Sikt
Kunnskapssektorens tjenesteleverandør

KONTINUITETSPLAN FOR INFORMASJONSIKKERHETSHENDELSER

En veileder for universiteter, høgskoler og forskningsinstitutt

Cybersikkerhetssenteret for forskning og utdanning **eduCSC**	
Versjon	1.0 / oktober / 2023
Skrevet av	Ingrid Moen

Innholdsfortegnelse

KONTINUITETSPLAN FOR INFORMASJONSIKKERHETSHENDELSER 1
Innledning 3
1 Om kontinuitetsplan 4
1.1 Hvordan utarbeide kontinuitetsplan 4
1.2 Faser ved en hendelse 5
2 Forberedelser – workshop 5
2.2 Workshop for forankring av planen 6
3 Gjennomføring - Lag kontinuitetsplanen 8
3.1 Innhold 9
3.2 Nyttige vedlegg 10
4 Etterarbeid - Kvalitetskontroll, øvelse, revidering 10
4.1 Kvalitetskontroll 10
4.2 Øvelse, øvelse, øvelse 10
4.3 Revidering 11
4.4 Debrief etter krise eller øvelse 11
4.5 Lagring av planen 12
Referanser 13
Grunnlag for utarbeiding av veilederen 13
Relaterte veiledere og anbefalinger 13

Eventuelle uklarheter i innholdet kan meldes inn til kontakt@sikt.no.

Vi håper veilederen er til nytte!

Cybersikkerhetssenteret for forskning og utdanning, eduCSC

Sikt – Kunnskapssektorens tjenesteleverandør

Innledning

Det finnes flere rammeverk, standarder og anbefalinger som omhandler kontinuitetshåndtering, og som beskriver hva en kontinuitetsplan er og hva den bør inneholde. Målet med denne veilederen er å klargjøre rammene til kunnskapssektoren med fokus på informasjonssikkerhet og hjelpe virksomhetene i arbeidet med å lage sine egne kontinuitetsplaner.

Informasjonssikkerhetshendelser omfatter typisk hendelser som kan påvirke tilgjengelighet, integritet og konfidensialitet og dekker både villede og ikke-villede hendelser fra brann, ulykker, feil etter planlagte endringer til målrettede cyberangrep, sabotasje eller tyveri av data/informasjon.

Kontinuitet handler om å kunne opprettholde aktivitet til tross for en uønsket hendelse, og å sørge for at verdiskapingen i et system, en tjeneste eller en arbeidsprosess holdes i gang.

Kunnskapsdepartementet stiller krav om at underliggende virksomheter jobber helhetlig og systematisk med sikkerhet og beredskap[1], og de fastslår at de skal:

- Etablere planer for hvordan kritiske arbeidsoppgaver kan utføres ved langvarig bortfall av viktige digitale systemer, tjenester eller datanettverk.
- Fastsette egne krav til kontinuitet og sikre tilstrekkelige ressurser til dette arbeidet.[2]

Om veilederen

Veilederen omhandler hva en kontinuitetsplan er, hvordan den kan utarbeides, råd og anbefalinger rundt workshops i forkant, oppsett av planen og etterarbeid/videre arbeid Til slutt i veilederen finner dere en liste over standarder og planverk som vi har brukt som utgangpunkt og inspirasjon til veilederen, og som dere også kan ha god nytte av.

Målgrupper

Veilederen retter seg spesielt mot ansatte som har ansvar for at informasjonssikkerheten blir ivaretatt dersom en hendelse inntreffer. Det kan være CISO (informasjons-sikkerhetsansvarlig), IT-ansatte, IRT-leder eller tilsvarende. I tillegg kan øvrig ledelse i virksomheten også dra nytte av veilederen i forbindelse med arbeidet med planen.

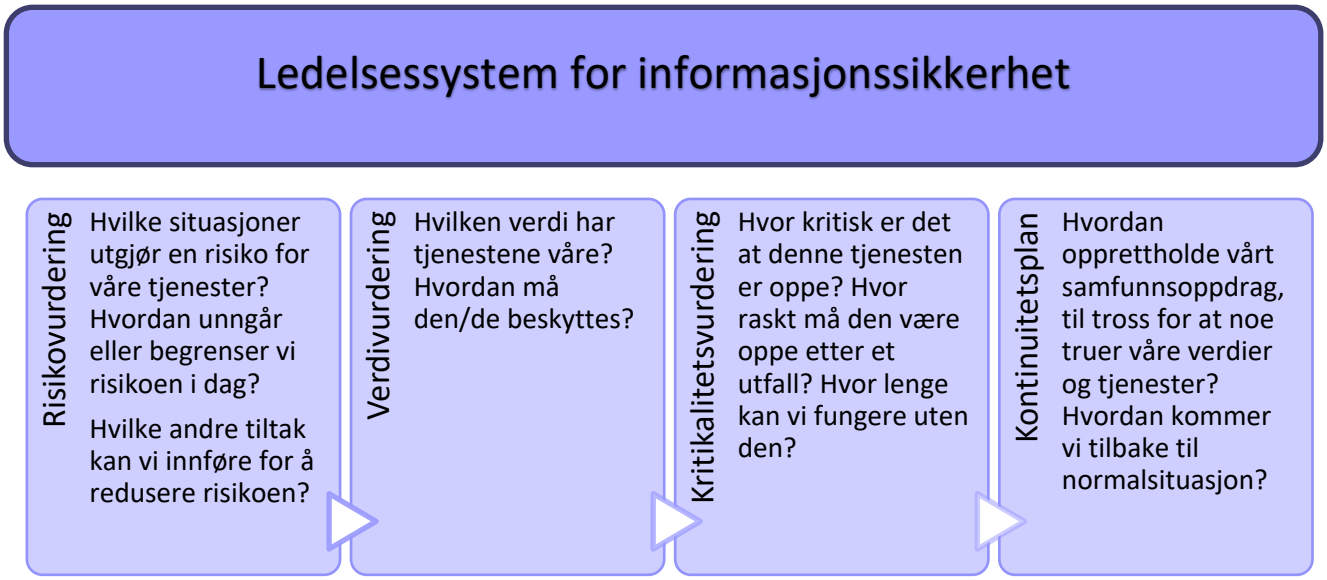
[1] Styringsdokument for arbeidet med samfunnssikkerhet og beredskaps i kunnskapssektoren
[2] Policy for informasjonssikkerhet og personvern (2020)

1 Om kontinuitetsplan

En kontinuitetsplan skal hjelpe virksomheten med å håndtere en krisesituasjon, slik at tjenesteproduksjonen kommer raskest mulig tilbake i normal drift med minimalt tap av data. Har dere planlagt for, og øvd på, ulike krisesituasjoner, kan dere umiddelbart starte arbeidet med å bygge opp igjen når noe skjer, fremfor å måtte lete etter en plan som ingen har lest i en stressende situasjon. Den skal for eksempel hjelpe dere med å håndtere virkelig store hendelser, som cyberangrep (tjenestenekt, løsepengevirus), brann på serverrom, langvarig sykdom på kritisk personell, terroraksjoner, og lignende, mens «normale» avvik og nedetider innenfor akseptable tidsperioder ikke vil favnes av planen.

1.1 Hvordan utarbeide kontinuitetsplan

En kontinuitetsplan bygger gjerne på verdivurderinger, kritikalitetsvurderinger og risikovurderinger som er gjort for virksomheten og tjenestene. De gir dere oversikt over hva som er viktigst for dere og hvilke sårbarheter de har.



I tillegg til oversikt over sårbarheter, vil en risikovurdering kunne identifisere *restrisikoen*. Restrisiko er det som gjenstår, selv om tiltak iverksettes, og den kan heller ikke på en enkel måte elimineres. Hendelser som involverer restrisiko, vil typisk føre til at kontinuitetsplanen aktiveres. Når alle skadebegrensende tiltak er nytteløse, og dere ikke enkelt eller kjapt kan komme dere tilbake til en normalsituasjon, må dere tenke alternative former for ivaretakelse av driften. De mest kritiske og sårbare tjenestene, er gjerne det man sikrer først. Spesielt viktig er tjenester som har nasjonal interesse, eller som andre tjenester er avhengige av for å fungere.

1.2 Faser ved en hendelse

Aktivering og varslingsfasen
Noe har skjedd og man må iverksette planen for å opprettholde kontinuitet i virksomheten. Herunder finne ut skadeomfang, varsle de som skal være med i gjenopprettingsarbeidet, og aktivere kontinuitetsplanen. Dette må ses i sammenheng med beredskapsplanen til virksomheten. Dere må definere kriteriene som trigger at planen aktiveres. Kriteriene bør være konkrete og konsise, basert på hva som er smertegrensen til det planen omhandler.

Gjenoppbyggingsfasen
I denne fasen handler det om å få oversikt over skadeomfanget og få systemer og tjenester opp og gå igjen (basert på kritikalitetsvurderingen). Sørg for å ha oversikt over hvordan den kritiske aktiviteten, systemet eller ressursen gjenopprettes etter en uønsket hendelse. Her kan det være greit å ha dokumentert krav til testing av funksjon, bestilling av nytt utstyr, hvem som har ansvar for å gjøre hva og tiden det tar (Recovery Time Objective (RTO)).

Normaliseringsfasen
Når gjenopprettingen er gjennomført og omstendighetene tilsier at situasjonen kan gå tilbake til normalen, starter arbeidet med å komme tilbake i ordinær drift og planen deaktiveres. Test og valider kapasitet og funksjonalitet og sørg for å dokumentere arbeidet for ettertiden.

Obs! Vurder om dokumentasjonen skal være unntatt offentlighet.

2 Forberedelser – Workshop

Før dere starter arbeidet, bør dere sørge for at dere tilstrekkelig ressurser for å kunne lage en god plan. En plan som ikke er tydelig på roller og ansvar, hvilke tiltak dere kan iverksette innenfor budsjettrammer, eller dekker alle steg som er nødvendig for å gjenoppbygge tjenesteproduksjonen, vil ikke ha en reell nytteverdi. Sørg for at ledelsen er med på laget, finn de riktige nøkkelpersonene til å delta i arbeidet, fordel ansvar og oppgaver, samle inn all relevant dokumentasjon, lag og presenter plan for gjennomføringen av planprosessen.

For å samle relevant informasjon fra de som skal delta vil en workshop være en god innsamlingsmetode.

2.1 Før workshopen

Ledelsesforankring
Arbeidet med kontinuitetsplanen bør forankres hos ledelsen, slik at dere får den tiden og de ressursene dere trenger for å kunne utarbeide en god plan. **Sikkerhet og beredskap er, og vil alltid være, et lederansvar.**

Ledelsens ambisjoner bør beskrives i en policy som setter rammene for arbeidet, enten som en frittstående policy eller som en del av policy for informasjonssikkerhet. De bør også gi dere en avklaring på hvilke ressurser dere vil ha tilgjengelig underveis i prosessen, og oversikt over hvem som har beslutningsmyndighet til å utføre ulike tiltak som beskrives.

Det er viktig at også resten av virksomheten er kjent med arbeidet, og i beste fall forstår nytteverdien av det. Det øker sannsynligheten for at flere vil bidra i arbeidet, og at de setter seg inn i kontinuitetsplanen når den er utarbeidet.

Avgrens innholdet
Ha en tydelig avgrensning i hvilket system/tjeneste/prosess planen skal omhandle, og hvilke krisescenarier som skal inngå i planen, slik at planen ikke blir for stor og uhåndterbar. Samtidig bør den ikke være så snever og spesifikk at dere må bruke flere kontinuitetsplaner samtidig for å håndtere en krise. Da er det lett å miste oversikten. En måte å løse det på er å ha en overordnet hovedplan som gjelder hele virksomheten, med flere delplaner som er knyttet til hver seksjon/fakultet/avdeling.

Finn de riktige folkene
Arbeidet med kontinuitetsplaner bør gjennomføres sammen med nøkkelpersonell og beslutningstakere, gjerne gjennom workshops. Sørg for at gruppen til sammen har tilstrekkelig kompetanse på alle relevante områder av tjenesten. Arranger et formøte før selve workshopen, for presentasjon av metode og forventningsavklaring.

Medlemmene i gruppen bør kunne sette av nok tid til å sette seg inn i eventuelt grunnlagsmateriale, i tillegg til å delta i workshoper og selve arbeidet med å utforme kontinuitetsplanen.

Har dere ansatte som har vært gjennom en krisesituasjon, inkluder dem i arbeidet slik at dere kan dra nytte av erfaringene de har.

Vi fraråder at en person blir sittende alene med jobben. Det gir begrenset forankring i virksomheten ellers, og manglende felles eierskap til planen. Planen blir også bedre om dere har en arbeidsgruppe som dekker ulike perspektiver, kompetanser og faginteresser.

Kartlegg og analyser
Har dere oversikt over verdiene til virksomheten (verdikartlegging), hvor kritiske de er (kritikalitetsvurdering), og hvilke sårbarheter verdiene har (risikovurdering), har dere allerede en oversikt over hvilke områder dere bør sikre gjennom en kontinuitetsplan. Sørg for å kartlegge både det tekniske og det menneskelige aspektet av kontinuitetshåndteringen. Selv om tjenester og systemer er verdier som skal jobbes med, så bør ivaretakelse av de ansatte også stå som et punkt i planen, med tanke på rullering/turnus ved langvarig hendelseshåndtering, debrief og tilbakestilling til normaldrift. Personavhengigheter knyttet til systemer og tjenester bør også kartlegges og analyseres.

For virksomheter som har verdier som er underlagt sikkerhetsloven – vurder om det bør være en todelt plan hvor den en håndteres etter bestemmelsene i loven.

2.2 Workshop for forankring av planen

Workshopen består av 5 deler, hvor dere skal innom dimensjonerende scenario, vurdering av skadepotensialet, av kontinuitetsevnen, beredskapstiltak og prioritering av hvilke tiltak som skal etableres når. I hver del skal deltakerne diskutere seg imellom hva de ønsker å skrive opp av momenter. Dersom diskusjonen går i stå eller de sporer av, vil det hjelpe å ha en ordstyrer som sørger for at deltakerne i workshopen holder seg til det som er relevant og ikke går seg vill i detaljer. I hovedsak varer hver del rundt 30 minutter, etterfulgt av en kort pause. Før oppstart på neste del tar ordstyrer en kort gjennomgang av hva deltakerne kom frem til i forrige del for å holde tråden i workshopen.

TIPS:
Tenk på å beskrive løsningene så konkret som mulig, slik at de kan kunne forstås av flere i virksomheten. Den som leder workshopen kan stille spørsmålet

«vet alle hvordan dette gjøres/vet alle hvor reserveløsningen finnes?».

*Det er ikke uvanlig at viktig kunnskap finnes i hodet på erfarne medarbeidere, men ikke er nedskrevet, eller at de tenker at «det løser vi når det skjer, vi er så flinke at det fikser vi!». I de fleste tilfeller kan de det, men for å effektivisere håndteringen av en hendelse, så er det bra å ha tenkt igjennom løsningene **før** noe faktisk inntreffer. Hensikten med planene er at hvem som helst i virksomheten skal kunne anvende dem ved behov.*

1. Dimensjonerende scenario
Her presenteres det for deltakerne at de skal diskutere hvilke scenarier som vil kunne utløse og være dimensjonerende for kontinuitetsplaner for virksomheten. Formuler 3-5 scenario som krever at kontinuitetsplan blir iverksatt. **Scenariene blir utgangspunktet for de neste punktene i workshopen.**

OBS! I denne delen av workshopen skal dere **kun** finne ulike scenarier, kommer diskusjonen over på de andre temaene så bør ordstyrer peile gruppen tilbake til hva som er i fokus.

For å hjelpe deltakerne:
- *Dersom noen ønsket å ramme virksomheten, hva kunne de gjort?*
- *Hva er det verste som kan skje, og hvordan påvirker det oss?*
- *Hva kan forårsake alvorlige forsinkelser av våre leveranser/tjenester?*
- *Hva kan hindre oss i å ivareta vårt samfunnsoppdrag?*

Eksempel: brann i egne kontorlokaler så ansatte ikke kan jobbe derfra, terroraksjon i nærheten av der serverparken er lokalisert og alle serverne er ødelagt, dataangrep hvor store mengder tjenester er kompromittert, eller hackere som har kommet seg inn i systemene og fått full tilgang til personinformasjon.

2. vurdering av skadepotensialet
Her vurderes skadepotensialet de scenarioene dere har kommet frem til i forrige del kan ha med hensyn til leveranseevne til tjenesten. Her bør dere komme inn på blant annet skade eller tap på personell, materiell, funksjonsevne, økonomi, omdømme osv.

For å hjelpe deltakerne:
- *Hvordan kan dette treffe eller påvirke organisasjonen, verdikjedene og tjenesteleveransene?*
- *Hvor ille kan det bli - «worst case konsekvenser»?*

Eksempel: Virksomheten utsettes for et omfattende dataangrep som kompromitterer store mengder tjenester, noe som setter virksomheten ute av stand til å bruke de fleste digitale løsninger. Dette hemmer kommunikasjon, påvirker gjennomføring av eksamen, fører til negativ medieomtale og utløser store økonomiske kostnader.

3. Vurdere kontinuitetsevne
I denne delen skal deltakerne vurdere hva hendelsen vil kreve av teamet/gruppen/ avdelingen. Her går dere gjennom hvilke behov dere ser og hvilke krav og forventninger som må kunne stilles til tjenestens beredskapsevne til å håndtere ekstraordinære hendelser for å sikre kontinuitet, uavhengig av omfang av hendelsen.

For å hjelpe deltakerne:

- *Hvilke alternativer har vi dersom det vi bruker i det daglige er utilgjengelig?*
- *Hvordan får vi gjort jobben vår dersom første scenario fra del 1 inntreffer?*
- *Hvor har dere sikkerhetskopier av system/tjeneste?*
- *Hjelpeformulering – «evne til å…»*

Eksempel: Virksomheten må ha evne til å ivareta personvern til tross for kompromittering av tjenester, eller iverksette skadereduserende tiltak så raskt som mulig.

4. Beredskapstiltak - hvordan løser vi det?
Hvilke konkrete konsekvensreduserende tiltak bør vi iverksette? Må det etableres ekstraordinære ressurser? Antall (kapasitet)? Egenskaper (kapabilitet)? Utstyr? Lokasjon?

For å hjelpe deltakerne kan det deles opp:

- *Organisatoriske tiltak og ressurser*
- *Teknologiske tiltak og ressurser*
- *Fysiske tiltak og ressurser*
- *Menneskelige tiltak og ressurser*

Eksempel: Økt tilgangsstyring, begrense hvilke tjenester som kan nås fra nett, oppdater driftsrutiner for å lukke sikkerhetshull så snart som mulig, osv.

5. Prioritering – hvilke tiltak skal prioriteres, hvordan prioriterer hva som etableres når
I denne delen ser dere på de beredskapstiltakene som dere kom frem til på forrige del. Spørsmål som dere bør stille dere er: Hva er mest kritisk? Hva bør prioriteres og etableres først? Når skal det være etablert? Hvem bør etablere hva? Særskilte krav som må avtales?

For å hjelpe deltakerne:

- *Rangering av tiltak etter kritikalitet*
- *Når bør enkelte tiltak være etablert?*
- *Hvem bør etablere hvilke tiltak*

Eksempel: *Tiltak «se over og oppdater driftsrutiner» har pri 1. Ola Normann har ansvaret for at tiltaket blir gjort. Dette skal på plass innen Q1 2024.*

3 Gjennomføring - Lag kontinuitetsplanen

Når dere har identifisert kritisk tjenesteproduksjon og krisesituasjoner som kan skade den, kommer jobben med å utforme selve planen. Den bør inneholde all informasjon dere trenger for å kunne iverksette de riktige tiltakene så raskt som mulig. Husk at den også må fungere i papirversjon, i tilfelle dere mister tilgang til systemet den er lagret i.

For at planen ikke skal bli for lang og omfattende bør planen ha henvisninger til relaterte planer, som plan for hendelseshåndtering (Incident Response), beredskapsplan, kommunikasjonsplan og ulike sjekklister.

3.1 Innhold

Sikt har utarbeidet mal for kontinuitetsplan (se vedlegg) til utforming av selve planen.

Innholdsfortegnelse

Administrativt
- Navn på system/tjeneste/prosess som planen gjelder for
- Tjenesteansvarlig og systemeier
- Versjon og dato for sist revidert

Kritikalitetsverdi til tjenesten
- Lav/medium/høy/svært høy
- Krav til tilgjengelighet; RTO, RPO, om manuelt arbeid er mulig
- Lenke til vurdering av virksomhetskritikalitet

Tjenestebeskrivelse
- Kort info
- Informasjonssystemer og infrastruktur som kreves for å utføre prosessene i tjenesten

Avhengigheter og integrasjoner
- Finn nivå for hver avhengighet

Kontaktliste intern
- Navn, rolle, epost og telefon

Kontaktliste leverandør/ekstern/kunder
- Navn, rolle, epost og telefon

Oversikt eksterne driftsleverandører
- Hvilke tjenester, tjenestemodell, kontaktinformasjon, infrastruktur, lokasjoner, driftsavtale, tjenestenivåavtale, kontinuitetsplan fra leverandør, merknader

Opprettholdelse av kritiske funksjoner ved høyt personellfravær
- Hvilke aktiviteter og leveranser er mest kritisk?
- Hvilke er mest sårbare ved personellfravær?
- Hvilke er avhengig av eksterne leverandører?
- Forebyggende tiltak
- Beredskapstiltak

Aktiverings- og varslingsfase
- Aktiveringskriterier: hva skal til for at planen aktiveres?
- Varslingsprosedyrer: hvem skal varsles? Ses i sammenheng med beredskapsplan
- Skadevurdering: omfang og alvorlighet – hvor lang tid vil det ta å komme tilbake til normalen?
- Kommunikasjonsplan: Hvem skal ha hvilken informasjon og når?

Gjenoppbyggingsfase
- Gjenopprettingsaktiviteter og prosedyrer
  - Eksterne driftsleverandører
  - Skytjenester
  - Datarom og andre fasiliteter
  - Maskinvare og annen infrastruktur
  - Programvare
  - Integrasjoner
  - Gjenopprette data
  - Testing
  - Eskalering og varsling

Normaliseringsfase
- Varsling
- Opprydding
- Sikkerhetskopiering
- Dokumentasjon

Opplæring, testing og øvelser

Vedlegg til planen
- BIA (virksomhetskritikalitetsvurdering)
- Risikovurdering
- Tjenestedokumentasjon
- Systemdokumentasjon
- Driftsdokumentasjon
- Dokumentasjon for gjenoppbygging
- Referanser

3.2 Nyttige vedlegg

I tillegg til de vedlegg som er nevnt ovenfor kan det i tillegg være til nytte å ha med:

Testplan for system/tjeneste/prosess for å sikre at det som gjenoppbygges fungerer som det skal, og at eventuelle sikkerhetshull er fikset.
Evalueringsplan av virksomhetens håndtering av en krise eller øvelse.
Revisjonsrutine for kontinuitetsplanen.
Øvelse- og opplæringsplan for bruk av kontinuitetsplanen.
Plan for ivaretakelse av ansatte under og etter en krise.

4 Etterarbeid - Kvalitetskontroll, øvelse, revidering

4.1 Kvalitetskontroll

Når dere har utkast til planen klar, er det viktig å sjekke at den er tydelig og forståelig. Hvem som skal ha ansvaret for dette bør defineres på forhånd, og helst involvert i tidligere arbeid.

Er den begripelig? Ustrukturert informasjon uten forankring og sammenheng, gir ikke en lett forståelig plan. Den bør være kort, oversiktlig og med forståelig innhold.

Er den håndterbar? En plan på mange sider blir fort en plan ingen rekker å lese. Når ting skjer, må det være enkelt å iverksette tiltak uten å måtte lese titalls med sider.

Er den meningsfull? Planen må være relevant for den aktiviteten virksomheten bedriver, og tett kobling mellom innholdet i planen og virksomhetens ansvarsområder.

Er den tilgjengelig? Planen bør være tilgjengelig i papirversjon i tillegg til digital versjon. Det kan oppstå situasjoner hvor man ikke får tilgang til PC eller internett.

Er den øvd på? En god plan har ingen betydning om ingen i virksomheten vet hva som står der. Dere bør derfor sørge for å gjøre den kjent i virksomheten, særlig hos personell som har en nøkkelrolle i hendelseshåndteringen.

4.2 Øvelse og trening

Skal kontinuitetsplanen ha nytteverdi, er det viktig at alle nøkkelpersoner ***vet*** hvordan de skal respondere på forskjellige hendelser. Når krisen skjer, har dere ikke tid til å sette dere inn i planene. Om dere heller ikke har øvd på å få tak i planen når strøm eller internett er nede, så hjelper det ikke om dere har verdens beste plan.

For veiledningsmateriell knyttet til øvelser anbefaler vi DSB sine øvelsesveiledere som gir en god innføring i de ulike øvelsesformene (dsb.no). I tillegg har eduCSC rådgivere som kan bistå med øvelsesplanlegging og -gjennomføring.

4.3 Revidering

Hvor ofte en kontinuitetsplan skal revideres er avhengig av blant annet hvilke retningslinjer virksomheten har rundt revidering av planverk. Det anbefales å gjennomføre en revidering årlig i forbindelse med eksisterende rutiner (for eksempel gjennomgang av ledelsessystemet eller beredskapsplanen), eller etter hendelser eller øvelser hvor planen har vært i bruk.

En første versjon av planen vil trolig ikke være den mest optimale versjonen, så ha et opplegg for å finne ut om planen fungerer, og revidere den jevnlig for å forbedre den.

4.3.1 Skyldløs Post-Mortem

Luftfartsindustrien har lenge hatt fokus på systemfeil heller enn individuelle feil. Dette har de blant annet gjort gjennom bruk av noe som kalles skyldløs post-mortem (*Blameless Post-Mortem*)[3], hvor fokuset ikke er på hvem som har ansvaret for hva, men heller at man får et objektivt og nøyaktig bilde av hva som skjedde, og i fellesskap finner ut av tiltak man kunne gjort for å oppdage det tidligere, hindre at det skjer igjen, hindre at størrelsen på hendelsen ble slik den ble osv.

Dette kan være et godt hjelpemiddel som et ledd i forbedring av planverket til virksomheten.

4.4 Debrief etter krise eller øvelse

I arbeidet med kontinuerlig forbedring vil debrief være en nyttig arena for å hente ut læringspunkter fra hver enkelt av de involverte etter enten en øvelse eller en reell hendelse. Post mortem er mer en teknisk gjennomgang av hva som har skjedd, men det vil også være nyttig for beredskapsledelsen å ha en gjennomgang.

Debrief etter øvelse

I etterkant av en øvelse bør debriefen ha fokus på hva som fungerte og hva som ikke fungerte i planen. For å bygge videre på disse erfaringene husk å revidere planen i etterkant, dersom det den ikke fungerte etter hensikten.

Debrief etter krise

Ved en reell hendelse vil det være naturlig å gjennomføre en debrief når alle systemer/tjenester/prosesser er gjenoppbygd, og virksomheten er tilbake i normal drift. Alle som har vært involvert i hendelseshåndteringen bør få anledning til å delta. Her kan man da velge om man ønsker å ha en post mortem for teknikere og en separat debrief for øvrige involverte, eller om alt skal kjøres samlet.

Det som skiller debrief etter en krise fra debrief etter en øvelse, er viktigheten av å ivareta de ansatte som har stått på i en intens unntakssituasjon. En gjennomgang av hendelsen og opplevde utfordringer og bekymringer, vil være til god nytte. Det gir de ansatte mulighet til å nullstille seg etter en krevende situasjon, og forhindre utmattelse og sykmelding.

[3] Incident postmortem template | Atlassian

Forslag til punkter man kan gjennomgå i en debrief:

- Hva skjedde? Hvorfor skjedde det på den måten? Er det noe vi kunne gjort for å unngå at det skjedde, eller for å begrense omfanget?
- Hvordan reagerte vi? Vurderte vi situasjonen korrekt? Hvilke vurderinger ble gjort i forbindelse med aktivering av planen?
- Hva ble konsekvensen av tiltakene vi satte i gang?
- Hvem gjorde hva? Hvordan var arbeidsfordelingen?
- Hvordan kom vi tilbake til normalen? Hva måtte erstattes, gjenopprettes eller avvikles?
- Hva ble kostnadene på dette? Er det endringer vi ønsker å gjøre i forbindelse med gjenopprettingsprosessen?
- Tok vi godt nok vare på de ansatte underveis? Følte de ansatte seg presset til å ignorere behov for mat, pauser eller søvn for å løse krisen så raskt som mulig? Er vi for personavhengige på enkelte områder? Hva kan vi gjøre for å rette opp i det?
- Var kontinuitetsplanen til hjelp eller hinder for oss?
- Hadde vi kompetansen og oversikten vi trengte for å løse oppdragene? Visste alle hvilken rolle og ansvar de hadde?

I etterkant av en sånn gjennomgang bør det skrives en rapport som tar for seg de læringspunktene man har erfart, med forslag til hvilke tiltak som kan iverksettes for å forhindre å gjøre samme feiltrinn på nytt eller for å begrense omfanget. Dette vil og være nyttig i forhold til revidering av planen.

4.5 Lagring av planen

Først og fremst: den må være lagret trygt og tilgjengelig. Planen må være kjent i virksomheten, og være lagret i både fysisk og digitalt format slik at den alltid er tilgjengelig uavhengig av hva som har skjedd. Planen bør være mulig å få tak i selv om det brenner i kontorlokalene, og serverne den er lagret på er utilgjengelig. Samtidig bør den lagres slik at ikke uvedkommende kan få tak i informasjon om sårbarhetene til virksomheten.

5. Oppdatering av veilederen

Denne veilederen er tenkt til å være et utgangspunkt for de som jobber med kontinuitet og beredskap i sin virksomhet i kunnskapssektoren. Det vil helt sikkert være behov for justeringer og endringer av veilederen, og de som best ser hva som ikke fungerer eller hva som eventuelt fungerer bra er de som sitter og jobber med det. Vi er derfor avhengige av tilbakemeldinger dersom dere ser at veilederen trenger justeringer.

Alle tilbakemeldinger settes stor pris på og kan sendes til kontakt@sikt.no

Referanser

GÉANT (2021) *GÉANT Community Requirements for Business Continuity Planning.* Deliverable D8.12: GN4-3-21-43C319.

International Standard Organisation (2019) *Security and resilience – business continuity management systems – Requirements.* ISO 22301:2019

Kunnskapsdepartementet (2021) *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor*. Tilgjengelig fra: Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor (Sist lest: 30.03.23)

Rundskriv F-04-20 1 (2020) Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. Tilgjengelig fra: Rundskriv-f-04-20.pdf (regjeringen.no)

Grunnlag for utarbeiding av veilederen

Nasjonal sikkerhetsmyndighet (2020) *NSMs grunnprinsipper for IKT-sikkerhet. Versjon 2.0* Grunnprinsipper for IKT-sikkerhet 2.0

Nasjonal sikkerhetsmyndighet (2020) *NSMs grunnprinsipper for sikkerhetsstyring.* Grunnprinsipper for sikkerhetsstyring

National Institute of Standards and Technology Special Publication (2010) *Contingency Planning Guide for Federal Information Systems.* NIST Special Publication 800-34 Rev. 1 NIST 800-34, Rev 1 Contingency Planning Guide for Federal Information Systems

Myndigheten för samhällsskydd och beredskap (2020) *Kontinuitetsplan.* Publ.nr MSB1507 29036.pdf (msb.se)

Relaterte veiledere og anbefalinger

Veileder verdioversikt (eduCSC)

Veileder sikkerhetsstyring sikkerhetsorganisasjon (eduCSC)

Kurs i risikovurdering (eduCSC)

GÉANT (Det europeiske datanettverket for forsknings- og utdanningsmiljø), (2021) har i sitt utviklingsarbeid om kontinuitetsplaner hos virksomheter i utdanning og forskning skrevet en kort anbefaling og hva som kan legges i arbeidet:

1. *Operasjonell planlegging og kontroll – implementering av kontinuitetsplan burde være et prosjekt.*
2. *Strategi for kontinuitet – kost/nyttevurdering, teknologisk infrastruktur og kostnader knyttet til den som sørger for at virksomheten tåler tidsavbrudd og datatap, som sørger for at kritiske systemer opprettholder drift (unntatt ved ekstreme hendelser).*
3. *Etablere og implementere prosedyrer for kontinuitet – plan for hendelseshåndtering + gjenopprettingsplan (en generell plan med link til underdokumenter som er mer detaljerte). Informer om innholdet til de planen gjelder for.*
4. *Øvelse og testing – for å finne feil og mangler. Gi grunnleggende informative treninger til ansatte + mer spesifikk trening for de som har ekstra ansvar.*