STYRDOKUMENT
Dnr GU 2024/15

Policy för informationssäkerhet vid Göteborgs universitet

Beslutsfattare	Rektor
Ansvarig enhet	Enheten för juridik och informationsförvaltning
Beslutsdatum	2024-01-25
Giltighetstid	Aktualitetsgranskas och/eller revideras senast 2027
Sammanfattning	Göteborgs universitets informationssäkerhetspolicy anger universitetets övergripande mål, principer, ansvar och roller gällande arbetet med informationssäkerhet. Informationssäkerhet handlar om att skydda information i alla dess former. Målet är att säkerställa verksamhetens behov av tillgänglighet och riktighet, samt skydd mot obehörig åtkomst, det vill säga behov av konfidentialitet. Arbetet med informationssäkerhet ska bedrivas systematiskt och riskbaserat med stöd av standarden SS-ISO/IEC 27001 och 27002. Policyn omfattar universitetets hela verksamhet, information, informationssystem och nätverk, alla anställda och studenter, samt leverantörer och externa parter beroende på avtalsförhållanden.

Inledning

Information och tillhörande informationsteknik är en ytterst viktig strategisk resurs för verksamheten vid Göteborgs universitet. För att universitetet effektivt och med hög kvalitet ska kunna utföra sina uppgifter inom utbildning, forskning, verksamhetsstöd och samverkan med det omgivande samhället ska därför ett aktivt arbete med informationssäkerhet bedrivas inom alla områden. Detta bidrar till att universitetet uppfattas som en attraktiv arbetsgivare, en betrodd samarbetspartner och ett universitet för världen.

Arbetet med informationssäkerhet har som syfte att stödja verksamheten, uppfylla lag- och regleringskrav samt avtalskrav. Brister i detta arbete kan leda till att forskningsdata eller information om enskilda förloras eller sprids otillbörligt, vilket kan skada såväl individen som universitetets och forskningslandskapets anseende. Detta kan i sin tur påverka medarbetares, studenters och samarbetspartners förtroende för universitetet. Andra oönskade konsekvenser kan vara förlorad forskningsfinansiering, kostsamma åtgärdspaket eller dryga sanktionsavgifter.

Informationssäkerhet handlar om att skydda information i alla dess former, som exempelvis digitalt, i informationssystem, i nätverk, på papper och i muntlig form. Denna policy är en del av Göteborgs universitets ledningssystem för informationssäkerhet. I ledningssystemet finns styrdokument för informationssäkerhet för ytterligare vägledning.

Omfattning

Informationssäkerhetspolicyn omfattar alla anställda, studenter och övriga personer som har tillgång till Göteborgs universitets IT-resurser och information. Policyn omfattar hela universitetets informationshantering och all information som universitetet äger.

Mål med informationssäkerhetsarbetet

Arbetet ska inriktas på att säkerställa följande övergripande informationssäkerhetsmål**:**

- konfidentialitet, genom att styra åtkomst till information och informationsbehandlingsresurser baserat på behov,
- tillgänglighet till information och tjänster när de behövs
- informationens riktighet genom skydd mot oavsiktlig och avsiktlig förvanskning.

Universitetets arbete med informationssäkerhet ska bedrivas på ett systematiskt, formaliserat och riskbaserat sätt. Det ska också säkra efterlevnaden av gällande lagar, förordningar och föreskrifter. Vidtagna åtgärder ska utifrån verksamhet och risk vara ändamålsenliga och kostnadseffektiva. Informationssäkerhetsarbetet ska bedrivas med stöd av aktuell version av den internationella och svenska standarden för informationssäkerhet, SS-ISO/IEC 27001.

Principer för informationssäkerhet

Universitetets arbete med informationssäkerhet utgår från följande principer:

A - Informationsklassning
En universitetsgemensam modell för informationsklassning ska tillämpas gällande hur informationens behov av konfidentialitet, tillgänglighet och riktighet bestäms och upprätthålls. Modellen utgår från ett riskbaserat angreppssätt.

B – Säkerhet som en integrerad del av lösningen
Inför nyanskaffning av system som hanterar information, som applikationer, tjänster och andra komponenter, ska säkerhet kravställas. Detta enligt principen om att säkerhet ses som en integrerad del av lösningen. Risker och beroenden ska beaktas i hela informationsflödet. Detta gäller även vid förändringar i verksamheten och vid förändringar av system.

C – Universitetets digitala arbetsplats, IT-tjänster och verktyg
Tekniska lösningar, lagringslösningar och tillhörande tillämpningar är avgörande för en säker hantering av information. Medarbetare ska därför i första hand använda den digitala arbetsplats (dator, mobiltelefon och tillhörande programvara och lösningar) som tillhandahålls av universitetets IT-enhet. Denna digitala arbetsplats ska ha adekvata skyddsåtgärder för att kunna hantera majoriteten av verksamhetens information. Vid ytterligare behov/krav på hantering av information, ska IT-enheten erbjuda lämpliga lösningar med adekvat eller höjd skyddsnivå. Vid avsteg ansvarar informationsägaren för att nyttjade lösningar lever upp till universitetets krav, i enlighet med denna policy och tillhörande regler och riktlinjer.

D – Säker autentisering
Tekniker för säker autentisering ska tillhandahållas av IT-enheten och tillämpas för att vid behov säkert avgöra identitet och behörighet till informationstillgångar och minimera risker för identitetsstölder.

E – Omvärldsbevakning och incidenthantering
Omvärldsbevakning och incidenthantering ska bedrivas och är en viktig del av universitetets proaktiva och reaktiva säkerhetsarbete. Detta ger förutsättningar att vidta förebyggande åtgärder för att motverka risken för externa hot samt ger möjlighet att snabbt och effektivt agera på uppkomna, oönskade händelser. Lärdomar från inträffade incidenter är också en viktig komponent i det ständiga arbetet med att förbättra motståndskraften. En grundläggande förutsättning för att processen ska fungera är att samtliga som omfattas av denna policy har kunskap om att, var och hur incidenter ska rapporteras.

Ansvar och roller

Rektor fastställer policy för informationssäkerhet samt principerna för ett ledningssystem för informationssäkerhet. Dessa bereds av informationssäkerhetschef och uppdateras kontinuerligt för att förbättra och effektivisera informationssäkerhetsarbetet i förhållande till förändringar i verksamhetens förutsättningar och behov.

Övriga behov av metodstöd, som exempelvis checklistor och arbetsbeskrivningar tas fram och beslutas av den ansvarig det berör, vilket kan vara exempelvis informationssäkerhetschef, informationsägare eller systemägare. Chefer och verksamhetsansvariga har ett ansvar för att gällande policy och relaterade regelverk för informationssäkerhet är kända och tillämpas inom det egna ansvarsområdet.

Varje användare har ansvar för att informationssäkerhet tillämpas i det egna arbetet i enlighet med gällande policy och relaterade regelverk. Varje enskild användares agerande räknas, då ett enda mänskligt misstag kan åstadkomma universitetsövergripande konsekvenser. Medarbetare och studenter ska vid nyttjande av IT-tjänster, digitala verktyg och informationstillgångar följa gällande policy och relaterade regelverk för informationssäkerhet i det egna arbetet/studierna.

Externa verksamheter som är anslutna till universitetets informations- och IT-resurser ska tillämpa de organisatoriska och tekniska säkerhetsåtgärder som krävs för att uppfylla motsvarande krav i universitetets policy och relaterade regelverk för informationssäkerhet.

Universitetsstyrelsen och rektor ska regelbundet informeras av informationssäkerhetschef om informationssäkerhetsarbetet vid universitetet, exempelvis om i vilken utsträckning införda säkerhetsåtgärder motsvarar verksamhetens behov, allvarliga risker som inte åtgärdats, och övriga hinder för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet.

All information som behandlas ska ha en informationsägare. Informationsägare är den inom Göteborgs universitet som bestämmer varför (ändamålet för informationsbehandlingen) och på vilket sätt informationen lämpligen ska behandlas, handläggas, förvaltas eller på annat sätt får hanteras vid respektive institution/motsvarande. Informationsägaren svarar för att informationen värderas utifrån aspekterna konfidentialitet, riktighet och tillgänglighet med syftet att bestämma skyddsbehov. Ansvaret följer således med ansvaret för verksamheten där informationen behandlas.

Alla informationsbehandlande system på universitetet ska ha en systemägare. Systemägare säkerställer att tillräckliga säkerhetsåtgärder införs i systemet, enligt principen om säkerhet som en integrerad del av lösningen. Säkerhetsåtgärderna ska anpassas när organisationens behov eller förhållanden i omvärlden förändras.

Följande roller är centrala för informationssäkerhetsarbetet vid Göteborgs universitet:

- Säkerhetschef ansvarar för det strategiska säkerhetsarbetet vid Göteborgs universitet som inkluderar informationssäkerhet.
- CISO (informationssäkerhetschef) ansvarar för universitets informationssäkerhetsarbete med att systematiskt utveckla, förvalta, följa upp och förbättra ledningssystemet för informationssäkerhet. Vidare ska CISO etablera en ändamålsenlig organisation för verksamhetens behov av stöd med det operativa informationssäkerhetsarbetet. CISO rapporterar till universitetets styrelse, rektor och universitetsdirektör och har en oberoende, kravställande och granskande roll.
- IT-enheten ansvarar för att leda, samordna och driva arbetet inom IT- och cybersäkerhet, som är en integrerad del av informationssäkerhetsarbetet. Detta arbete syftar till att skydda information, informationssystem och nätverk, med hjälp av ändamålsenliga säkerhetsåtgärder. I området ingår också ett särskilt ansvar att bedriva omvärldsbevakning och agera på identifierade hot och risker.