REKTORS KANSLI

2023-03-13 Dnr C2023/269

Riktlinjer för kontinuitetshantering i ledningssystem för informationssäkerhet (LIS) vid Karlstads universitet

Syfte

Riktlinjernas syfte är att beskriva hur Karlstads universitet säkerställer tillgång till verksamhetskritisk information och funktion. Riktlinjerna är framtagna för att stödja verksamheten att uppfylla kraven i MSB:s föreskrift om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

MSB:s metodstöd för kontinuitetshantering 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 44/23	Dnr:	C2023/269	Ersätter:	-	Dnr:	-
Giltighet fr.o.m:	2023-03-13	t.o.m:	Tills vidare	Handläggare:	Niklas Nikitin		

1 Inledning

Kontinuitetshantering handlar om att upprätthålla Karlstads universitets verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för.

Med kontinuitetshantering avses den planering som behövs för att minimera de negativa effekter som kan bli resultatet av olika typer av avbrott i tillgång till informationen. Avbrotten kan vara av olika karaktär, allt från mindre störningar till katastroftillstånd.

Avsikten med planeringen är att upprätthålla för Karlstads universitet kritiska verksamhetsprocesser och, så snabbt som möjligt efter ett avbrott, återgå till normalläge med korrekt och fullständig information.

2 Omfattning

Dessa riktlinjer gäller för all hantering av Karlstads universitets informationstillgångar med höga krav på tillgänglighet oavsett var eller i vilken form hanteringen sker.

3 Definitioner

Definitionerna nedan kommer från SIS-TR 50:2015[1] eller SS-ISO/IEC 27000:2020 om inte annat uttryckligen anges.

Hot: möjlig, oönskad händelse med negativa konsekvenser för verksamheten.

Händelse: förekomst eller förändring av särskilda omständigheter.

Incident: enskild eller flera oönskade eller oväntade händelser som har negativa konsekvenser för verksamheten.

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

Konsekvens: resultat av en händelse med negativ inverkan.

Konsekvensanalys: process för analys av verksamhet och den effekt som ett avbrott skulle kunna ha på verksamheten.

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.

Risk: produkten av konsekvens och sannolikhet för att ett hot realiseras.

Sannolikhet: ett mått på hur troligt det är att ett hot realiseras.

Störning: incident, som kan vara förutsedd eller oförutsedd, som orsakar en oplanerad, negativ avvikelse från den förväntade leveransen av produkter och tjänster i enlighet med en organisations mål[2].

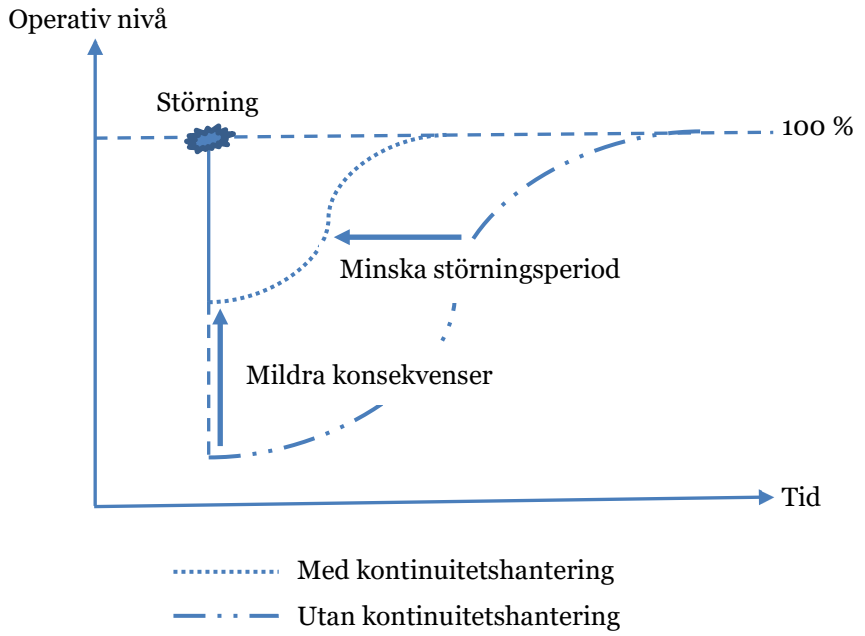
---

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

[2] Definierat i MSB:s metodstöd för kontinuitetshantering.

4 Arbetet med kontinuitetshantering

Kontinuitetshantering handlar om att planera för att upprätthålla Karlstads universitets verksamhet på en tolerabel, det vill säga för myndigheten acceptabel, nivå oavsett vilken störning den utsätts för. Med kontinuitetshantering kan myndigheten snabbare återhämta sig från och mildra konsekvenserna av en inträffad händelse, se Figur 1. Det innebär kortare störningsperioder i verksamheten och förhindrar att personella, ekonomiska, funktionella och informationsrelaterade värden går förlorade.



Figur 1, Kontinuitetshanteringens två syften

Inom ramen för verksamhetens arbete med kontinuitetshantering ska Karlstads universitet kritiska verksamhetsprocesser och krav på kontinuitet för dessa identifieras. Därefter ska organisationen identifiera vilka informationstillgångar som krävs för att de verksamhetskritiska processerna ska fungera som avsett. Även beroenden till nyckelpersoner för att upprätthålla verksamheten ska identifieras och dokumenteras i detta arbete.

Arbetet ska generera en kravspecifikation för verksamhetsprocesserna, som definierar krav på återstartstider samt maximal toleranstid för förlust av data vid ett avbrott. Att definiera krav på återstartstid innebär den maximala tid som en aktuell process tillåts vara otillgänglig.

Kravspecifikationen ska sedan utgöra underlag för vilka kontinuitetslösningar som väljs och hur reservrutiner ska utformas.

Kontinuitetshanteringen ur informationssäkerhetssynpunkt innehåller två delar. En del är verksamhetens kontinuitetsplan. Den andra delen är den avbrottsplan som IT-levererande part och övriga teknikresursägare ska ha och som ska svara mot verksamhetens ställda krav.

Informationshanteringsrådet på Karlstads universitet ska som stöd till arbete med myndighetens kontinuitetshantering ta fram och regelbundet uppdatera metodstöd

för hur kontinuitetsplaner upprättas. IT-chefen på Karlstads universitet ska som stöd till arbete med myndighetens kontinuitetshantering ta fram och regelbundet uppdatera mallar för hur avbrottplanerna upprättas.

Planerna ska finnas tillgängliga i olika format, för att säkra åtkomst vid händelse av störning. Planerna ska även förvaras skyddat enligt den informationsklassning planerna har, så att inte känslig information blir åtkomlig för obehöriga.

Verksamhetens olika kontinuitetsplaner ska fortlöpande stämmas av med myndighetens krishanteringsplan, för att säkerställa att dessa fungerar effektivt tillsammans. Genom krisövningar kontrolleras planernas aktualitet och användbarhet för krisledningsorganisationen.

5 Ansvar

Informationsägare[3] ska, som grund för kravställning mot systemägare[3] och teknikresursägare[3], identifiera för Karlstads universitet kritiska verksamhetsområden och informationsprocesser. Syftet är att i samband med störningar och krissituationer kunna prioritera och säkerställa för Karlstads universitet kritisk funktionalitet. Informationsägaren ansvarar också för att kontinuitets- och avbrottsplan harmoniserar med varandra, samt att kontinuitetsplanerna regelbundet testas/övas, utvärderas och revideras.

Systemägare och teknikresursägare ansvarar för att upprätta avbrottsplaner, som tar sin utgångspunkt ifrån informationsägarens prioritering och informationsklassning, samt att avbrottsplanerna regelbundet utvärderas och revideras.

6 Stöd

Informationssäkerhetsanvarig är ett stöd till verksamheten vid kontinuitetshantering.

3 Se Riktlinjer för ansvar och roller i LIS.