Beredskapsplan for #Regnskapsførervirksomheten etter God Regnskapsføringsskikk pkt. 2.8.5 IT-sikkerhet

Versjonsnummer:	#.#	
Oppdatert dato:	##.##.####	
Ansvarlig for vedlikehold av planen:	Navn: Telefon: Epost:	# # #

Beskrivelse av beredskapsløsningen for vesentlige driftsavbrudd:

Denne planen beskriver roller og ansvar hvis det oppstår et alvorlig driftsavbrudd på IT hos virksomheten. Planen gjøres kjent for alle ansatte og relevante eksterne.

Formålet med denne beredskapsplanen er å sikre tilgjengelighet og integritet av data etter et alvorlig driftsavbrudd. Dette innebærer at data i tilknytning til regnskapsoppdraget skal kunne gjenopprettes med samme kvalitet som opprinnelig innen en akseptabel tid. Løsningen er tilpasset regnskapsvirksomhetens størrelse og kompleksitet og kundenes forventninger til egen tilgang og tidsfrister. Planen identifiserer hendelser og tiltak, og angir ansvarlig, hvem som skal varsles og hvilke frister det er for gjenopprettelse.

Planen tar utgangspunkt i at ansvarlig for hendelsen eller dennes stedfortreder har fått varsel om en alvorlig situasjon som har rammet vesentlige deler av IT-systemene. Varslingsrutiner og ansvarsfordeling starter i det ansvarlig har fått melding om driftsstans, og beskriver hovedtrekkene frem til normal driftssituasjon er opprettet. Opplevelse av alvorlig driftsavbrudd er en subjektiv følelse. Det viktige med beskrivelsene nedenfor er å ha en felles og mest mulig objektiv definisjon av når varslingsrutinene skal benyttes og de videre tiltakene skal iverksettes. Tiltakene testes minst årlig.

Forebyggende tiltak vil eksempelvis være løpende sikkerhetskopiering, kryptering, viruskontroll, alternativ nettilgang, avtale om reserveutstyr og –lokaler, avbruddsforsikring og fysisk sikring av egne lokaler.

Der hvor kundene har tilgang til systemer og data, må disse varsles uten ugrunnet opphold. Videre må kunder og myndigheter varsles straks det blir klart at driftsavbruddet påvirker evnen til å rapportere innen offentlige frister.

Systemer dekket av beredskapsplanen:

Systemene som er listet her er vurdert som kritiske for virksomheten og leveransen av regnskapstjenester innen offentlige frister. Øvrige systemer er vurdert mindre kritiske og er ikke dekket av denne planen.

Systemnavn	Leverandør	Systemets funksjon i virksomheten	Driftes hos	Internt ansvarlig for systemet
[…]				

Beredskapsplan:

Hovedkategori	Hendelse	Hvem er ansvarlig og stedfortreder hos regnskaps-virksomheten?	Hvem skal varsles når hendelsen inntrer?	Hvilke tiltak skal iverksettes når hendelsen inntrer? (Eksempler)	Rekke-følge på tiltakene	Hva er akseptabel tid for gjenoppretting til normal drift?	Når er tiltaket testet og hvordan?	Vedlegg
1. Hendelser tilknyttet egne lokaler	1.1. Kontoret er (lang)varig utilgjengelig på grunn av brann eller annen fare for liv og helse.	[…]	[…]	Sikre personell og området i samråd med brannvesen eller politi. Flytte inn i reservelokaler eller bruke hjemmekontor. Opprette nytt nettverk på reservested for sentrale IT-ressurser. Skaffe erstatningsutstyr i henhold til avtale.		[…]	[…]	[…]
	1.2. Teknisk utstyr på kontor er ødelagt av vann, brann eller er stjålet.			Sikre personell og området i samråd med brannvesen eller politi. Flytte inn i reservelokaler eller bruke hjemmekontor. Opprette nytt nettverk på reservested for sentrale IT-ressurser. Skaffe erstatningsutstyr i henhold til avtale.				
	1.3. Nettverk er ikke tilgjengelig på kontoret.			Etablere midlertidig mobilt nettverk på kontoret for sentrale IT-ressurser. Nettverksleverandør kontaktes for å gjenopprette nettverket til normalt.				
	1.4. Lengre strømbrudd i bygget eller i området.			Flytte inn i reservelokaler eller bruke hjemmekontor. Opprette nytt nettverk på reservested for sentrale IT-ressurser. Igangsette nødaggregat.				
2. Hendelser på egne servere i egne lokaler	2.1. Datalagringsenhet (harddisk mv) på server er ødelagt – Datasett er ikke tilgjengelig.			Ny harddisk skaffes fra leverandør i henhold til avtale. Data gjenopprettes i fra siste sikkerhetskopi. Datasett testes for fullstendighet og dataintegritet.				

Hovedkategori	Hendelse	Hvem er ansvarlig og stedfortreder hos regnskaps-virksomheten?	Hvem skal varsles når hendelsen inntrer?	Hvilke tiltak skal iverksettes når hendelsen inntrer? (Eksempler)	Rekke-følge på tiltakene	Hva er akseptabel tid for gjenoppretting til normal drift?	Når er tiltaket testet og hvordan?	Vedlegg
	2.2. Hardwarefeil – Maskin eller operativsystem responderer ikke ved oppstart.			Ny server skaffes fra leverandør i henhold til avtale. Operativsystem, systemer og konfigurasjonsfiler installeres. Data gjenopprettes i fra sikkerhetskopi hvis eksisterende harddisk ikke kan benyttes. Datasett testes for fullstendighet og dataintegritet.				
	2.3. Virusangrep - data kan være eksponert eller korrupt			Kjør virusskanning med isolering av filer med virus. Data gjenopprettes i fra sikkerhetskopi hvis eksisterende datasett ikke kan benyttes videre. Datasett testes for fullstendighet og dataintegritet. Passord skiftes for alle brukere.				
3. Hendelser på servere hos eksterne driftsoperatører	3.1. Systemene er ikke tilgjengelig via den normale forbindelsen til operatør (linjebrudd utenfor eget lokale / nettverksutstyr).			Etablere alternativ nettverksforbindelse for å kommunisere med ekstern driftsoperatør. Etablere midlertidig mobilt nettverk på kontoret hvis reserveforbindelse heller ikke virker.				
	3.2. Alle, eller deler av, regnskapsdata er ikke tilgjengelig i systemene hos operatør.			Be om at data gjenopprettes i fra sikkerhetskopi hvis eksisterende datasett i henhold til operatør ikke kan benyttes videre. Datasett testes for fullstendighet og dataintegritet.				
4. Hendelser knyttet til oppgradering av programvare	4.1. Systemene og/eller regnskapsdata er ikke tilgjengelig etter oppgradering av programvare.			Foreta sikkerhetskopi av alle relevante datasett. Legg tilbake forrige versjon av programvare. Benytt eksisterende datasett eller legg tilbake siste				

Hovedkategori	Hendelse	Hvem er ansvarlig og stedfortreder hos regnskaps-virksomheten?	Hvem skal varsles når hendelsen inntrer?	Hvilke tiltak skal iverksettes når hendelsen inntrer? (Eksempler)	Rekke-følge på tiltakene	Hva er akseptabel tid for gjenoppretting til normal drift?	Når er tiltaket testet og hvordan?	Vedlegg
				sikkerhetskopi. Kontroller for fullstendighet og integritet i datasettet.				
5. Hendelser knyttet til personlig datautstyr (PC, nettbrett eller mobil)	5.1. Personlig datautstyr med konfidensiell regnskaps-informasjon er mistet eller stjålet.			Varsle politi og forsikrings-selskap. Kjøre «remote kill» mot utstyret. Bytte av passord for relevante brukere som har mistet utstyr. Skaffe erstatningsutstyr i henhold til avtale.				
	5.2. Personlig datautstyr med konfidensiell regnskaps-informasjon er korrupt med virus e.l.			Kjør virusskanning med isolering av filer med virus. Data gjenopprettes i fra sikkerhetskopi hvis eksisterende datasett ikke kan benyttes videre.				
6. Hendelser knyttet til portable datamedier (Transportable harddisker, minnepinne, CD, DVD mv)	6.1. Portable datamedier med konfidensiell regnskaps-informasjon er mistet eller stjålet.			Bytte av passord for relevante brukere som har mistet utstyr.				
7. Feil på sikkerhetskopi	7.1. Ved forsøk på tilbakelegging av sikkerhetskopi avdekkes det at denne er ødelagt eller mangelfull.			Fastslå siste fullstendige sikkerhetskopi. Vurder om logger kan benyttes for å komplettere siste fullstendige sikkerhetskopi. Legge sikkerhetskopi og eventuelt logger tilbake på systemet. Identifiser siste oppdateringer på kunders regnskap. Foreta ny innleggelse av bokførte opplysninger mv. for å gjenopprette situasjonen til normal oppdatering av regnskapsinformasjon. Avstem regnskapet.				
8. Hendelser på telefonsystem	8.1. Telefonsystemet er ikke tilgjengelig for kunder og andre eksterne.			Informere om alternative telefonnummer (spesifisert i vedlegg) på nettsidenes				

Hovedkategori	Hendelse	Hvem er ansvarlig og stedfortreder hos regnskaps-virksomheten?	Hvem skal varsles når hendelsen inntrer?	Hvilke tiltak skal iverksettes når hendelsen inntrer? (Eksempler)	Rekke-følge på tiltakene	Hva er akseptabel tid for gjenoppretting til normal drift?	Når er tiltaket testet og hvordan?	Vedlegg
				forside. Kontakte leverandør av telefonsystem for gjenoppretting av normalsituasjon.				