

| | | | |
|-----------------------|---|-----------------|------------|
| Beslutsfattare: | Rektor | Beslutsdatum: | 2025-06-23 |
| Dokumenttyp: | Styrande dokument | Träder i kraft: | 2025-06-23 |
| Giltighetstid: | Tillsvidare | | |
| Dokument som upphävs: | Informationssäkerhetspolicy LTU-2292-2019 | | |

Informationssäkerhetspolicy

1. Inledning

1.1 Dokumentets syfte

Denna policy är en del av Luleå tekniska universitets ledningssystem för informationssäkerhet. Syftet med policyn är att säkerställa förutsättningarna för ett systematiskt informationssäkerhetsarbete som ger ett ändamålsenligt och välavvägt skydd och kvalitet i universitetets informationshantering. Policyn beskriver mål, organisation, övergripande roller och ansvar inom informationssäkerhetsområdet.

Informationssäkerhetspolicyn konkretiseras vidare genom riktlinjer, regler och rutiner.

Policyn omfattar hela universitetets informationssäkerhetsarbete, samtliga informationstillgångar som universitetet äger eller hanterar och berör samtliga medarbetare, studenter och övriga intressenter som har tillgång till universitetets information och IT-resurser. Policyn ska även tillämpas då universitetet upphandlar produkter och tjänster inom informationshanteringen.

1.2 Bakgrund och definitioner

Luleå tekniska universitet är en myndighet med uppdraget att bedriva utbildning och forskning, vilket innebär att lärosätet genererar och hanterar stora mängder information, både i fysisk och digital form. Denna information är en av universitetets viktigaste tillgångar för att kunna fullgöra uppdraget. För universitetet är en god informationssäkerhet ett förhållningssätt som ska genomsyra hela universitetets verksamhet.

Informationssäkerhet handlar om att på ett systematiskt sätt hantera och skydda information på ett tillfredsställande sätt. Dels genom att klassificera all den information som universitetet hanterar, dels genom att säkerställa att information utifrån klassning skyddas på rätt sätt för att förhindra att information läcker ut, förvanskas eller förstörs.

Informationssäkerhet omfattar områdena administrativ, organisatorisk och teknisk säkerhet. Det är ett förhållningssätt som inte bara begränsas till system, utan även gäller för olika former av informationsbärare, som exempelvis papper, tal mellan individer, bild och annan lagringsmedia.

Arbetet med informationssäkerhet utgår främst från lagar, förordningar, föreskrifter, universitetets egna krav samt ingångna avtal. Som myndighet är universitetet skyldigt att följa gällande lagstiftning inom området och då särskilt beakta förordningen (2022:524) om statliga myndigheters beredskap och Myndigheten för samhällsskydd och beredskaps föreskrifter för informations- och IT-säkerhet (MSBFS 2020:6 och 2020:7).

Informationsägare är en term som används inom informationssäkerhetsområdet, och så även i detta dokument, och innebär ett chefsansvar på samma sätt som budget-, kvalitets- och miljöansvar. Informationshanterare är likaså en term som används inom informationssäkerhetsarbetet och avser samtliga medarbetar, studenter, samarbetspartners och övriga intressenter som har tillgång till universitetets information.

Informationssäkerhetsarbetet ska samordnas med övrigt säkerhetsarbete vid universitetet.

2. Informationssäkerhetsarbetet vid Luleå tekniska universitet

Informationssäkerhetsarbetet ska vara en integrerad del i all verksamhet som bedrivs vid Luleå tekniska universitet i syfte att förebygga och begränsa negativa effekter av oönskade händelser.

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

- Informationssäkerhetsarbetet ska bygga på den etablerade standardserien ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS).
- Informationssäkerhetsarbetet ska bedrivas aktivt, systematiskt och vara grundad i riskanalyser. Riskanalyserna utgår från aktuell hotbild och ger ett stöd i arbetet med att klassa informationens värde utifrån universitetets beslutade klassificeringsmodell. Kostnaden ska vara vägd mot nyttan och risktagandet.
- För att skyddet ska få rätt nivå och omfattning ska universitetets informationssäkerhet vara grundad i informationsklassning och risk-och sårbarhetsanalys.
- Informationsägaren, tillika verksamhetschef, ansvarar för att det finns en dokumenterad bild över information som hanteras inom dennes verksamhetsområde och att den årligen uppdateras. All information bör klassificeras så att det går att avgöra vilket skydd informationen behöver och hur den får hanteras.
- Arbetet ska vara en integrerad del av medarbetarens ansvar för den egna verksamheten. Den viktigaste delen i att skapa en säker informationshantering är alltid medarbetarnas kunskap, medvetenhet och motivation.
- Vid samarbete med extern part och/eller utlandsvistelse ska en bedömning av informationens skyddsvärde och en riskanalys alltid ske.

- För arbetet ska det finnas målgruppsanpassad information samt tillgängliga instruktioner och mallar. Informationstillfällen som ger möjlighet till dialog rörande informationssäkerhetsfrågor ska tillhandahållas.

3. Målsättning

Informationssäkerhetsarbetet ska vara riskbaserat. Arbetet för varje verksamhetsområde ska planeras, styras och utföras strukturerat för en robust, säker och tillförlitlig informationshantering.

Följande mål gäller för universitetets informationssäkerhetsarbete och ska följas upp av ledningen:

- Det ska alltid finnas utpekade informationsägare som har ett tydligt ansvar för sin del av universitetets informationshantering.
- Informationssäkerhetsarbetet ska uppfylla efterlevnaden av lagar, föreskrifter och avtal som reglerar informationshantering.
- Universitetet ska ha en utvecklad säkerhetsmedvetenhet och uppmuntra till engagemang hos alla medarbetare till att följa gemensamma regler samt motivera dem att delta i att ständigt förbättra informationssäkerheten för informationshanteringen.
- Medarbetare eller andra informationshanterare ska vara utbildade och kunniga i informationssäkerhet i relation till sin roll.
- Utifrån klassningsnivå ska informationen som hanteras alltid vara skyddad mot obehörig åtkomst, den ska vara korrekt, tillgänglig vid behov och i de fall där så krävs ska det kunna fastställas vem som har haft tillgång till informationen. Detta svarar mot de centrala begreppen inom informationssäkerhet: konfidentialitet, riktighet, tillgänglighet och spårbarhet.

4. Organisation och ansvar

Det övergripande ansvaret för universitetets informationssäkerhet har universitetsstyrelsen och rektor. I detta ansvar ingår att säkerställa att det finns styrande dokument för informationssäkerhetsarbetet och de resurser som behövs för att genomföra det som styrdokumentet föreskriver. Rektor ansvarar även för att en systematisk uppföljning av informationssäkerhetsarbetet vid universitetet genomförs.

Av Rektors besluts- och delegationsordning framgår att prefekt och chef för verksamhetsstödet ansvarar för informationssäkerhet inom sitt område. Samtliga informationsägare (verksamhetschefer) ansvarar för sin informationshantering och därmed också tillämpningen av informationssäkerheten i den egna verksamheten.

Informationsägare ansvarar även för att medarbetarna är tillräckligt informerade om sina roller och ansvar gällande informationssäkerhet innan de ges åtkomst till universitetets informationssystem. Ansvarig verksamhetschef ska säkerställa att det finns förutsättningar för att informationen ska kunna klassificeras och hanteras enligt fastställd modell.

Samordningsansvaret för informationssäkerhetsarbetet ligger hos informationssäkerhetsfunktionen och innebär ansvar för planering, samordning, uppföljning och kontroll av efterlevnad av informationssäkerhetsarbetet. Informationssäkerhetschefen ansvarar för att rektor och universitetets ledning får uppdaterade lägesbilder över identifierade hot och risker som kan påverka eller påverkar universitetets informationshantering och därmed informationssäkerhetsarbetet. Rektor beslutar om hur dessa informationssäkerhetsrisker ska hanteras.

5. Uppföljning och rapportering

Informationssäkerhetspolicyn ska regelbundet ses över och uppdateras för att säkerställa att den är effektiv och anpassad till förändringar i verksamheten och omvärlden.

I samband med universitetets tertialuppföljningar ska även uppföljning av informationssäkerhetsarbetet ske.

Huvudföredragande i informationssäkerhetsfrågor är informationssäkerhetsansvarig.

6. 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.