

Beslutsfattare: Rektor Dokumenttyp: Policy Giltighetstid: tillsvidare	Beslutsdatum: 2019-10-28 Träder i kraft: 2019-11-01 .
Dokument som upphävs: LTU-531-2013	

Informationssäkerhetspolicy vid Luleå tekniska universitet

Innehållsförteckning

1.	INLEDNING	3
2.	INFORMATIONSSÄKERHETSARBETET VID LULEÅ TEKNISKA UNIVERSITET	3
3.	MÅLSÄTTNING	4
4.	ORGANISATION OCH ANSVAR.....	4
5.	HANTERING AV AVVIKELSER OCH UNDANTAG	5

1. Inledning

Luleå tekniska universitet genererar och hanterar stora mängder information. Information är en av universitetets viktigaste tillgångar. Universitetets informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt med en helhetssyn på informationssäkerhet som inbegriper universitetets alla verksamhetsdelar. En säker informationshantering utgör en förutsättning för att universitetet ska kunna fullgöra uppdraget med att tillhandahålla utbildning, bedriva forskning samt att samverka med det omgivande samhället.

Arbetet med informationssäkerhet utgår främst från lagar, förordningar, föreskrifter, universitetets egna krav samt avtal. Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet¹ ska ligga till grund för universitetets informationssäkerhetsarbete.

Informationssäkerhetsarbetet ska samordnas med övrigt säkerhetsarbete vid universitetet.

Denna policy beskriver målsättning, organisation, ansvar och roller avseende informationssäkerhetsarbetet och syftar till att säkerställa en säker hantering av universitetets informationssäkerhetstillgångar.

Dokumentet omfattar hela universitetets informationssäkerhetsarbete, samtliga informationstillgångar universitetet äger, hanterar eller bedriver forskning på och berör samtliga medarbetare, studenter och övriga intressenter som har tillgång till universitetets information och IT-resurser.

2. Informationssäkerhetsarbetet vid Luleå tekniska universitet

Informationssäkerhetsarbetet vid Luleå tekniska universitet ska bedrivas aktivt och systematiskt. Detta i syfte att bidra till att nå uppsatta mål, att skapa trygghet för medarbetare och samarbetspartners samt för att minska/undvika skador.

Universitetets informationssäkerhetsarbete ska ske med långsiktighet, kostnadseffektivitet och på ett strukturerat sätt.

Följande principer ska vara styrande för informationssäkerhetsarbetet vid Luleå tekniska universitet:

- Informationssäkerhetsarbetet ska vara en integrerad del av det dagliga arbetet. Informationssäkerheten ska hålla kravställd nivå, oberoende av var och i vilken form informationsbehandlingen sker.
- Informationssäkerheten vid samarbete med extern part och/eller utlandsvistelse, bör säkerställas genom särskild informationssäkerhetsklassning

och risk- och sårbarhetsanalys.

- All information inom universitetet bör klassificeras så att det går att avgöra vilket skydd informationen behöver och hur den får hanteras.

3. Målsättning

Informationssäkerhetsarbetet ska vara riskbaserat. Kostnaden för skyddsåtgärder ska vägas mot nyttan och nivå av risktagande. Arbetet för varje område ska planeras, styras och utföras strukturerat.

Utgångspunkten för arbetet bör alltid utgå från nedanstående aspekter:

- informationen och informationsresurserna ska alltid vara skyddade mot obehörig åtkomst (*konfidentialitet*),
- informationen ska vid varje tillfälle vara korrekt och informationsresurserna och den administrativa säkerheten ska säkerställa att informationen inte kan förvanskas genom obehörig eller felaktig hantering (*riktighet*),
- alla medarbetare ska ha tillgång till den information som de behöver för att utföra sina arbetsuppgifter och åtaganden (*tillgänglighet*) och
- alla aktiviteter i IT-system, som behandlar skyddsvärd information ska kunna härledas till en identifierad användare så att det går att ta reda på vem/vad som hanterat informationen (*spårbarhet*).

4. Organisation och ansvar

Det övergripande ansvaret för myndigheten har universitetsstyrelsen och rektor, vilket inbegriper ansvaret för universitetets informationssäkerhet. Rektor fastställer policy och övergripande riktlinjer för säkerhetsarbetet vid universitetet. Av Rektors besluts- och delegationsordning framgår att samordningsansvaret för informationssäkerhet innebär ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av informationssäkerhetsarbetet.

Av Rektors besluts- och delegationsordning framgår att prefekt och chef för verksamhetsstödet ansvarar för informationssäkerhet inom sitt område samt att medarbetare är tillräckligt informerade om sina roller och ansvar ifråga om informationssäkerhet innan de ges åtkomst till universitetets informationssystem.

Ansvarig chef ska säkerställa att det finns förutsättningar för att informationen ska kunna klassificeras och hanteras enligt fastställd modell.

5. Hantering av avvikelser och undantag

De informationstillgångar som universitetet äger eller ansvarar för ska vara säkrade även om oförutsedda händelser inträffar som störningar och incidenter. Prefekt och chef för verksamhetsstödet ansvarar för att rutiner, processer eller motsvarande finns för att säkerställa detta.