IT-Beredskabsplan

En planlægningsmetode ved tab af adgang til IT-systemer

En fem-faset plan for krisehåndtering

20. maj 2025

Indhold

Faser i Beredskabsplanen

For bedre at kunne afstemme indsatsen med trusselsbilledet arbejder vi med en fem-faset model. Hver fase har sit eget fokus, tilpasset trusselsniveauet og organisationens aktuelle behov:

1.1 Fase 1: Ingen handling nødvendig

- Truslen vurderes som så usandsynlig, at ingen forberedelse er nødvendig.
- Fokus på opmærksomhed, men ingen tekniske eller organisatoriske tiltag igangsættes.

1.2 Fase 2: Planlægningsfase

- Truslen er stadig usandsynlig, men tilstrækkelig til at beredskabsplaner udarbejdes.
- Overblik over afhængigheder, systemer og nødvendige tilpasninger dokumenteres.
- Projektet offentliggøres muligvis i open source-format for at styrke samarbejde og samfundsberedskab.

1.3 Fase 3: Blød overgang

- Truslen er sandsynlig nok til, at man begynder en gradvis transition.
- Fokus på balancering af økonomi og organisatorisk forandringsledelse.
- Pilottests igangsættes, fx med:
  - Linux på klientmaskiner
  - Alternativ kontorpakke (LibreOffice, OnlyOffice, Collabora)
  - Lokal e-mailserver
  - Udskiftning af cloud-tjenester med lokale alternativer

1.4 Fase 4: Akut overgang

- Truslen vurderes som umiddelbar og troværdig.
- Alle ressourcer mobiliseres til hurtig implementering af planlagte løsninger.
- Kritiske tjenester migreres under tidspres for at sikre fortsat drift.
- Nødprocedurer for områder uden hurtige løsninger aktiveres.

1.5 Fase 5: Systemfejl og nødprocedurer

- Situationen er indtruffet uden varsel.
- Nødløsninger iværksættes, f.eks. papirbaserede skemaer og kommunikation uden cloud-tjenester.
- Målet er at opretholde minimumsdrift og genetablere stabilitet hurtigst muligt.
- Plan for genetablering af systemer igangsættes, når situationen tillader det.

Fase 1: Observation og Forberedende Overvågning

2.1 Fasedefinition

Fase 1 repræsenterer det laveste trusselsniveau. Her vurderes risikoen for tab af adgang til amerikansk software, tjenester eller licenser som **meget usandsynlig**. Det betyder, at der **ikke igangsættes nogen tekniske eller organisatoriske ændringer**. Formålet med denne fase er at sikre opmærksomhed, skabe en bevidsthed om potentielle afhængigheder og opretholde en basal informationsberedskab i organisationen.

2.2 Overordnede handlinger

2.2.1 Dokumentation af nuværende infrastruktur

- Hvis der ikke foreligger en velstruktureret og opdateret dokumentation over infrastrukturen, bør der oprettes et grundlæggende overblik med følgende elementer:
  - Hardware (servere, klienter, netværksudstyr, mobile enheder)
  - Software (installerede systemer og applikationer, versioner og konfigurationer)
  - Licenser og abonnementer (inkl. udløbsdatoer og leverandørbetingelser)
  - Certifikater og adgangskoder (opbevares sikkert og adskilt, fx i password manager)
  - Eksterne vedligeholdelsespartnere og serviceaftaler
- Identificere kontaktpersoner, der er ansvarlige for beredskabsplanens videreførelse, hvis trusselsniveauet ændrer sig
- Sikre opbevaring og synlighed af eksisterende beredskabsplaner (fx fase 2–5)
- Orientere relevante ledelsesniveauer om eksistensen af beredskabsmodellen
- Vurdere behovet for fremtidig kommunikation eller informationsstrategi
- Følge relevante nyhedsstrømme, trusselsrapporter eller politiske signaler der kan påvirke IT-afhængigheder

2.3 Kommunikation

- Ingen bred intern eller ekstern kommunikation
- Informationsniveau begrænses til beredskabsansvarlige og evt. topledelse
- Forberede skabeloner til fremtidig eskalationskommunikation

2.4 Output fra denne fase

- Navngivne kontaktpersoner og ansvarlige
- Journalisering af beslutning om at forblive i fase 1
- Notat om næste vurderingstidspunkt (f.eks. hvert kvartal eller ved specifik geopolitisk ændring)

2.5 Risikostyring i denne fase

- Lav trussel: Ingen aktioner iværksættes
- Overvågning og bevidsthed prioriteres over teknisk forberedelse
- Næste fase (Fase 2) aktiveres ved ændret politisk, teknisk eller kommerciel situation

Fase 2: Planlægningsfase

3.1 Fasedefinition

I denne fase er truslen om licens- eller tjenesteafbrydelse stadig usandsynlig, men vurderes som tilstrækkeligt realistisk til, at der bør udarbejdes kontingensplaner og tekniske overvejelser. Formålet er at dokumentere og analysere vores afhængighed af amerikansk-baserede teknologier og forberede strategier til at kunne håndtere en potentiel afbrydelse.

3.2 Overordnede handlinger

3.2.1 System- og tjenesteidentifikation

- Identificere alle kritiske systemer og tjenester afhængige af amerikanske leverandører (Microsoft, Apple, Google, Cisco m.fl.)

3.2.2 Juridisk og teknisk vurdering

- Vurdere juridiske og tekniske muligheder for erstatning eller afkobling

3.2.3 Udkast til migreringsplaner

- Udarbejde udkast til migreringsplaner for (inklusive øvrige afhængigheder, værktøjer og systemnære komponenter):
  - Operativsystemer
  - Kontorpakker
  - E-mail og kalender
  - Autentificering og adgangsstyring
  - Cloud-lagring og samarbejdsværktøjer
  - Netværksudstyr, telefoni og mobile løsninger (inkl. vurdering af afhængighed af Apple og Android enheder og mulige alternativer som Fairphone, /e/OS eller Linux-baserede systemer)
  - Backup-løsninger og lagring
  - Databaser
  - DNS
  - Firmwareopdateringer (BIOS, UEFI, drivere og anden enhedsnær software med afhængighed af producentens infrastruktur)
  - Øvrige specialiserede applikationer afhængigt af organisationens behov, f.eks.:
    - AI-værktøjer
    - Grafisk software
    - Videoredigering

    - Overvågning og adgangskontrol
    - CAD-software
    - Social media-værktøjer (EU-venlige alternativer)

3.3 Teknologiske alternativer (eksempler)

Bemærkning: Enkelte af de foreslåede løsninger har oprindelse i USA (f.eks. Keycloak, FreeIPA, Jitsi, GitLab CE, Ansible, Puppet), men er fuldt open source og kan selvhostes uden afhængighed af kommercielle tjenester eller licensbindinger. De er medtaget i kraft af deres robusthed, modenhed og uafhængighed i driftsmiljøer. Målet er ikke fuldstændig isolation, men reduktion af kritisk afhængighed.

- **Operativsystem:** Linux Mint, Debian eller Arch i testmiljø
- **Kontorpakke:** LibreOffice, OnlyOffice eller Collabora
- **E-mail:** Dovecot + Postfix, evt. i kombination med Nextcloud Kalender og Kontakter
- **AD/Azure AD:** Keycloak og FreeIPA
- **Cloud/SharePoint:** Nextcloud
- **Kommunikation (Teams):** Jitsi og Matrix
- **GitHub:** Gitea eller selvhostet GitLab CE
- **SCCM:** Ansible, shell-scripts eller Puppet
- **ERP/Navision:** Odoo, Dolibarr, Tryton
- **Database:** PostgreSQL, MariaDB, MySQL (alle open source og EU-venlige)
- **Backup-løsninger:** BorgBackup, Restic, Duplicity, eller Veeam med lokal lagring
- **Mobile enheder:** Fairphone med /e/OS eller Ubuntu Touch, PinePhone, Librem 5

3.4 Kommunikation

Etablering af en klar kommunikationsplan er central i denne fase og skal sikre, at information om planen, dens formål og forløb bliver kommunikeret effektivt og rettidigt til alle interessenter.

Kommunikationen bør:

- Udformes som en plan for internt og eksternt beredskab
- Understøtte gennemsigtighed og tillid til planens formål og metode
- Muliggøre videndeling og samarbejde med andre organisationer og open-source-miljøer
- Formidle opdateringer løbende gennem passende kanaler
- Publicering af planen i open source-format (f.eks. via GitHub), med henblik på at styrke gennemsigtighed og tillid til planens formål og metode. Dette vil samtidig gøre det muligt for andre organisationer at kommentere, genbruge og bidrage til indholdet på tværs af sektorer og landegrænser.
- Starte kontakt til andre organisationer og open-source-miljøer for videndeling og fælles udvikling

3.5 Arbejdsgruppe

Det anbefales at oprette en tværfaglig arbejdsgruppe med repræsentanter fra relevante dele af organisationen. Denne gruppe skal understøtte koordinering, forankring og fremdrift i planens arbejde.

Arbejdsgruppen bør:

- Bestå af:
  - Styregruppe
  - Økonomiansvarlige
  - Implementeringsansvarlige
  - Supportfunktioner
  - Kompetenceudviklingsansvarlige
  - Ansvarlige for intern kommunikation
- Have ansvar for:
  - Løbende afstemning med ledelse og nøglepersoner
  - Indsamling af feedback fra brugere og medarbejdere
  - Vurdering af behov for eksternt samarbejde og koordinering
  - Forberedelse af kulturskift og organisatorisk forankring

3.6 Output fra denne fase

3.6.1 Dokumenterede kontingensplaner

- Dokumenterede kontingensplaner for alle hovedsystemer, herunder for hver løsning:
  - Valg af alternativ og begrundelse
  - Implementeringskrav (teknisk og organisatorisk)
  - Migrationsmuligheder og -metoder (eksportfunktioner, scripting, manuel overførsel eller nyopsætning fra bunden)
  - IT-kompetenceudvikling: krav til opkvalificering eller behov for outsourcing
  - Slutbruger-kompetenceudvikling: træning og support
  - Budgetovervejelser: estimater for licens, hardware og drift
  - Tidsforbrug og estimeret implementeringshorisont

3.6.2 Pilotprojekter

- Pilotprojekter defineret og eventuelt igangsat, herunder:
  - Opsætning af sandkassemiljø til test af FOSS-løsninger uden produktionseksponering
  - For hvert pilotprojekt bør følgende defineres:
    - Hvad måles og testes?
    - Hvilke konkrete spørgsmål ønskes besvaret?
    - Hvor længe kører forsøget?
    - Hvilke systemer og brugergrupper indgår?
    - Hvem evaluerer og dokumenterer erfaringerne?

3.6.3 Licens- og afhængighedskortlægning

- Klarlæggelse af licensforhold og afhængigheder, herunder:
  - Hvilke systemer kræver løbende licensvalidering?
  - Hvilke systemer påvirkes indirekte, hvis licens eller adgang til et andet system ophører?
  - Er der afhængigheder til cloud-baserede login-, aktiverings- eller valideringstjenester?
  - Hvor hurtigt forventes forskellige systemer at stoppe med at fungere ved licensafbrydelse?
  - Hvilke systemer har nødlicens, offline-funktionalitet eller lokale fallback-muligheder?

3.6.4 Kompetenceudvikling

- Overblik over nødvendige kompetenceudviklingsområder (f.eks. Linux, Ansible, e-mailadministration)

3.7 Risikostyring i forhold til fokus i denne fase

- Ingen akutte handlinger tages endnu
- Fokus på dokumentation, analyse og samarbejde
- Planen evalueres og opdateres løbende ved ændring i trusselsbilledet

Fase 3: Blød overgang

4.1 Fasedefinition

I denne fase vurderes truslen som **realistisk og tiltagende**, men der er stadig tid til at foretage en planlagt og kontrolleret overgang. Der fokuseres på en **gradvis og økonomisk afbalanceret transition**, der tager hensyn til organisationens forandringsparathed og ressourcer.

Målet er at reducere kritiske afhængigheder og samtidig sikre, at forandringer implementeres med så lav forstyrrelse af driften som muligt.

4.2 Overordnede handlinger

- Prioritere kortlægning og migrering af **kritiske systemer og hardware** først, hvor afhængighed udgør en væsentlig forretningsrisiko
- Udarbejde en prioriteringsmatrix for systemer og enheder baseret på:
  - Kritikalitet for forretningsdrift
  - Risiko ved fortsat afhængighed af amerikanske leverandører
  - Kompleksitet og omkostninger ved migrering
- Prioritere migrering af systemer med lav kompleksitet og høj risiko ved fortsat afhængighed
- Evaluere og justere pilotprojekter, der er igangsat i Fase 2, og begynde udrulning i begrænsede driftsmiljøer
- Balancere økonomiske hensyn med nødvendigheden af at sikre uafhængighed
- Indgå eventuelle nye aftaler med EU-baserede leverandører og open-source communities

4.3 Pilotprojekter og gradvis implementering

- Gennemføre pilotprojekter for eks.:
  - Linux på klientmaskiner i udvalgte afdelinger
  - Alternativ kontorpakke (LibreOffice, OnlyOffice eller Collabora)
  - Lokal e-mailserver (Dovecot + Postfix)
  - Udskiftning af Teams med Matrix eller Jitsi
  - GitHub-migrering til Gitea eller selvhostet GitLab CE
- For hver pilot skal følgende være defineret:
  - Succeskriterier for drift og brugertilfredshed
  - Plan for opfølgning og evaluering
  - Økonomisk ramme og tidsplan for eventuel udvidelse

4.4 Kommunikation

- Tydelig kommunikation til hele organisationen om overgangen
- Løbende informationsmøder og statusopdateringer
- Synliggørelse af resultater og erfaringer fra pilotprojekter
- Forventningsafstemning med brugere om ændringer i arbejdsgange og værktøjer

4.5 Kompetenceudvikling

- Identificere konkrete kompetencebehov i IT-afdelingen i forbindelse med overgangen
- Definere hvilke kompetencer der kan opkvalificeres internt, og hvor der er behov for ekstern træning eller konsulentbistand
- Udarbejde en træningsplan med:
  - Tidshorisont for opkvalificering
  - Økonomisk budget for kompetenceudvikling
  - Ansvarlige for gennemførelse af træning

4.6 Arbejdsgruppe og ledelse

- Udvide arbejdsgruppen fra Fase 2 med nøglepersoner fra drift og support
- Sikre ledelsesmæssig opbakning til ændringer
- Udarbejde detaljerede implementeringsplaner og milepæle

4.7 Output fra denne fase

4.7.1 Dokumenterede beslutninger og milepæle

- Gennemførte og evaluerede pilotprojekter
- Migrering af mindre kritiske systemer
- Klar og synlig kommunikationsplan for næste skridt
- Beslutning om, hvilke områder der er klar til fuld overgang,

4.7.2 Næste skridt

- Beslutning om eventuel eskalering til Fase 4
- Planlægning af fuld migrering for prioriterede områder
- Kommunikation af næste beslutningspunkt til hele organisationen

4.8 Risikostyring i forhold til fokus i denne fase

- Aktiv overvågning af trusselsbilledet
- Løbende vurdering af om tempoet i overgangen skal øges
- Risikoanalyse for hver større ændring, der implementeres
- Udarbejdelse af fallback-planer i tilfælde af uforudsete udfordringer

Fase 4: Akut overgang

5.1 Fasedefinition

I denne fase vurderes truslen som **umiddelbar og troværdig**. Situationen kræver øjeblikkelig handling for at sikre fortsat drift og mindske risikoen for systemnedbrud eller tab af adgang til essentielle tjenester.

Alle tilgængelige ressourcer mobiliseres for hurtigst muligt at implementere de løsninger, der er forberedt i tidligere faser. Fokus er på at sikre, at kritiske systemer fungerer og er uafhængige af sårbare eksterne afhængigheder.

5.2 Overordnede handlinger

- Indhendt info fra Fase 2 og 3
- Prioritere migrering af **kritiske tjenester** under tidspres
- Allokere al tilgængelig IT- og supportkapacitet til opgaven
- Aktivere nødprocedurer for områder, hvor migrering ikke kan gennemføres i tide
- Suspendere ikke-kritiske projekter for at frigive ressourcer
- Ekspresanskaffelse af nødvendigt hardware eller software
- Etablere hurtige beslutningsveje og ledelsesmæssig eskalation

5.3 Kritiske fokusområder

- Migrering af e-mail og kommunikation til sikre og kontrollerede løsninger
- Sikring af adgangs- og identitetssystemer (f.eks. Keycloak, FreeIPA)
- Implementering af lokale fil- og backup-løsninger
- Opsætning af interne DNS- og netværkstjenester
- Udskiftning af cloud-baserede samarbejdsværktøjer med lokale alternativer (f.eks. Nextcloud)

5.4 Kommunikation

- Kriseinformationsplan aktiveres
- Tæt kommunikation mellem IT, ledelse og berørte afdelinger
- Kort og klar kommunikation til alle brugere om ændringer og begrænsninger
- Brug af alternative kommunikationskanaler, hvis cloud-baserede løsninger fejler

5.5 Kompetenceudvikling

- Fokus på akut oplæring i de alternative løsninger, der nu implementeres
- Udnytte interne superbrugere som støtte til hurtig vidensoverførsel
- Afholde korte, fokuserede workshops eller online sessioner for brugere og IT-personale

5.6 Arbejdsgruppe og ledelse

- Der åbnes op for anvendelse af overarbejde og ekstra ressourcer i denne fase. Ledelsen har samtidig ansvar for at overvåge medarbejdernes belastningsniveau og aktivt forebygge udbrændthed.
- Arbejdsgruppen fra Fase 2 aktiveres som den centrale operative enhed i denne fase.
- Arbejdsgruppen udvides med:
  - Direktøren eller en ledelsesrepræsentant med fuldt mandat til at træffe hurtige og afgørende beslutninger.
  - Økonomiansvarlige og ressourcestyringsansvarlige for hurtig godkendelse af nødvendige anskaffelser og allokering af midler.
- Arbejdsgruppen har ansvaret for den praktiske eksekvering, mens ledelsesrepræsentanter sikrer hurtig beslutningstagen og fjernelse af organisatoriske barrierer.
- Sikre konstant ledelsesopbakning og tilstedeværelse i den operative drift.
- Etablere hurtige og effektive beslutningsveje for at kunne reagere på nye udviklinger i realtid.

5.7 Output fra denne fase

- Kritiske systemer migreret til sikre og bæredygtige løsninger
- Nødprocedurer aktiveret for områder, hvor migrering ikke kunne ske
- Kommunikationskanaler etableret og aktivt anvendt
- Beredskabsstatus løbende dokumenteret og rapporteret til ledelsen

5.8 Risikostyring i forhold til fokus i denne fase

- Kontinuerlig overvågning af trusselsbilledet
- Daglige evalueringer af fremdrift og kapacitetsbehov
- Løbende risikovurdering af prioriterede migrationsopgaver
- Udarbejdelse af handlings planer for overgangen til Fase 5, hvis situationen forværres yderligere

Fase 5: Systemfejl og Nødprocedurer

6.1 Fasedefinition

Situationen er **indtruffet uden varsel**. Kritiske systemer er utilgængelige, og adgangen til essentielle IT-tjenester er mistet. Der er ikke længere tid eller mulighed for at gennemføre planlagte migreringer. Fokus er nu på at sikre absolut minimumsdrift og stabilitet gennem nødprocedurer, indtil normale forhold gradvist kan genetableres.

6.2 Overordnede handlinger

- Udarbejde en prioriteret liste over kritiske driftsfunktioner, som skal opretholdes under alle omstændigheder
- Aktivere evt forberedte nødprocedurer fra fase 4
- Tage manuelle, papirbaserede arbejdsgange i brug (skemaer, tilstedeværelseslister, manuel registrering af kritiske data)
- Etablere lokal kommunikation via ikke-digitale midler eller alternative netværk (radio, SMS, fysisk mødeaktivitet)
- Udpege et fysisk samlingspunkt for koordinering og kommunikation
- Udpege nøglepersoner med ansvar for hver kritisk driftsfunktion
- Sikre fysisk adgang til nødvendige faciliteter og udstyr uden afhængighed af digitale adgangssystemer

6.3 Kritiske fokusområder

- Bevare informationssikkerhed trods manuelle arbejdsgange
- Beskytte tilgængeligt data og udstyr mod fysisk tab eller skader
- Prioritere ressourcer til de mest nødvendige funktioner (kerneopgaven, sikkerhed, lønudbetaling)
- Sørge for fysisk tilstedeværelse af ledelses- og kommunikationsansvarlige
- Vurdere muligheder for hurtigst muligt at genetablere kerne-IT-funktioner lokalt uden eksterne afhængigheder

6.4 Kommunikation

- Anvende nødkommunikationsplanen baseret på manuelle og offline-kanaler
- Sikre daglige briefinger med statusopdateringer til medarbejdere og interessenter

- Udpege en kommunikationsansvarlig til at koordinere og formidle al intern og ekstern kommunikation
- Dokumentere alle midlertidige foranstaltninger og beslutninger for senere analyse og evaluering

6.5 Kompetenceudvikling og support

- Sikre adgang til krisepsykolog eller stresshåndteringsressourcer, hvis krisen trækker ud
- Udnytte eksisterende superbrugere og personale med erfaring i manuelle processer
- Aktivere backup-ressourcer, herunder pensionerede IT-medarbejdere eller studiejobsøgende med relevant erfaring, hvis muligt. Overvej også at inddrage medarbejdere fra andre afdelinger til at assistere med ikke-komplekse opgaver efter en kort grundtræning.
- Fokusere på rolig kriseledelse og støtte til medarbejdere for at undgå panik og forvirring

6.6 Arbejdsgruppe og ledelse

- Arbejdsgruppen omdannes til en krisestab med fuldt mandat til at træffe hurtige beslutninger
- Overarbejde kan aktiveres for at opretholde kritiske funktioner. Ledelsen har ansvar for at balancere brugen af overarbejde med hensynet til medarbejdernes trivsel og forebyggelse af udbrændthed. Der bør etableres klare rammer for, hvor længe overarbejde kan pålægges uden at iværksætte personalerotation eller inddragelse af backup-ressourcer.
- Direktøren eller stedfortræder er til stede fysisk som kriseleder
- Alle beslutninger og tiltag skal logges manuelt for senere opfølgning og rapportering

6.7 Output fra denne fase

6.7.1 Stabilisering og Tilpasning efter Krise

- Udarbejde en plan for systematisk dokumentation af nye arbejdsprocesser, så erfaringerne fra krisen fastholdes og bliver en integreret del af den fremtidige drift.
- Arbejdsgruppen har ansvaret for at lede og koordinere denne fase baseret på organisationens behov og de erfaringer, der er gjort under krisen.
- Udarbejde en plan for, hvordan alle medarbejdere løbende får den nødvendige oplæring til at tilpasse sig de nye systemer og arbejdsprocesser.
- Vurdere behov for at skabe eller tilpasse eksisterende arbejdsprocesser i alle afdelinger, så de understøtter de implementerede systemer bedst muligt.
- HR i samarbejde med afdelingsledere skal udarbejde en plan for håndtering af overarbejde efter krisen, som sikrer:
  - At medarbejdere tilbydes mulighed for afspadsering eller kompensation.
  - At udbrændthed forebygges gennem planlagt restitution.
  - At for mange medarbejdere ikke holder fri samtidig, så organisationens drift kan fortsætte uforstyrret.

- Udarbejdelse af plan for digitalisering og korrekt integration af data indsamlet manuelt under krisesituationen
- Udpege ansvarlig for sikring og opbevaring af krisedokumentation til brug i audit og senere evaluering
- Opnået opretholdelse af minimumsdrift via nødprocedurer
- Nødløsninger dokumenteret og erfaringer opsamlet
- Plan for genetablering af systemdrift udarbejdet og igangsat, når situationen tillader det

6.8 Risikostyring i forhold til fokus i denne fase

- Udarbejde klare kriterier for afslutning af nødprocedurer og overgangen til normaliseret drift
- Udarbejde en plan for vedvarende krisedrift, herunder personalerotation, forsyningssikkerhed og fortsat opretholdelse af kerneopgaven
- Kontinuerlig vurdering af personalets trivsel og belastning
- Overvågning af fysisk sikkerhed og adgangsforhold
- Løbende vurdering af, hvornår overgangen til genetableringsfase kan påbegyndes
- Evaluering og prioritering af hvilke systemer, der genetableres først

Faseovergang og Eskalationskriterier

Dette dokument definerer konkrete kriterier og observationer, som udløser overgangen mellem faserne i kriseberedskabsplanen. Målet er at sikre rettidig reaktion baseret på faktuelle forhold og risikovurderinger.

7.1 Overgang fra Fase 1 → Fase 2

Fra Observation til Planlægning

- Geopolitisk udvikling eller lovgivning, der indikerer kommende handels- eller teknologirestriktioner.
- Officielle advarsler fra relevante myndigheder (fx PET, FE, EU's cybersikkerhedsagentur ENISA).
- Interne tekniske vurderinger viser høj afhængighed af amerikanske eller eksterne leverandører.
- Ledelsen beslutter proaktivt at igangsætte planlægning for øget robusthed.

7.2 Overgang fra Fase 2 → Fase 3

Fra Planlægning til Gradvis Implementering

- Konkrete annonceringer fra leverandører om ændrede licensbetingelser eller ophør af support i nær fremtid.
- Dokumenterede afhængigheder vurderes som kritiske uden tilstrækkelige fallback-løsninger.
- Nye trusselsvurderinger hæver sandsynligheden for leverandøraftaler ophører.
- IT-ledelsen vurderer, at systemkritiske funktioner har utilstrækkelig resiliens.

7.3 Overgang fra Fase 3 → Fase 4

Fra Gradvis Overgang til Akut Krisetilstand

- Akut forværring af geopolitisk situation eller indførelse af øjeblikkelige sanktioner.
- Licenser eller cloud-tjenester afbrydes med kort eller ingen varsel.
- Kritiske systemer viser ustabilitet eller reduceret funktionalitet.
- Øget risiko for datatab, sikkerhedsbrud eller tab af adgang til nødvendige forretningssystemer.
- Direktion beslutter at aktivere Fase 4 for at sikre drift under tidspres.

7.4 Overgang fra Fase 4 → Fase 5

Fra Akut Overgang til Nødprocedurer og Minimumsdrift

- Kritiske systemer eller adgang til essentielle cloud-tjenester er fuldstændigt tabt.
- Der kan ikke opretholdes tilstrækkelig IT-drift trods nødprocedurer i Fase 4.
- Kommunikation via digitale kanaler bryder fuldstændigt sammen.
- Der er opstået fysisk sikkerhedstrussel eller omfattende forsyningssvigt.

7.5 Overgang fra Fase 5 → Genetablering af Normal Drift

Fra Nødprocedurer til Stabilisering

- Kritiske systemer genetableres eller erstatninger er implementeret.
- Kommunikationen til interessenter er genetableret.
- Der foreligger en plan for at migrere tilbage til normale forretningsgange.
- Personaletrivsel er under kontrol, og der er kapacitet til at påbegynde normalisering.

Denne plan skal gennemgås og opdateres mindst én gang årligt eller ved væsentlige ændringer i trusselsbilledet.

Licens og Deling

> **Åben anvendelse tilladt:** Denne plan stilles frit til rådighed for enhver organisation eller enkeltperson, der ønsker at bruge, tilpasse eller videreudvikle den. Det er ikke nødvendigt med tilladelse eller kreditering, men feedback, forbedringer samt forslag til samarbejde og fælles videreudvikling modtages meget gerne.

Dette dokument er tænkt som et bidrag til fælles resiliens i en usikker digital verden. Vi tror på, at gennemsigtighed, samarbejde og deling er centrale byggesten i opbygningen af digital suverænitet. Derfor lægger vi ikke begrænsninger på brugen, og vi byder både offentlige og private aktører velkommen til at anvende materialet.

8.0.1 Anbefalinger ved genbrug:

- Tilpas indholdet til egen kontekst og behov.
- Del gerne forbedringer eller tilpasninger tilbage til fællesskabet.
- Undgå at gengive dokumentet som officiel myndighedsvejledning uden lokal tilpasning.

8.0.2 Licens

Denne plan stilles til rådighed under **Creative Commons CC0 1.0 Universal (Public Domain Dedication)**.

- **CC0 betyder:**
  - Du må frit kopiere, ændre, tilpasse og distribuere materialet til ethvert formål, også kommercielt.
  - Der kræves ingen kreditering af ophav eller kilde.