# Overordnet beredskapsplan for informasjonssystemene

## Innledning

### Generelt

Hensikten med beredskapsplanlegging er å planlegge hvordan virksomheten skal håndtere uventede avbrudd i forretningsprosessene, samt å beskytte kritiske tjenester og systemer mot negative konsekvenser ved feil eller uhell.

Dette dokument beskriver overordnet struktur for beredskapsplaner og organisering av beredskap for informasjonssystemene ved *<Virksomhet>*. Dokumentet beskriver rutiner for håndtering av hendelser og iverksettelse av forebyggende tiltak i henhold til sikkerhetsstrategi definert i dokumentet «Informasjonssikkerhetspolicy – sikkerhetsmål og sikkerhetsstrategi».

I forbindelse med beredskapsarbeid benyttes ofte ulike begreper som katastrofeplan, kriseplan, beredskapsplan, «business continuity plan» og kontinuitetsplan om hverandre. I dette dokument benyttes begrepet beredskapsplan.

### Målsetting

Målsettinger med beredskapsplanen omfatter:

* Utarbeide og iverksette forebyggende tiltak for å forhindre eller begrense effektene av en eventuell katastrofe/hendelse.
* Utarbeide rutiner for å håndtere alvorlige hendelser eller katastrofer.
* Gjennomføre effektive tiltak basert på skadeomfang og prioritering av systemer, slik at drift kan gjenopptas uten unødig opphold.
* Forberede IT-personell som naturlig vil yte støtte ved en beredskapssituasjon gjennom øvelser og revisjon av planen.
* Iverksette læreprosess etter hendelse for å redusere sannsynligheten for at lignende hendelser skjer igjen.

### Omfang

Beredskapsplanen gjelder for de systemer, tjenester og infrastruktur som behandler elektronisk informasjon som tilhører *<Virksomhet>*. Systemer som skal omfattes av beredskapsplanen må klassifiseres i henhold til beskyttelsesbehov (konfidensialitet, integritet, tilgjengelighet og robusthet).

Beredskapsplanens detaljeringsgrad gjenspeiler de ulike systemenes beskyttelsesbehov (for eksempel Meget høyt, Høyt, Middels og Lavt).

## Struktur for beredskapsplanen

*<Virksomhet>s* beredskapsplan for informasjonssystemene er bygget opp rundt et rolleorientert rammeverk. Beredskapsdokumentasjonen er strukturert med et overordnet styrende dokument som beskriver struktur og rutiner (dette dokumentet). Dette dokumentet er ment å gi en statisk beskrivelse av etablert beredskapsstruktur og rutiner ved *<Virksomhet>*.

Videre kan beredskapsstrukturen bestå av organisering og et antall underliggende dokumenter og rutiner som inngår i operativ beredskapsplan.

Figur 1 viser overordnet struktur for beredskapsplanen:

Overordnet beredskapsplan – infosyst.

Forebyggende tiltak

Driftsrutiner

Beredskaps

-

øvelser

Hendelser/Operative tiltak

Kriseledelse

Kriterier for

varsling

Oversikt og

Prioritering av

Systemer /

tjenester

Lokale forhold

(fysisk utenfor

IT

-

avdeling

Varslingsliste

Registrering av

Hendelse

Hendelseslogg

Lukking av hendelse

Sjekkliste hendelse:

Rutiner for

læreprosess

IT

-

drift

IDS

Telefoni

Spesifikke

sjekklister hendelse

### Overordnet IT-beredskapsplan

|  |  |
| --- | --- |
| Ansvarlig: | IT-sikkerhetsansvarlig |
| Målgruppe: | Alle som ønsker oversikt over organisering, ansvar, overordnede proaktive og reaktive tiltak knyttet til IT beredskap hos <Virksomhet> |
| Beskrivelse: | Overordnet beredskapsplan (dette dokument) er et styrings-, opplærings- og oversiktsdokument som bl.a. beskriver:* Struktur på beredskapsdokumentasjon
* Ansvar / organisering
* Forebyggende tiltak – Organisasjon (bl.a. prosess for kriseledelse)
* Trusselvurdering
* Beredskapsøvelser
* Forebyggende tiltak for systemer og tjenester
* Revisjon av beredskapsplaner, rutiner og tiltak
 |
| Revisjon: | Revideres i forbindelse med sikkerhetsrevisjoner, beredskapsøvelser og ved organisatoriske endringer. Normalt vil dokumentet være relativt statisk og oppdateres sjelden. |

### Forebyggende tiltak

Proaktive (forebyggende) tiltak forhindrer eller begrenser negative effekter av en hendelse. Etablerte driftsrutiner inneholder proaktive tiltak som benyttes under normal drift. Driftsrutinene inngår derfor som en del av *<Virksomhet>*’s beredskapsplanen for informasjonssystemene. Ansvarlig for oppdatering og vedlikehold av driftsrutinene er IT-avdeling ved IT-driftsansvarlig. Det utøvende ansvar er delegert til hver enkelt avdelingsleder.

### Hjelpemidler ved hendelse

Beredskapsplanen omfatter et antall roller, rutiner og dokumenter. Disse hjelpemidlene utgjør den operative delen av beredskapsplanen til *<Virksomhet>* internt.

<*Følgende roller og rutiner kan inngå:*

* *Kriseleder (rolle og sjekkliste)*
* *Kriterier for hendelsens alvorlighet*
* *Kriterier for varsling (rutine)*
* *Varslingsliste (dokumentasjon)*
* *Sjekklister hendelser - IT-avdelingen (rutine)*
* *Hendelseslogg (inngår i sjekkliste for hendelser)*
* *Spesifikke sjekklister hendelse - IT-drift*
* *Oversikt og prioritering/kategorisering av systemer, forbindelser og tjenester*
* *Systemrelaterte direktiver (manuelle brukerrutiner)*
* *Lokale forhold (rutine)>*

## Ansvar og roller

Organisering av beredskap ved *<Virksomhet>s* IT-avdeling omfatter et antall roller med ulikt ansvar relatert til håndtering av hendelser.

*Eksempel på oversikt over IT-beredskapsplanens roller og ansvar:*

| **Rolle** | **Beskrivelse av ansvar** | **Kommentar** |
| --- | --- | --- |
| Administrerende direktør | Administrerende direktør har det overordnede ansvar for godkjenning og iverksettelse av beredskapsplaner ved *<Virksomhet>*. Det daglige ansvar for IT-sikkerhet er delegert til IT sikkerhetsansvarlig. | Ansvarlig for kon­takt med myndig­heter / media (dette ansvaret kan være delegert) |
| Kriseleder | Skal vurdere omfang og behov for å informere og involvere annet personell for å håndtere hendelse samt eskalering til ledelse. Skal lede og følge opp alvorlige hendelser. |  |
| Lokal sikkerhetskoordinator | Ansvarlig for rutiner relatert til lokale fysiske forhold. |  |
| Brukermiljø | De ulike avdelingene ved <Virksomhet> er ansvarlig for å ha manuelle rutiner oppdaterte og til­gjeng­elige for brukere /roller i virksomheten.  |  |
| Kunde/bruker (internt/eksternt) | Brukere av *<Virksomhet>s* informasjonssystemer skal henvende seg til Service Desk (mottak av forespørsler) dersom informasjonssystemer ikke er tilgjengelige eller ved feil. |  |
| *<Virksomhet>s* 1., 2. og 3.linje brukerstøtte | Håndtering av hendelser er dekket opp av driftsrutiner for 1., 2. og 3.linje support (Service Desk, dagvakt, Front- og sekundærbak­vakter). Ved alvorlig hendelse skal kriseleder kontaktes. |  |

## Organisering

### Hendelseshåndtering ved *<Virksomhet>*

*Beskrivelse av blant annet:*

* *Hvordan brukerhenvendelser og IT relaterte hendelser håndteres.*
* *Hvordan håndtere brudd på personopplysningssikkerheten (artikkel 33 og 34 i personvernforordningen)*
* *Indikere de ulike typer hjelpemidler som er tilgjengelige i de ulike faser av håndteringen.*
* *Bruk av et integrert verktøy for registrering hos Service Desk (mottak av forespørsler) og oppfølging).*

### Brukerstøtteorganisasjon – IT-avdelingen

*Beskrivelse av blant annet:*

* *Bruk av interne ressurser ved IT-avdelingen*
* *Brukerstøtte for systemer og tjenester*
* *Service Desk / skift*
* *Personell for 1., 2. og 3.linje brukerstøtte*
* *Henvendelser utenfor normal arbeidstid (kveld/helg/natt)*
* *Henvendelser på dagtid (hverdager kl. xx.xx - xx.xx).*
* *Mottak av meldinger om alvorlige hendelser.*
* *Oversikt over varslingskjeden.*

### Rutiner for kriseledelse

*<Beskrivelse av blant annet informasjon til brukere med status på hendelseshåndtering, forventet tid for feilretting osv.*

*Eksempel på kriseleders ansvar (figur kan vise hvilke parter som normalt er involvert ved håndtering av alvorlige hendelser/kriser)****:>***

|  |  |  |
| --- | --- | --- |
| **Rolle** | **Ansvar** | **Kommentar** |
| Kriseleder | * Inngå i vaktordning (24/7). Skal være tilgjengelig på telefon og ha tilgang til planlagte hjelpemidler
* Skal være IT-avdelingens kontaktpunkt ved alvorlige hendelser.
* Analysere hendelse og koordinere iverksettelse av tiltak for å begrense skade samt for å gjenopprette normal drift så raskt som mulig gjennom å involvere nødvendige enheter/personer hos *<Virksomhet>* og leverandører. Dette inkluderer brudd på personopplysningssikkerheten ved å melde fra til Datatilsynet uten ugrunnet opphold (innen 72 timer) og eventuelt varsle de berørte uten ugrunnet opphold.
 |  |

#### Definisjon på alvorlige hendelser

Alvorlige hendelser skal formidles til vakthavende kriseleder. Alvorlige hendelser er definert som:

* alle hendelser hvor liv og helse står på spill,
* alle hendelser som medfører at *<Virksomhet>s* informasjonssystemer eller tjenester er utilgjengelige lengre enn hva som er definert,
* alle hendelser som medfører at informasjon er blitt kjent eller endret av uvedkommende og
* alle hendelser som medfører mistanke om at informasjon er blitt kjent eller endret av uvedkommende, inkludert alle hendelser hvor sensitive personopplysninger har kommet eller mistenkes å ha kommet uvedkommende i hende.

### Verktøykasse for håndtering av alvorlige hendelser

*<Det kan utarbeides en verktøykasse som skal være tilgjengelig for vakthavende kriseleder. Verktøykassen kan inneholde blant annet følgende:*

* *Overordnet beredskapsplan (dette dokumentet).*
* *Kriterier for hendelsens alvorlighet.*
* *Kriterier for varsling.*
* *Varslingsliste.>*

### Læreprosess/Avvikshåndtering

*<Systematisk læreprosess, både etter hendelser og etter beredskapsøvelser, kan beskrives.>*

## Forebyggende administrative tiltak

* Oppfølging av hendelser.
* Endringskontroll og konfigurasjonsstyring.
* Avtaler med leverandører.
* Trusselvurdering.
* Beredskapsøvelser / tester.
* Fastlagt risikonivå for når brudd på personopplysningssikkerheten skal meldes til Datatilsynet og når de berørte av et brudd skal varsles.

## Forebyggende tekniske tiltak for systemer og tjenester

* Forebyggende tiltak ved endringer i informasjonssystemer.
* Generelle tekniske beredskapstiltak.

*<Eksempel på oversikt over generelle IT-beredskapstiltak:>*

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Systemer/tjenester med krav til tilgjengelighet** |  |
|  | **Krav til:** | **Lavt** | **Middels** | **Høyt** | **Meget høyt** | **Merknad** |
| **Organisatoriske tiltak** | Beredskapsplan (iverksetting, ansvar, tiltak, varslingslister, rapportering) | - | √ | √ | √ |  |
| Drift og vedlikeholdsrutiner (tilgangskontroll, passord, antivirus, backup, gjenoppretting, overvåking, oppdatering, logging, konfigurasjons­kontroll, endringshåndtering, håndtering av avvik) | √ | √ | √ | √ |  |
| Fysisk sikkerhet (brann, vann, innbrudd, adgangs­kontroll, sikring av serverrom og bygninger, evakuering) | √ | √ | √ | √ |   |
| Gjennomføring av egen-kontroll/ øvelser og test av egne rutiner | - | √ | √ | √ |  |
| **Generelle tiltak** | Start feilsøking innen | 24t | 8t | 2t | 1t | I åpningstid (tidsrom hvor aktuelt system skal være tilgjengelig) |
| Gjenoppretting innen | En uke | 24 t | 4t | 2t | I åpningstid (tidsrom hvor aktuelt system skal være tilgjengelig) |
| Drift og brukerstøtte Service Desk | Man-fre xx.xx - xx.xx | Man-fre xx.xx - xx.xx | Man-fre xx.xx - xx.xx | Man-fre xx.xx - xx.xx |  |
| Driftsovervåking av systemer og tjenester | - | Alle dg 06-23 | 24/7 | 24/7 | For systemer i kategori Lavt oppdages feil / hendelser gjennom varsling fra brukere |
| Alternativt driftssenter/sted skal være tilgjengelig | - | - | √ | √ |  |
| **Systemer og tjenester** | Redundans | - | - | √ | √ |  |
| Sikkerhetsmessig herding | √ | √ | √ | √ | Årlig gjennomgang |
| Backup/sikkerhetskopiering | 1 døgn | 1 døgn | 4t | 2t | Ikke eldre enn |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Revisjon av beredskapsplaner, rutiner og tiltak

Beredskapsplaner, rutiner, sjekklister og tiltak for informasjonssystemene må vedlikeholdes for at beredskapsnivået skal være tilfredsstillende. Ansvar for revisjon, oppdatering og vedlikehold av overordnet beredskapsplan (dette dokumentet) er tillagt sikkerhetsansvarlig for IT. Planene skal revideres/oppdateres ved behov.