Gäller för: Västra Götalandsregionen
Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2025-01-30
Giltig till: 2029-12-31

Kontinuitetshantering av IS/IT-tjänst

Regional rutin 2025–2029

Ledningssystem för informationssäkerhet och dataskydd

Rubrik: Kontinuitetshantering av IS_IT-tjänst - Regional rutin 2024 -2028
Dokument-ID: RS10162-1596316381-279
Version: 1.0

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

1 Inledning 3
2 Omfattning 4
3 Termer och begrepp 4
4 Ansvar och roller 5
4.1 Ägare av IS/IT-tjänst 5
4.2 Informationsägare 5
4.3 Regional processägare 5
5 Kontinuitetshantering av IS/IT-tjänst 5
5.1 När ska en kontinuitetsplan tas fram? 6
5.2 Vad ska en kontinuitetsplan innehålla? 6
5.3 Riskhantering 7
5.4 Incidenthantering 7
5.5 Testning, övning och utvärdering 8
5.6 Kommunikation och medvetenhet 8
5.7 Dokumentation 8
6 Relaterade dokument 8

1 Inledning

Mål: Det ska finnas kontinuitetshantering för att säkerställa tillgång till information, IS/IT-tjänster och funktioner som krävs för att upprätthålla av ledningen prioriterad verksamhet. Planeringen ska regelbundet testas och uppdateras.

Kontinuitetshantering är en förutsättning för upprätthållande av informationssäkerhet vid störning[1]. Genom att upprätthålla beredskapsplanering och verksamhetskontinuitet kan organisationens mål med informationssäkerhet fortsatt nås vid störning.

Kontinuitetshantering av IS/IT-tjänster är en central del i den övergripande kontinuitetshanteringen och informationssäkerheten, för att säkerställa att organisationens mål fortsatt kan nås vid störning.

Kontinuitetshantering av IS/IT-tjänst innebär att upprätta och tillämpa plan för kontinuerlig leverans och hantering vid avbrott eller störning gällande delar av IT-miljö eller IS/IT-tjänst som av verksamheten bedöms vara kritiska i och med att de används för att tillhandahålla samhällsviktiga tjänster alternativt omfattas av höga krav på tillgänglighet.

Denna regionala rutin anger hur kontinuitetshantering av IS/IT-tjänst ska ske. Rutinen är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD).

Rutinen utgör ett komplement till den övergripande regionala riktlinjen Kontinuitet - Regional riktlinje 2023 – 2027 som anger enligt vilken modell kontinuitetsarbetet ska bedrivas och vilka krav som ställs på förvaltningar och majoritetsägda bolag inom området.

Kontinuitetshantering av IS/IT-tjänst ska utgå från och svara upp till gällande informationsklassning, främst nivå av tillgänglighet, för de informationstillgångar som berörs.

[1] Säkerhetsåtgärd 5.29 (SS-ISO/IEC 27002:2022).

2 Omfattning

Rutinen gäller för IS/IT-tjänster bestående av IT-system, nätverk, applikationer och/eller tekniska resurser vilka är en del av VGR:s IT-miljö, inklusive IS/IT-tjänst bestående av resurser från extern IT-miljö som används av VGR.

Rutinen tillämpas kontinuerligt under förvaltning och avtalsvård av IS/IT-tjänst, nätverk, applikationer och tekniska resurser. Vid upphandling, utveckling och införande ska det säkerställas att krav för kontinuitetshantering motsvarande regional rutin finns med.

Rutinen omfattar säkerhetsåtgärder för avsnitt 5.29 Informationssäkerhet vid störning, 5.30 Kontinuitetsberedskap inom IKT samt 8.14 Redundans för informationsbehandlingsresurser i SS-EN ISO/IEC 27002:2022.

3 Termer och begrepp

Huvuddelen av termer och begrepp är hämtade från MSB termbank för informationssäkerhet, Kontinuitetshantering (msb.se) och *Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027* (RS 2023-02811)[3].

Driftskontinuitet	Konfiguration, övervakning, underhåll och administration av hårdvara, programvara och nätverk för att säkerställa kontinuerlig drift av IS/IT-tjänst.
IS/IT-tjänst	Är en avgränsning av en eller flera digitala informationsbehandlingsresurser. Exempelvis IT-system, applikation, mjukvara, nätverk, lagringssystem eller infrastruktur.
Kontinuitet för informationssäkerhet	Processer och rutiner som säkerställer att informationssäkerheten upprätthålls
Kontinuitetshantering	Innebär att planera för att upprätthålla sin verksamhet på en tolerabel nivå när den utsätts för en störning.
Kontinuitetshantering av IS/IT-tjänst	Innebär att planera för, förebygga och hantera störningar så att tillgängligheten kan upprätthållas.
Kontinuitetsplan	En kontinuitetsplan för IS/IT-tjänst innehåller plan för förebyggande åtgärder och åtgärder vid en störning så att alla vet

	vad som ska göras. Kallades tidigare avbrottsplan. Kallas i ISO 27002 IKT-kontinuitetsplan.
Redundans	Tillstånd då mer än ett medel finns för att upprätthålla ett givet funktionssätt syftande till att säkerställa kontinuerlig drift och därigenom öka feltoleransen. Dubbel eller flerfaldig uppsättning av viktiga komponenter för att IS/IT-tjänst ska fungera även om något slutar fungera.

4 Ansvar och roller

4.1 Ägare av IS/IT-tjänst

Ägare av IS/IT-tjänst ansvarar för att säkra kraven på kontinuitet i sin tjänst utifrån de krav som verksamheten har. Ägare av IS/IT-tjänst ansvarar för att kontinuitetsplan för IS/IT-tjänst tas fram.

4.2 Informationsägare

Informationsägare ansvarar för att kravställa på tillgänglighet och kontinuitetshantering av IS/IT-tjänst.

Informationsägare ansvarar för att verksamhetens kontinuitetsplan och kontinuitetshantering av berörda IS/IT-tjänster harmoniserar med varandra.

4.3 Regional processägare

För regionala processer företräder regional processägare informationsägare och ansvarar för att kravställa på tillgänglighet och kontinuitetshantering av regionala IS/IT-tjänster.

5 Kontinuitetshantering av IS/IT-tjänst

Kontinuitetshantering av IS/IT-tjänst innebär att planera för, förebygga och hantera störningar så att tillgängligheten kan upprätthållas. Hur långt man ska gå i kontinuitetshantering av respektive tjänst avgörs av verksamhetens krav uttryckta som tillgänglighet i informationsklassningen samt om IS/IT-tjänsten ingår som förutsättning för upprätthållande av en samhällsviktig verksamhet.

Kontinuitet för verksamhet styrs av Kontinuitet - Regional riktlinje 2023 – 2027.

5.1 När ska en kontinuitetsplan tas fram?

Med kontinuitetsplanering avses den planering som behövs för att minimera de negativa effekter som kan bli resultatet av olika typer av avbrott i tillgång till informationen.

En kontinuitetsplan ska utvecklas och upprätthållas för varje IS/IT-tjänst där verksamheten kravställer och prioriterar kontinuitet. Minst de delar av IT-miljö som hanterar information med konsekvensnivå allvarlig (3) för tillgänglighet alternativt används för att tillhandahålla samhällsviktiga tjänster, enligt NIS-direktivet och §14 i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, ska omfattas fullt ut av rutinen. Kontinuitetsplan ska finnas innan installation eller ändringshantering av IS/IT-tjänsten enligt Change Management.

5.2 Vad ska en kontinuitetsplan innehålla?

Kontinuitetsplanen utgår från konsekvensanalys som genomförs inom ramen för verksamhetens kontinuitetshantering samt informationsklassningens krav på tillgänglighet. För verksamhetens kontinuitet ansvarar ytterst förvaltnings- eller bolagschef i enlighet med Kontinuitet - Regional riktlinje 2023 – 2027.

Förvaltningar och bolag ska enligt Kontinuitet - Regional riktlinje 2023 – 2027 identifiera sin lägsta nivå av riskacceptans och maximal tolerabel avbrottstid (MTA). Tillsammans med informationsklassning utgör de underlag för plan för kontinuitetshantering av IS/IT-tjänst.

Ägare IS/IT-tjänst ansvarar för att kontinuitetsplan för IS/IT-tjänst tas fram. Planen ska inkludera förebyggande åtgärder utifrån risk, incidenthantering, arbetsrutiner och mål för återställning och återgång samt kontaktlista för kommunikation och beslut. Planen omfattar åtgärder runt driftskontinuitet, redundans, backup och reservkapacitet som implementeras i syfte att minska störningar och säkerställa klassad nivå av tillgänglighet. Planen ska hänvisa till verksamheternas MTA och informationsklassning. Planen bör uttrycka Recovery Time Objective (RTO), som innebär maxtid för återställning av IS/IT-tjänst efter avbrott, och Recovery Point Objective (RPO), som

uttrycker hur långt tillbaka data maximalt får förloras vid avbrott av IS/IT-tjänsten.

Planen ska omfatta upprätthållande av informationssäkerhet under störning genom tillämpning av ISO/IEC 27002, avsnitt 2.29 och åtgärder för redundans ska säkerställa tillämpning av ISO/IEC 27002, avsnitt 8.14.

5.2.1 Återställning och återgång

Det ska i kontinuitetsplan för IS/IT-tjänst finnas utarbetade planer för hur IS/IT-tjänst återställs efter avbrott. Roller och ansvar, återställningstid och rutin för återställning ska vara tydligt definierade för att genomföra återställning och verifiera återgång till normalläge.

5.3 Riskhantering

Kontinuerlig riskhantering och sårbarhetshantering ska ske enligt respektive regional rutin för att identifiera potentiella hot och sårbarheter i IT-infrastrukturen, vilka kan påverka kontinuerlig drift. Se Regional rutin riskhantering för informationssäkerhet 2024 – 2028 samt Regional rutin för hantering av sårbarheter i IT-miljö 2024 – 2028. Resultatet ska användas för att prioritera och justera åtgärder i kontinuitetsplanen för att minska riskerna.

5.4 Incidenthantering

Incidenthantering ska ske enligt regional rutin incidenthantering.

Ägare IS/IT-tjänst ansvarar för att kontinuitetsplaner löpande förbättras när ny kunskap tillkommer. Kontinuitetplaner ska uppdateras regelbundet eller vid incidenter som har eller kan få en avsevärd påverkan på kontinuitet i IS/IT-tjänst. Sådana incidenter måste också rapporteras enligt lag för verksamheter som omfattas, till exempel hälso- och sjukvård genom lag (NIS2-direktivet) och direktivet om kritiska entiteters motståndskraft (CER-direktivet). Incidenter med IS/IT tjänster som är medicintekniska produkter eller som påverkar medicintekniska produkter måste bedömas om de också ska anmälas till tillverkaren och Läkemedelsverket som en händelse eller tillbud med en medicinteknisk produkt (HSLF-FS 20221:52).

Koncernstab digitalisering (KSD) ska följa gällande incidenthanteringsprocess för att rapportera, utreda och hantera störningar och incidenter som kan påverka IS/IT-tjänster. Det

säkerställer en tydlig och koordinerad respons vid störningar enligt kontinuitetsplan.

5.5 Testning, övning och utvärdering

Ägare IS/IT-tjänst ansvarar för att det minst årligen utförs periodisk översyn och utvärdering av kontinuitetshanteringen av IS/IT-tjänst. Kontinuitetsplaner för IS/IT-tjänster ska testas och övas regelbundet. Tester som kan komma att påverka systemets tillgänglighet, även vid korta avbrott, måste planeras med verksamheterna som använder IS/IT-tjänsten. Resultatet av översyn och tester ska användas för att identifiera brister och förbättra kontinuitetsplanerna.

5.6 Kommunikation och medvetenhet

Digitaliseringsdirektör ansvarar för att berörd KSD-personal informeras och utbildas om sitt ansvar för kontinuitetshanteringen av IS/IT-tjänst. Alla berörda ska vara medvetna om sina roller och ansvar för kontinuitetshantering samt var dokumentation kan hittas.

5.7 Dokumentation

Alla kontinuitetsplaner, incidentrapporter, testresultat och återhämtningsaktiviteter kopplat till IS/IT-tjänsten ska dokumenteras enligt överenskomna dokumentmallar och förvaras för spårbarhet och revisionsspårning. Respektive ägare av IS/IT-tjänst, motsvarande systemägare och produktansvarig, ansvarar för att detta sker. Informationen ska hanteras enligt myndighetens informationshanteringsplan.

6 Relaterade dokument

Styrdokument som relaterar till regional rutin för kontinuitetshantering av IS/IT-tjänst.

Informationssäkerhet och dataskydd - Regional riktlinje 2023 - 2027

Kontinuitet - Regional riktlinje 2023 – 2027

Regional rutin för hantering av sårbarheter i IT-miljö 2024 – 2028

Regional rutin för incidenthantering 2024 – 2028

Regional rutin riskhantering för informationssäkerhet 2024 – 2028

Regional rutin för säker drift 2024 – 2028

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-279

Version: 1.0

Giltig från: 2025-01-30

Giltig till: 2029-12-31