

Informationssäkerhetspolicy

Rektor har 2023-06-01 beslutat om Policy för informationssäkerhet (SU FV-2209-23). Policyn ersätter de tidigare Riktlinjer för informationssäkerhet vid Stockholms universitet, Dnr SU FV-2.11.2-1923-16, beslutsdatum 2017- 01-26.

1. Inledning

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

Stockholms universitet är en myndighet med uppdraget att bedriva utbildning och forskning, vilket innebär att verksamheten innefattar produktion, bearbetning, lagring och överföring av en stor mängd information som är av olika karaktär i både fysisk och digital form.

Informationssäkerhet handlar dels om att klassificera all den information som universitetet hanterar och dels om att säkerställa att information utifrån klassning skyddas på rätt sätt för att hindra att information läcker ut, förvanskas eller förstörs.

Arbetet med säker informationshantering utgår från lagar, förordningar, föreskrifter, egna krav och 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).

Ansvar för en säker informationshantering är en integrerad del av ansvaret för de olika verksamheterna inom universitetet. Detta innebär att informationssäkerhetsansvaret följer det delegerade verksamhetsansvaret, så att chefer för verksamhet också ansvarar för säker hantering av verksamhetens information. Informationsägare är en term som används inom informationssäkerhetsområdet. Rollen innehas främst av prefekt/föreståndare eller avdelningschef. Informationsägarskapet innebär ett chefsansvar på samma sätt som budget-, kvalitets- och miljöansvar. Informationshanterare är likaså en term som används inom informationssäkerhetsarbetet med detta avses samtliga medarbetar, studenter, samarbetspartners och övriga intressenter som har tillgång till universitetets information.

1.1 Omfattning

Policyn omfattar hela universitetets informationshantering och all information som universitetet äger, hanterar eller bedriver forskning på. Policyn berör i form av eget ansvar samtliga som har tillgång till universitetets information. Policyn ska även tillämpas då universitetet upphandlar produkter och tjänster inom informationshanteringen.

1.2 Dokumentets beslutsordning, dokumentansvarig och uppdatering

Policyn ska årligen ses över. Beslut ska tas i enlighet med beslutandeprocess för styrdokument vid universitetet. Informationssäkerhetschefen är dokumentansvarig och ansvarar för årlig översyn av policyn.

2. Policy för informationssäkerhet

Stockholms universitets policy för informationssäkerhet sammanfattas enligt nedanstående principer:

Universitetets policy är att informationssäkerhetsarbetet ska bedrivas aktivt, systematiskt och med hänsyn tagen till potentiella risker och att kostnaden ska vara vägd mot nytta och risktagandet.

För att skyddet ska få rätt nivå och omfattning ska universitetets informationssäkerhet vara grundad i riskanalyser. Riskanalyserna utgår från aktuell hotbild och ger ett stöd i arbetet med att klassa informationens värde utifrån universitetets beslutade klassificeringsmodell. Arbetet följer verksamhetsansvaret. Informationsägaren ansvarar för att det finns en dokumenterad bild över information som hanteras inom dennes verksamhetsområde och att den årligen uppdateras. I dokumentationen ska även informationens klassning och regler för gallring respektive arkivering gå att utläsa.

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 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. Universitets mål med informationssäkerhetsarbetet

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.

Särskild hänsyn ska ägnas åt information som regleras av särskild lagstiftning.

Universitetet ska ha en utvecklad säkerhetsmedvetenhet och uppmuntra till engagemang hos alla medarbetare samt förutom att följa gemensamma regler, motivera dem att delta i att ständigt förbättra 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. Ansvar och organisation

Rektor har det yttersta ansvaret för informationssäkerheten. I detta ansvar ingår att säkerställa att det finns styrdokument 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.

Rektor och universitetets ledning ska årligen få en uppdaterad lägesbild över identifierade hot och risker som kan påverka eller påverkar universitetets informationshantering och därmed informationssäkerhetsarbetet. Rektor beslutar om hur dessa informationssäkerhetsrisker ska hanteras.

Informationssäkerhetsansvaret följer verksamhetsansvaret enligt universitetets besluts- och delegationsordning och innefattar hur informationssäkerhetsarbetet genomförs och upprätthålls inom respektive ansvarsområde. Samtliga informationsägare ansvarar för sin informationshantering och därmed också tillämpningen av informationssäkerhet i den egna verksamheten. Vicerektorer och universitetsdirektören ansvarar och beslutar för hur informationssäkerhetsarbetet genomförs och upprätthålls inom respektive område samt inom förvaltningen.

Informationssäkerhetschefen ansvarar för att driva, samordna och stödja universitetets arbete med informationssäkerhet. Här ingår att ta fram styrande dokument såsom regler, handläggningsordningar och andra instruktioner. 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. Informationssäkerhetschefen tillhandahåller relevant underlag till rektor inför uppföljningstillfällena.

5. Uppföljning och rapportering

Informationssäkerhetsarbetet ska årligen följas upp av rektor och universitetets ledning.

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

Samordning och hantering av informationssäkerhetsfrågor med representation från kärnverksamheten och specialistfunktioner sker inom ramen för IT-styrgruppen. Huvudföredragande i informationssäkerhetsfrågor är informationssäkerhetschefen.