Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT SLU ID: SLU ua.2019.2.10-2681

Sakområde: Säkerhet och informationssäkerhet

Dokumenttyp: Anvisning/Instruktion	Beslutsdatum: 2019-07-01
Beslutsfattare: Säkerhetschef Johan Sjöblom	Träder i kraft: 2019-07-01
Avdelning/kansli: Säkerhetsenheten	Giltighetstid: [20ÅÅ-MM-DD]
Handläggare: Informationssäkerhetsstrateg Christian Nähl	Bör uppdateras före: 2022-07-01

Ev dokument som upphävs:

Bilaga till:

Anvisning för kontinuitetsplanering ur ett informationssäkerhetsperspektiv

Syfte och målgrupp

Det huvudsakliga målet med kontinuitetsplanering för SLU:s olika verksamheter är att säkerställa att eventuella avbrott i tillgången till information inte får allvarliga konsekvenser. Det innebär att det måste finnas en plan för att säkerställa att verksamheten kan fortsätta och återgå till normalläget inom en acceptabel tidsrymd.

I Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) står i 11§ att myndigheten ska ha rutiner för kontinuitetshantering som tydliggör hur verksamheten informationshantering upprättshål vid större störningar och avbrott.

Den som äger informationen ansvarar för att kontinuitetsplan görs. Ägaren kan vara systemägare, informationsägare, chef eller annan person.

En viktig del i kontinuitetsplanering är att minska personberoendet så att fler kan åtgärda eventuellt avbrott.

Omfattning

All verksamhet och de IT-system som är kritiska för verksamhetens förmåga **ska** kontinuitetsplaneras för att säkerhetsställa att ett avbrott skyndsamt kan åtgärdas.

Ansvar

I en kontinuitetsplan är det viktigt att fastställa ansvarsfördelning och vem som ska göra vad vid ett eventuellt avbrott. Alla berörda parter ska veta hur, när och vilka åtgärder som ska vidtas när ett avbrott inträffar så att konsekvensen för verksamheten blir så liten som möjligt, både under och efter avbrottet.

Det är systemägaren, informationsägaren eller annan person som ansvarar för informationens tillgänglighet som ansvarar för kontinuitetsplaneringen. Om den är väsentlig för att SLU:s verksamhet ska kunna fortgå vid ett avbrott bör kontinuitetsplanen rapporteras till säkerhetsenheten.

Innehåll

I kontinuitetsplanen ska det tydligt framgå vad den berör. Planen ska beslutas av den ansvariga informationsägaren.

En riskanalys ska genomföras vid informationstillgångens införande och därefter uppdateras efter behov. I riskanalysen ska det ingå en konsekvensanalys med fokus på bristande tillgänglighet till kritisk information. Den analysen används sedan för att identifiera verksamhetens behov av och krav på tillgänglighet.

Konsekvensanalysen används även för att definiera kritiska återstartstider för verksamheten, till exempel den maximala tid som en verksamhet tillåts vara otillgänglig.

Använd med fördel säkerhetsenhetens mall för kontinuitetsplanering. Beskriv konsekvensen av varje identifierad risk och vilken åtgärd som ska vidtas. Åtgärderna ska utformas så att de är praktiskt och ekonomiskt genomförbara.

När kontinuitetsplanen är klar ska informationsägaren informeras och godkänna den.

Granskning och övning

En förutsättning för att medarbetarna ska våga lita på kontinuitetsplanen är att man i så stor utsträckning som möjligt granskar och övar dem. Övningsfrekvensen måste anpassas dels till risknivån, dels till kostnaden för att genomföra övningen. Det är inte alltid nödvändigt med skarpa övningar. Om det går bör man försöka lägga in övningsmoment i de normala driftrutinerna.

Utvärdera och uppdatera

För att en kontinuitetsplan ska vara användbar när den faktiskt behövs bör den uppdateras regelbundet och finnas tillgänglig både digitalt och i pappersform.

Risker, konsekvens, åtgärder, ägare och förvaltare kan förändras med tiden. Planen ska därför uppdateras en gång per år och vara en del av den normala driften.