Informationssäkerhet

Styrdokument Örebro universitet
Kategori: Riktlinjer
Ärendenummer: ORU 2024/02820
Beslutsfattare: Rektor
Senast ändrad: 2024-05-21
Fastställd: 2018-03-20
Dokumentansvarig: Avdelningen för digitalisering och IT

Innehåll

Inledning

Informationshanteringspolicyn anger Örebro universitets mål och inriktning när det gäller informationssäkerhet. Syftet med föreliggande riktlinjer för informationssäkerhet är att skapa goda förutsättningar för en god informationssäkerhet vid Örebro universitet.

Informationssäkerhet

Information är en av Örebro universitets viktigaste tillgångar och dagligen hanteras stora mängder information, både i elektronisk och i fysisk form. Om inte informationen hanteras på rätt sätt kan universitetets verksamhet, goda namn och rykte äventyras. Säker hantering av information utgör också en förutsättning för att Örebro universitet ska kunna fullgöra uppdraget att tillhandahålla utbildning, bedriva forskning samt samverka med det omgivande samhället.

Informationssäkerhet omfattar information och informationstillgångar och handlar om hur informationen hanteras och skyddas så

- att den alltid finns när vi behöver den (tillgänglighet),
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet),
- att endast behöriga personer får ta del av den (konfidentialitet),
- att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet).

Informationssäkerhetsarbetet ska ske systematiskt och riskbaserat med ett tydligt uppdrag från universitetets ledning. Förankring och medvetenhet hos alla anställda och studenter utgör grunden i säkerhetsarbetet. Detta uppnås genom rollanpassad utbildning och kontinuerlig kompetenshöjning inom området.

Systematiskt och riskbaserat informationssäkerhetsarbete

För att informationen ska kunna ges ett relevant skydd ska alla informationstillgångar klassificeras av informationsägaren enligt Örebro universitets informations-klassningsmodell, vilket även innebär en bedömning av hanteringen av personuppgifter. För enskilda dokument och filer är det skaparen som är informationsägare tills dess att informationstillgången färdigställts. Då övergår informationsägarskapet till den roll som organisationsmässigt hanterar den samlade färdigställda informationstillgången.

För att säkerställa att information, processer och system får ett relevant och anpassat skydd ska riskanalyser genomföras som en del i verksamhetsplaneringen. Riskanalysen ska föreslå åtgärder för att identifierade risker kan minskas. När vidtagna åtgärder är genomförda redovisar riskanalysen accepterade risker.

Fastställd informationsklass och resultat av riskanalys ska ligga till grund för relevanta skyddsåtgärder. Skyddsåtgärder kan vara både tekniska och administrativa. Tekniska skyddsåtgärder åligger systemägaren, medan administrativa skyddsåtgärder kan omfatta både systemägare och informationsägare. För att säkerställa att vidtagna åtgärder ger

avsedd effekt och att förutsättningar inte förändras över tid, ska regelbunden utvärdering ske.

Om en extern part hanterar information, ska krav och överenskommelse dokumenteras. Avtal ska reglera vilka åtgärder som extern part ska vidta och även tydliggöra hur rapportering och uppföljning av efterlevnad ska ske.

Säkerhetsåtgärder avseende behandling av information

Verklig informationssäkerhetsnivå är starkt kopplad till användarens ambition, kunskap och vilja. Det innebär att bakgrundskontroller vid anställning ska ske. Dessa ska vara anpassade efter vilken tillgång till information eller system som den anställde kommer att få.

För specifika roller är kompetensbehovet större, och dessa ska få erforderlig och återkommande utbildning för den roll som de innehar. Detta krav ska också ställas på extern part, om information behandlas av annan organisation.

För att säkerställa att användare förstår och följer informationssäkerhetsregler ska det finnas tillgång till anpassad information och kompetenshöjande åtgärder. Kompetensnivån ska regelbundet följas upp så att dedikerat stöd kan ges vid behov.

Varje institution eller avdelning bör ha minst en resurs som har en utökad kompetens inom området för att säkerställa att arbetet inom institutionen eller avdelningen drivs i enlighet med informationssäkerhetsaspekterna.

Tillträde till lokaler som hanterar skyddsvärda informationstillgångar ska begränsas. Det ska finnas funktioner för att upptäcka om obehöriga överträder skyddet.

Kritiska informationstillgångar ska separeras i flera zoner.

Informationssäkerhetsincidenter ska rapporteras till IT-support. Större informations-säkerhetsincidenter hanteras av universitetets CERT (*Computer Emergency Response Team*) genom att säkra spår, avvärja pågående attacker och återställa funktionen för universitetets IT-system. Ordförande för CERT har mandat att vidta de åtgärder som bedöms nödvändiga för att minimera akut verksamhetspåverkan.

Alla verksamhetsansvariga ska planera för kontinuitet i sin verksamhet. Kontinuitet innebär att en viss nivå av verksamhet kan bedrivas via alternativa arbetsmetoder under en begränsad tid. Kontinuitetsplanering kan innebära både tekniska och administrativa åtgärder. Planerna ska revideras och övas årligen.

Uppföljning av informationssäkerhetsarbetet

Avdelningen för digitalisering och IT ansvarar för att årligen utvärdera nivån för Örebro universitets samlade informationssäkerhetsarbete. Utvärderingen ska både visa effekten av införda åtgärder, men även redovisa omfattningen av de aktiviteter som genomförts under året.

Universitetsledningen ska årligen informera sig om i vilken utsträckning som den samlade informationssäkerhetsnivån speglar universitetens samlade kravnivå och nivå för acceptabla risker.

Begreppsförklaring

- **Informationstillgångar** är allt som innehåller information och allt som bär på information.
- **Informationssäkerhet** är säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.
- **IT-säkerhet** är de åtgärder som utförs för att genom tekniskt och logiskt skydd i universitetets elektroniska utrustning upprätthålla en korrekt nivå på säkerheten i utrustningen. IT-säkerheten utgör skyddet för den utrustning som används för att förvara och behandla universitetets information.
- **Konfidentiell information** får inte nås av eller avslöjas för någon obehörig. Oftast gäller det innehållet i en informationstillgång, men ibland är även tillgångens existens hemlig.
- **Riktig information** innebär att informationen inte förändras av obehöriga, av misstag eller på grund av en funktionsstörning i något tekniskt system.
- **Tillgänglig information** innebär att informationen går att utnyttja av behörig användare när det behövs och så mycket som det behövs.