REKTORS KANSLI

2023-03-13 Dnr C2023/268

Riktlinjer för informationsklassning och val av säkerhetsåtgärder i ledningssystem för informationssäkerhet (LIS) vid Karlstads universitet

Syfte

Riktlinjernas syfte är att beskriva hur Karlstads universitets information och övriga informationstillgångar klassificeras och skyddas på rätt sätt. Riktlinjerna är framtagna för att stödja verksamheten att uppfylla kraven i MSB:s föreskrift om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

MSB:s interna styrdokument, Riktlinje för kontroll av tillgångar samt informationsklassning, MSB:s metodstöd för informationssäkerhet samt Riktlinjer för informationssäkerhet i Västra Götalandsregionen har använts som mall och inspiration.

Riktlinjerna är ett av de underdokument som kompletterar styrdokumentet Informationssäkerhetspolicy vid Karlstads universitet.

Det huvudsakliga arbetet med att ta fram riktlinjerna har utförts av Informationshanteringsrådet i samråd med IT-chefen och säkerhetschefen.

Beslut:	RB 43/23	Dnr:	C2023/268	Ersätter:	RB 25/15	Dnr:	C2015/176
Giltighet fr.o.m:	2023-03-13	t.o.m:	Tills vidare	Handläggare:	Niklas Nikitin		

1 Inledning

Alla informationstillgångar ska vara kopplade till en informationsägare[1], som har ansvar för att informationen klassificeras och skyddas på rätt sätt.

Informationsklassning och val av säkerhetsåtgärder är en process som är central för Karlstads universitets informationssäkerhetsarbete.

2 Omfattning

Informationsklassning och val av säkerhetsåtgärder ska ske beträffande alla informationstillgångar inom Karlstads universitet. Riktlinjerna gäller för all hantering av myndighetens informationstillgångar oavsett var eller i vilken form hanteringen sker.

3 Definitioner

Definitionerna nedan kommer från SIS-TR 50:2015[2] eller SS-ISO/IEC 27000:2020 om inte annat uttryckligen anges.

Användare: individ eller system som nyttjar informationstillgångar.

Information: innebörd i data.

Informationshantering (inom ramen för LIS vid Karlstads universitet): insamling, behandling, lagring och överföring av information så att informationen kan användas på ett ändamålsenligt och kontrollerat sätt.

Informationssäkerhet: bevarandet av konfidentialitet, riktighet och tillgänglighet hos information.

Informationstillgång: all information som är av värde för en organisation.

Konsekvens: resultat av en händelse.

Risk: osäkerhetens effekt på mål.

Riskanalys: process för att förstå riskens natur och för att avgöra risknivån.

Risknivå: storlek på en risk eller kombination av risker, uttryckt som en kombination av konsekvenser och deras sannolikhet.

Sannolikhet: chans att något inträffar.

Säkerhetsåtgärd: åtgärd som förändrar en risk. Säkerhetsåtgärder inkluderar varje process, policy, utrustning, praxis eller annan åtgärd som förändrar en risk.

4 Informationsklassning

Informationsklassning är en central aktivitet i informationssäkerhetsarbetet och har till syfte att bedöma informationens behov av skydd och ska genomföras på alla informationstillgångar inom Karlstads universitet. Ansvaret att initiera informationsklassningen ligger som huvudregel på informationsägaren.

---

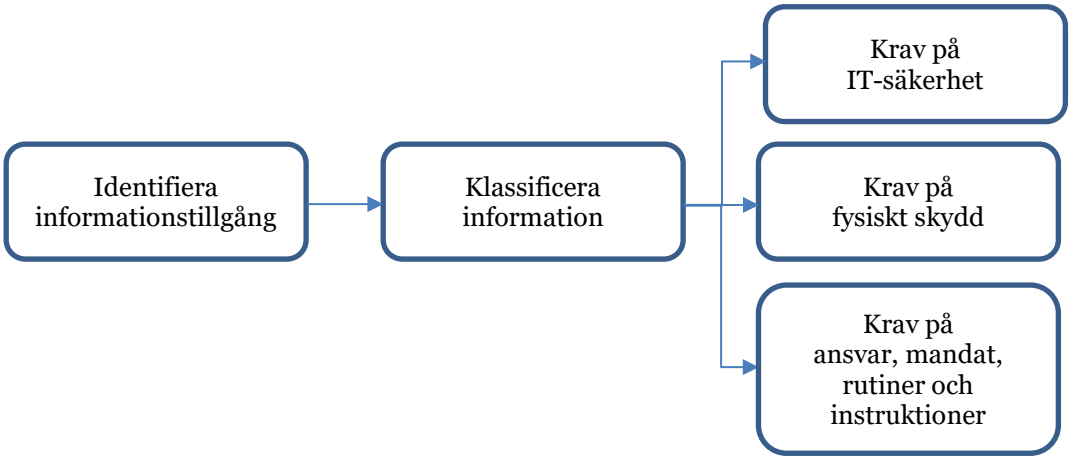
[1] Se Riktlinjer för ansvar och roller i LIS.

[2] Termer, definitioner och förklaringar är återgivna ur SIS Tekniska rapport, Terminologi för informationssäkerhet, utgåva 1, med vederbörligt tillstånd från SIS Förlag AB.

Bedömningen sker både utifrån den egna verksamhetens behov och utifrån myndighetens krav samt externa krav. Avsikten är att varje informationstillgång ska omges med rätt skydd.

Informationsklassningen är en process, se Figur 1, som innebär en kravställning på säkerhetsåtgärder från verksamheten till interna och externa leverantörer av IT-system, samt av resurser som lokaler och annan utrustning som påverkar informationshanteringen. Klassningen innebär även krav på användare av informationstillgångar.

Informationsklassning ska ses som en form av riskanalys som gäller specifika informationstillgångar. Klassningen ska ske utifrån en fastställd modell som omfattar en värdering av vilka negativa konsekvenser som kan bli resultatet om inte tillräckligt skydd upprätthålls kring olika informationstillgångar.



Figur 1, Processbeskrivning av informationsklassning

4.1 När informationsklassning ska genomföras

Informationsklassning ska ske beträffande alla informationstillgångar som inte har genomgått informationsklassning.

Informationsklassning ska som ett minimum även genomföras vid:

- Organisations- eller processförändringar som påtagligt kan påverka informationsbehandlingen
- Förändrade interna säkerhetskrav, eller förändrade externa säkerhetskrav (till exempel genom lagar, föreskrifter, eller krav från samarbetsparter), som påtagligt kan påverka informationsbehandlingen
- Tekniska förändringar som påtagligt kan påverka informationsbehandlingen, till exempel etablering av nya IT-system, eller outsourcing av funktioner eller IT-system

4.2 Klassificera information

Klassificeringen av informationen bestäms utifrån det värde den har för Karlstads universitet och vilka krav på skydd som ställs utifrån följande begrepp:

- Konfidentialitet[3], skydd mot obehörig insyn
- Riktighet, skydd mot oönskad förändring
- Tillgänglighet, åtkomst för behörig person vid rätt tillfälle
- Spårbarhet, entydig härledning av utförda aktiviteter till en identifierad användare

Ett metodstöd hjälper Karlstads universitet att värdera myndighetens information på ett enhetligt sätt utifrån interna och externa krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Ansvaret för att ta fram och regelbundet uppdatera ett metodstöd för informationsklassning ligger hos Informationshanteringsrådet på Karlstads universitet.

5 Säkerhetsåtgärder

För att nå syftet med informationsklassningen, nämligen att informationstillgången ska skyddas, behöver en kontroll göras för att säkerställa att tillräckliga säkerhetsåtgärder är vidtagna.

Säkerhetsåtgärderna ska vara baserade på bland annat den internationella standarden (ISO/IEC 27002), föreskrifter från Riksarkivets och MSB, samt externa krav (till exempel krav från samarbetsparter). Vissa av dem kan ses om en del av styrningen av informationssäkerhetsarbetet medan andra är konkreta åtgärder för att ge skydd i hantering av information.

En säkerhetsåtgärd kan vara:

- **Organisatorisk**: att man fördelar ansvar, roller och mandat i organisationen så att informationen skyddas mot felaktig hantering (vem gör vad för att undvika att saker hamnar mellan stolarna)
- **Administrativ**: att man skapar styrdokument, rutiner eller liknande samt genomför utbildningar som stöd för säker informationshantering
- **Fysisk**: att ha lås, larm, dörrar, fönster och motsvarande som skyddar information och informationssystem mot obehörig fysisk åtkomst
- **IT-teknisk**: att olika IT-lösningar används för att skydda informationen, till exempel antivirus, behörighetssystem, säkerhetsloggning och säkerhetskopiering

Olika säkerhetsåtgärder behöver ofta kombineras för att ge tillräckligt skydd. Exempelvis kan man behöva kombinera utbildning (administrativ säkerhetsåtgärd) kring till exempel nätfiske via e-post med att införa skydd mot skadlig kod (IT-teknisk säkerhetsåtgärd) som kan upptäcka och minska konsekvenserna av attacken om någon ändå skulle klicka på en skadlig länk.

---

[3] Observera att konfidentialitet ska ses i vidare perspektiv och inte tolkas som synonymt med sekretess i offentlighets- och sekretesslagens mening.

En säkerhetsåtgärd kan skydda mot brister i alla tre aspekterna (konfidentialitet, riktighet och tillgänglighet) medan andra åtgärder skyddar mot brist i en eller två av aspekterna.

5.1 Administrativa och organisatoriska säkerhetsåtgärder

Administrativa och organisatoriska säkerhetsåtgärder är de säkerhetsåtgärder som vidtas i form av rutiner, instruktioner och beslut för att Karlstads universitets medarbetare ska kunna hantera olika typer av information korrekt i sitt dagliga arbete.

Det är som huvudregel informationsägaren som behöver säkerställa att nödvändiga administrativa och organisatoriska säkerhetsåtgärderna tas fram och uppdateras vid behov.

5.2 Skyddsnivåer

Skyddsnivåer står här för IT-tekniska och fysiska säkerhetsåtgärder som sammanförts till olika nivåer för att motsvara de krav som ställs vid klassningen av informationen.

Syftet med att samla säkerhetsåtgärder i IT-tekniska och fysiska skyddsnivåer är att underlätta förvaltning av säkerhetsåtgärderna. Skyddsnivåerna underlättar för universitet att hitta de åtgärder som redan är godkända, istället för att behöva föreslå nya säkerhetsåtgärder för att ge tillräckligt skydd vid varje ny informationshantering. Universitets resurser kommer kunna användas mer effektivt om inte varje ny informationshantering resulterar i nya säkerhetsåtgärder som behöver godkännas och förvaltas.

Ansvaret för att ta fram och regelbundet uppdatera utformningen av skyddsnivåer (inklusive relevanta driftsrutiner) ligger hos IT-chefen respektive säkerhetschefen. Skyddsnivåerna ska också användas i avtal med utomstående leverantörer av system/tjänster, IT-drift och lokaler.

6 Riskhantering

I vissa fall kan det i klassningen uppkomma frågeställningar som kräver en djupare analys innan ställningstagande kan göras om vilka säkerhetsåtgärder som är lämpliga. Ett exempel är om behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Fördjupade analyser ska göras enligt Karlstads universitets fastställda metoder för riskhantering inom LIS respektive konsekvensbedömningar avseende dataskydd.

7 Ansvar

Informationsägare är ansvariga för att säkerställa att informationsklassning och val av adekvata säkerhetsåtgärder genomförs inom deras ansvarsområde.

8 Stöd

Informationssäkerhetsanvarig är ett stöd till verksamheten vid informationsklassningen och framtagande av skyddsnivåer.