

3 Mål

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

4 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 ska vidare ständigt förbättras och anpassas till förändringar i behov, förutsättningar, risker, och andra omständigheter. Mål för

informationssäkerhetsarbetet ska årligen fastställas av universitetsledningen utifrån verksamhetens förutsättningar och behov samt de omständigheter i övrigt som påverkar skyddet av information vid LiU.

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 ska ge ett konkret stöd för att reducera informationssäkerhetsriskerna till acceptabla nivåer, samt ska säkerställa 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.

5 Ansvar

Informationssäkerhet är en angelägenhet för hela LiU:s verksamhet. Ansvaret för informationssäkerhetsarbetet följer delegationsordningen och preciseras i de dokument som operationaliserar denna policy.

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, 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 tre till fem år.

6 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 samt immateriella tillgångar. |
| ISO 27001 | SS-EN ISO/IEC 27001:2022 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav, en standard för ledningssystem för informationssäkerhet. |
| ISO 27002 | SS-EN ISO/IEC 27002:2022 Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder, en förteckning över säkerhetsåtgärder att användas i kombination med ISO 27001. |
| 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. |

7 Ikraftträdande

Denna policy träder i kraft den 1 juli 2024.

Signature page

This document has been electronically signed
using eduSign.

eduSign