

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Styringsdokument internkontroll	Side 1 av 2

Styringsdokument internkontroll

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Rutine for kartlegging av personopplysninger

Mal for rutinen:

1. Hvorfor skal rutinen utarbeides, hva er hensikten med den
2. Hvem er ansvarlig for å utføre de ulike aktivitetene
3. Hva skal utføres av de ulike ansvarlige
4. Hvordan skal aktivitetene utføres
5. Når skal de ulike aktivitetene utføres (eller under hvilke betingelser)
6. Hva er forventet resultat ved utførelse av rutinen

2 Oversikt over personopplysninger

Se vedlegg 1.

<Se veilederen Internkontroll og informasjonssikkerhet for veiledning til og eksempel på utfylling.>

3 Begrunnelse for behandling av personopplysninger

<Begrunnelsen gjelder behovet for å behandle personopplysningene for å kunne levere virksomhetens tjenester.>

4 Krav og plikter som følge av behandling

<Beskrivelsene gjelder krav og plikter som virksomheten blir underlagt på grunn av behandlingen av personopplysninger og eventuelt krav og plikter gjennom andre lover og forskrifter.>

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-01 Styringsdokument internkontroll.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Oversikt over personopplysninger	Side 2 av 2

5 Vedlegg 1: Oversikt over personopplysninger

Informasjon Formål	Hjemmel	Melding/ Konsesjon	Klassifika- sjon	Sikrings- tiltak	Lagring og kom- munikasjo n	Opplysning- enes omfang	Avdeling	System- / dataeier

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-01_Styringsdokument_internkontroll.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Ledelsens gjennomgang	Side 1 av 3

Ledelsens gjennomgang

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

Denne malen er basert på krav til ledelsens gjennomgang for internkontroll og styringssystem for sikkerhet. Malen dekker ikke nødvendigvis krav til ledelsens gjennomgang på andre områder.

1 Innledning

1.1 Hensikt

Hensikten med ledelsens gjennomgang er:

- Følge opp de mål som er satt
- Gjøre korrigerende tiltak
- Vurdere oppfølging av korrigerende tiltak
- Endring av mål for prosess
- Sørgе for at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige, tilstrekkelig og effektive og at det tilfredsstiller relevante krav i personopplysningsloven og -forskriften.

Det er utarbeidet sikkerhetsmål for virksomheten. Med bakgrunn i målene utarbeides det planer (forbedringstiltak) for å nå disse målene.

Oppfølging av forbedringstiltak og korrigerende tiltak gjøres ved at resultatene fra egenkontroll og avviksbehandling gjennomgås og sammenlignes med de korrigerende tiltakene.

1.2 Ansvarsforhold

Det er ledelsen ved virksomheten som har ansvar for å gjennomføre ledelsens gjennomgang. Sikkerhetsansvarlig har ansvar for å tilrettelegge gjennomgangen. Ledelsens gjennomgang gjøres normalt en gang pr. år.

2 Utførelse

2.1 Revisjon

Revisjon av de elementer som er styrende for internkontroll og informasjonssikkerhet, som:

- **Internkontroll**
 - Vurdere endringer i omfang av dagens internkontroll
- **Sikkerhetsmål og -strategi**

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-02_Ledelsens_gjennomgang.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Ledelsens gjennomgang	Side 2 av 3

- Vurdere eventuelle forslag til endringer i sikkerhetsmål og sikkerhetsstrategi, dersom endringene i vesentlig grad har økonomiske eller andre virksomhetsmessige konsekvenser
- **Risiko- og sårbarhetsanalyse**
 - Ønske om ny funksjonalitet som medfører vesentlige investeringer eller endringer i eksisterende sikkerhetskonsept
- **Virksomhetskritisk informasjon og/eller system**
 - Vurdering av endringer i hvilken informasjon eller hvilke systemer som er virksomhetskritisk for virksomheten

2.2 Sikkerhetsmål

Sikkerhetsmål utarbeides for virksomheten. Bakgrunnsmateriale for utarbeidelse vil være:

- Resultater og hovedkonklusjoner fra risikoanalyser og egenkontroll
- Endringer i offentlige sikkerhetskrav, som kan medføre vesentlig endringer for virksomheten
- Vurdere om tilstrekkelige ressurser er tilgjengelige for å ivareta internkontroll og informasjonssikkerhet

2.3 Gjennomgang av avvik og hendelser

Ledelsen går detaljert gjennom de alvorligste hendelsene og avvikene som har vært gjennom året, kun summarisk gjennom de mindre alvorlige. Diskusjon bør omfatte årsaker til hendelser og avvik i vid forstand og hvordan hendelser og avvik er håndtert.

2.4 Forbedringstiltak

Forbedringstiltak, gjennomføring av tiltak til fastsatte tidspunkter, utarbeides av sikkerhetsansvarlig på bakgrunn av oppsatte mål, innen områdene:

- Organisering av sikkerheten
- Partnere og leverandører
- Personell og sikkerhet
- Fysisk sikkerhet
- Systemteknisk sikkerhet
- Dokumentsikkerhet
- Beredskap

Forbedringstiltakene skal godkjennes av virksomhetsleder.

2.5 Oppfølging

Oppfølging av sikkerhetsmål for å se om de nås og om forbedringstiltak og korrigerende tiltak virker, gjøres blant annet gjennom egenkontroll. En plan for egenkontroll må derfor utarbeides.

Oppfølging av at forbedringstiltakene virker, gjøres i forbindelse med ledelsens gjennomgang, som gjennomføres normalt en gang pr. år.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-02_Ledelsens_gjennomgang.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Ledelsens gjennomgang	Side 3 av 3

3 Referat

Sikkerhetsansvarlig skriver referat fra ledelsens gjennomgang og dette distribueres til ledelsen ved virksomheten.

I referatet skal det tydelig fremgå de avgjørelser og aksjoner som er bestemt og med hvilken begrunnelse.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-02_Ledelsens_gjennomgang.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 1 av 8

Sikkerhetsmål og -strategi

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Innledning

Sikkerhetsmål og strategi er <Virksomhet>s overordnet styrende dokument for informasjonssikkerhet.

Ledelsen i <Virksomhet> har det overordnede ansvaret for all informasjonssikkerhet hos <Virksomhet>. Sikkerhetsansvarlig har ansvar for utarbeidelse av mål og strategi for informasjonssikkerhet, utarbeidelse av rutiner samt kontroll med at rutinene følges.

Sikkerhetsmålene beskriver hva som ønskes oppnådd sikkerhetsmessig, mens sikkerhetsstrategien beskriver hvilke tiltak som skal gjennomføres for å oppnå sikkerhetsmålene.

2 Sikkerhetsmål

Sikkerhetsmålene skal understøtte og sikre virksomhetens drift, allmenne tillit og omdømme i det offentlige rom, ved å forebygge og begrense konsekvensene av uønskede hendelser. Sikkerhetsmålene beskriver <Virksomhet>s overordnede mål for beskyttelse av virksomhetens informasjonsbehandling mot interne og eksterne trusler av tilsiktet og utilsiktet art.

Det overordnede formålet med <Virksomhet>s behandling av personopplysninger er <Fyll inn virksomhetens formål med behandlingene her>

Følgende sikkerhetsmål er definert:

1. <Virksomhet> skal sikre at informasjon behandles iht krav i relevante lover og forskrifter.
2. Sikkerheten ved <Virksomhet> skal ha forankring i ledelsen ved <Virksomhet>.
3. Sikkerheten skal ivaretas som en integrert del av hele <Virksomhet>s organisasjon.
4. Den fysiske sikkerhet ved <Virksomhet> skal hindre at uautoriserte får adgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 2 av 8

5. Tilgang til systemer og informasjon gis kun til medarbeidere etter behov (Need to Know).
6. Tilgang til systemer og informasjon for uvedkommende skal forhindres.
7. <Virksomhet> skal sikre at informasjonsbehandling er korrekt og at informasjon ikke forandres uten lovlig tilgang.
8. <Virksomhet> skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid for de personer som er autorisert.
9. Det skal være mulig å spore uønskede hendelser.
10. Det skal være tatt i bruk rutiner for å håndtere uønskede inkludert virksomhetskritiske hendelser.
11. Det skal være tatt i bruk systematiske læreprosesser ved uønskede hendelser slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres
12. Forhindre at personer eller systemer hos <Virksomhet> bevisst eller ubevisst er årsak til sikkerhetsmessig uønskede hendelser mot egen eller andre virksomheter eller privatpersoner.
13. <Virksomhet> skal sikre at medarbeidere som bruker <Virksomhet>s informasjonssystemer har en tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov/krav.

Regelverk

- Personopplysningsloven
- Personopplysningsforskriften

Andre relevante lover/forskrifter

<Stryk de lover nedenfor som ikke er relevante, og legg eventuelt til andre relevante lover og forskrifter>

- Forvaltningsloven
- Offentlighetsloven
- Sikkerhetsloven
- Straffeloven
- Arkivloven
- Helseregisterloven
- Arbeidsmiljøloven
- Tjenestemannsloven

Mer informasjon om lovene og forskrifter finnes på www.lovdato.no.

3 Sikkerhetsstrategi

3.1 Organisering av sikkerheten

Sikkerhetsansvarlig

Sikkerhetsansvarlig ved <Virksomhet> har et overordnet utøvende ansvar for informasjonssikkerheten i <Virksomhet>. Ansvaret innebærer å organisere, koordinere og styre sikkerhetsarbeidet, utarbeide retningslinjer, iverksette egenkontroll, gjennomføre forbedringsprosesser samt følge opp at sikkerheten vedlikeholdes i alle ledd. Sikkerhetsansvarlig har videre myndighet og ansvar til blant

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 3 av 8

annet å kunne gjennomføre opplæring i informasjonssikkerhet, risikovurderinger, sikkerhetstester, avvikshåndtering, iverksette korrigerende og andre sikkerhetsrelaterte tiltak. Sikkerhetsansvarlig rapporterer til Ledelsen i <Virksomhet> i sikkerhetssaker. Ansvarsområdet reguleres av stillingsbeskrivelse.

Organisering

Deler av operativt sikkerhetsansvar vil normalt delegeres til personer i ulike avdelinger. Sikkerhetsorganiseringen skal til enhver tid fremgå av egen beskrivelse der roller og personer (inkludert kontaktinformasjon) inngår.

Kontrakter Alle formaliteter mellom <Virksomhet> og leverandører skal være formulert i formelle kontrakter (SLA - Service Level Agreement) og skal inkludere relevante sikkerhetskrav. <Virksomhet> skal alltid ha rett til innsyn og måling av hvorvidt sikkerhetskrav etterleves av en leverandør.

Egenkontroll

- Egenkontroll/måling av sikkerhetsnivå ved <Virksomhet> skal utføres regelmessig iht. systematiserte rutiner.
- Avvik fra sikkerhetsmål og strategi samt vedtatte rutiner og styrende dokumenter skal håndteres som en del av avvikshåndtering, se 3.9.

3.2 Personell og sikkerhet

Generell taushetserklæring

Alle som får tilgang til beskyttelsesverdig opplysninger om <Virksomhet> skal underskrive en taushetserklæring. Dette gjelder <Virksomhet>s ansatte, leverandørers ansatte eller andre som måtte komme i kontakt med slik informasjon.

Sikkerhetsinstruks

Alt personell med tilgang til informasjonssystemene skal underskrive "Sikkerhetsinstruks bruker".

Kompetanse

Ansatte hos <Virksomhet> skal gjennom opplæring og rutiner oppnå tilstrekkelig kunnskap til å forvalte informasjon og systemer på en sikker måte. Endringer i konfigurasjon av systemer og nettverk skal bare utføres av kvalifisert personell, og etter godkjenning fra <Virksomhet>.

Konsekvenser ved sikkerhetsbrudd

Brudd på sikkerhetsreglene beskrevet i sikkerhetsinstrukser, taushetserklæring og eventuell konfidensialitetserklæring, vil bli vurdert i henhold til de lover som står beskrevet i kap. 2.1 og kan få følger for ansettelsesforholdet.

3.3 Fysisk sikkerhet

Soneinndeling og adgangskontroll

- Adgang til <Virksomhet>s lokaler for eksternt (og internt) personell skal godkjennes av aktuell linjeleder og følge retningslinjer for tildeling av adgang. Adgang skal begrenses til det minimum av lokaler som vedkommende har behov for.
- Adgangskontroll med bruk av adgangskort med personlig kode utenfor arbeidstid eller nøkkel skal være montert.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 4 av 8

- Arkiv, serverrom og rom med annet sentralt IT-utstyr skal sikres og plasseres slik at det er mulig å begrense adgangen til området. Dør til slike områder skal alltid være låst. Dette gjelder også rom med sensitive personopplysninger og opplysninger gradert etter sikkerhetsloven.
- Utrangerte harddisker beskyttes tilsvarende servere.
- Ytterdører skal være låst etter arbeidstidens slutt.
- Når kontor forlates skal kontordør låses .
- Reserve besøkskort, adgangskort, nøkler og passord skal lagres i safe eller på annen sikker måte.

Alarmsystemer

- <Virksomhet>s adgangskontrollsystem skal gi alarm ved forsøk på uautorisert adgang til vaktsselskap.
- <Virksomhet>s døgnskategorisk innbruddsovervåking skal gi automatisk alarm til egen vakt.

3.4 Tilgang til informasjonssystem

- Nærmeste linjeleder er ansvarlig for å klarlegge og autorisere en ansatts behov for tilgang og formidle dette til IT-avdelingen ved ansettelse eller endringer i ansvar.
- Informasjonseier har ansvaret for å godkjenne tilgang til egen forvaltet informasjon.
- Nærmeste linjeleder er ansvarlig for å melde til IT-avdelingen at personell slutter slik at tilgangsrettigheter fjernes.
- IT-avdelingen eller den IT-avdelingen bemyndiger er ansvarlig for å vedlikeholde tilgangsrettigheter samt holde oversikt over de tilgangsrettigheter som er gitt.
- Linjeleder er ansvarlig for at verifikasjon av tilgangsrettigheter gjøres.

3.5 Dokumentsikkerhet

Alle dokumenter og lagringsmedia som inneholder beskyttelsesverdig informasjon, skal oppbevares, forsendes og destrueres på en slik måte at det ikke kommer uvedkommende i hende.

3.6 Konfigurasjonskontroll

Oversikt over gyldig sikkerhetsdokumentasjon, utstyr, programvare og systemkonfigurasjon skal utarbeides og vedlikeholdes.

- IT-avdelingen har ansvaret for å utarbeide og vedlikeholde oversikt over utstyr, programvare og systemkonfigurasjon.
- Sikkerhetsansvarlig har ansvaret for å utarbeide og vedlikeholde oversikt over sikkerhetsdokumentasjon.

3.7 Endringskontroll

- Ved endringer i <Virksomhet>s informasjonssystemer skal alltid beskyttelsesbehov vurderes, og om endring kan ha konsekvenser for sikkerheten.
- Endringer som kan ha konsekvenser for informasjonssikkerheten, skal godkjennes av sikkerhetsansvarlig.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 5 av 8

- For endringer som kan ha sikkerhetsmessig konsekvens, skal IT-avdelingen utarbeide en risikovurdering inkludert forslag til tiltak som oversendes sikkerhetsansvarlig som en del av endringsforespørsel.
- Sikkerhet skal være et vurderingspunkt gjennom alle faser av en endring.
- Krav til sikkerhet og overordnet vurdering av risiko skal inngå i eventuelle forprosjekt.
- Ved en eventuell kontrakt med tredjepart skal krav til sikkerhet inngå i kontrakten.
- Produksjonsdata som inneholder sensitive personopplysninger skal anonymiseres før de benyttes ved tester knyttet til endringer.
- Sikkerhetsnivå skal verifiseres før endringer idriftsettes.

3.8 Beredskap

Det skal etableres en beredskapsplan som dekker:

- Ansvar og vaktordning for håndtering av hendelser.
- Effektiv håndtering sikres gjennom rutiner som er tilgjengelig for relevante personer.
- Hendelser skal håndteres i henhold til hendelsens alvorlighet.
- Varslingsrutiner skal eksistere der både relevant personell hos <Virksomhet> og partnere inngår.
- Drift og kontinuitetsplan for å gjenopprette normaldrift skal finnes.

Tiltak for å hindre uhell/kriser

- Brann: Det skal være automatisk branndeteksjon, og varsling til brannvesen
 - for tekniske rom, serverrom, operasjonsrom, fortrinnsvis med automatisk brannslukningsutstyr.
 - i kontorer og korridorer.
- Vann: Sikring mot vannlekkasje i relevante rom (der servere er plassert).
- Tyveri/innbrudd: Skal detektere og forhindre innbrudd. Innbruddsalarm tilknyttet vaktentral med utrykning ved alarm.
- Brann eller andre uhell skal ikke slette eller ødelegge virksomhetskritisk informasjon.
- Strømsvikt og -ustabilitet: informasjonssystemene skal sikres mot overspenninger, servere skal beskyttes mot utilsiktet strømbrudd og separat strømforsyning skal være tilgjengelig.

3.9 Avvikshåndtering

- Alvorlige hendelser av sikkerhetsmessig betydning skal alltid rapporteres til sikkerhetsansvarlig.
- Ved alvorlige hendelser skal sikkerhetsansvarlig involveres i oppfølging og beslutning av korrigerende tiltak knyttet til hendelsen.
 - Sikkerhetsansvarlig har ansvar for oppfølging og beslutning av korrigerende tiltak som gjelder hendelser ved brudd på konfidensialitet eller integritet samt enkeltpersoners brudd på sikkerhetsreglene.
 - Hvis personopplysninger er kommet på avveie eller det er mistanke om det samme, skal Datatilsynet orienteres.
 - IT driftsansvarlig har ansvar for oppfølging og beslutning av korrigerende tiltak som gjelder hendelser relatert til tilgjengelighet på systemer og tjenester

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 6 av 8

3.10 Systemteknisk sikkerhet

3.10.1 Nødvendig sikkerhetsnivå – høy, middels, lav

Avhengig av det aktuelle system og informasjonen som behandles, vil de ulike aspektene ved sikkerhet (tilgjengelighet, konfidensialitet og integritet) ha ulik betydning. Følgende kategorisering benyttes for beskyttelsesbehov:

- Høy - gis bare systemer og informasjon med virksomhetskritisk beskyttelsesbehov.
- Middels - gis systemer og informasjon med beskyttelsesbehov.
- Lav, (lave krav til sikkerhet) kan gjelde alle systemer og informasjon med lite eller ingen beskyttelsesbehov.

Ulike delsystemer kan ha ulike beskyttelsesbehov.

3.10.2 Krav til dokumentasjon av beskyttelsesbehov

- <Virksomhet> skal vedlikeholde en oversikt over personopplysninger og andre digitale verdier som informasjonssystemer og eksterne kommunikasjonsgrensesnitt med faktisk beskyttelsesbehov.
- <Virksomhet> skal vedlikeholde kriterier for valg av beskyttelsesbehov.
- Sikkerhetstiltak skal vurderes og iverksettes i henhold til definert beskyttelsesbehov.
- Vurdering av beskyttelsesbehov skal inngå i alle system- eller infrastruktur endringer som kan påvirke informasjonssikkerheten.

3.10.3 Strategi for systemteknisk sikkerhet

Generelt

- Sikkerhetstiltak for <Virksomhet>s nettverk og systemer skal aldri basere seg på at system, person, eller virksomhet det kommuniseres med har en "sikker" infrastruktur, <Virksomhet>s lokale tiltak skal alltid iverksettes for å minimalisere risiko.
- Sikkerhetsbehov skal alltid vurderes relatert til hvor virksomhetskritiske systemene er (se over "Nødvendig sikkerhetsnivå").

Datakommunikasjon

- <Virksomhet>s nett skal inndeles i soner der hver sone bare utveksler relevant trafikk med andre interne/eksterne soner. Eksempler kan være driftsnett, server-sone og lignende.
- Brannmur og tilsvarende sikkerhetsbarrierer skal benyttes for å oppnå et sikkert skille mellom <Virksomhet> og eksterne nett.
- All ekstern kommunikasjon skal rutes via sikkerhetsbarrierer som filtrerer ulovlige tjenester, uønsket informasjon, adresser og trafikketretning.
- Det skal benyttes to sikkerhetsbarrierer mellom sikret sone og eksternt nettverk for behandling av sensitive personopplysninger.
- Det skal være elektronisk overvåking av ekstern nettverkstrafikk/kommunikasjon mot virksomhetskritiske systemer og nettverk ved <Virksomhet>.
- Support fra leverandører over eksterne linjer skal benytte VPN-løsning med kryptering. Tilkoplingen i <Virksomhet>s nettverk skal aktivt åpnes/lukkes etter

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 7 av 8

behov. Dersom det likevel etter en risiko/nyttevurdering anses som påkrevd med kontinuerlig forbindelse skal tilkobling skje i egen nettverkssone der trafikk overvåkes og kontrolleres.

Infrastruktur

- Mekanismer i underliggende nettverkskomponenter, operativsystem og annen programvare skal benyttes for å oppnå at brukere bare har tilgang til relevant informasjon.
- Autentiseringsmekanismer skal alltid være integrert med og bygge på underliggende autentiseringsmekanismer i operativsystem og nettverk.
- Antall passord eller tilsvarende som en bruker må kunne skal minimaliseres
- Automatisk passordbeskyttet skjermsparer skal benyttes.
- Systemene skal regelmessig oppdateres med relevante sikkerhetspatcher.
- Server og klienter skal være herdet mot innbrudd og nedetid.
- To-nivå automatisk viruskontroll og med automatisk oppdatering av signaturer skal være iverksatt. Med to-nivå menes intern viruskontroll og viruskontroll på ytre barriere.
- PC som ikke eies av <Virksomhet>, skal ikke tilkobles <Virksomhet>s nettverk. Dersom det likevel etter en risiko/nyttevurdering anses som påkrevd skal tilkobling skje i egen nettverkssone der trafikk overvåkes og kontrolleres.
- Alle PC'er tilknyttet <Virksomhet>s nettverk skal være innkjøpt, forvaltet og konfigurert av IT-avdelingen.
- På bærbare PC'er som benyttes til å lagre sensitive personopplysninger og eller annen sensitiv informasjon, skal harddisk (eller relevante deler av denne) krypteres, samt at beskyttelse mot endringer ved oppstart skal iverksettes.
- Bærbare PC'er kan bare koples direkte til eksternt nett dersom de er konfigurert og godkjent av IT-avdelingen.
- Informasjonssystemer skal være konfigurert til å logge uautorisert tilgang eller forsøk på uautorisert tilgang.
- Tilgang relatert til brukere skal være sporbart til brukernavn/-identifikasjon
- Utførelse av rutiner for egenkontroll og drift, samt håndtering av sikkerhetsrelaterte hendelser eller hendelser knyttet til manglende stabil drift, skal logges.
- Programvare- og maskinvare-plattformer benyttet i <Virksomhet>s informasjonssystem skal være standardisert. Det er ikke tillatt å installere egen programvare, all installasjon skal utføres av IT-avdelingen eller de som IT-avdelingen delegerer dette til.
- <Virksomhet> systemer og nettverk skal ha synkroniserte klokke.
- IT-avdelingen skal vedlikeholde en oversikt over beskyttelsesbehov for et gitt system, dette kan inkludere oversikt over hvilke informasjonsfelter som må beskyttes med indikasjon av nødvendig sikkerhetsnivå.

3.10.4<Virksomhet>s spesifikke applikasjoner

For <Virksomhet>s spesifikke applikasjoner, dvs applikasjoner som utvikles spesielt for <Virksomhet>s, gjelder følgende:

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsmål og -strategi	Side 8 av 8

- Ansvar for håndtering av sikkerhetsbehov i <Virksomhet>s spesifikke applikasjoner ligger hos systemeier. Utøvende ansvar kan delegeres til prosjektleder eller andre navngitte personer.
- All programvare skal utvikles på bakgrunn av detaljerte kravspesifikasjoner der også krav til sikkerhet inngår.
- Teknisk sikkerhetsnivå skal verifiseres i alle prosjektets faser ved utvikling.
- Før programvaren/systemer settes i produksjon, skal teknisk sikkerhetsnivå verifiseres. Ved feil eller mangler skal retting av eventuelle feil/mangler gjennomføres før systemet settes i produksjon. Rettelser av feil og mangler skal verifiseres.
- Før programmer eller systemer settes i produksjon skal rutiner for drift, proaktiv overvåkning og beredskap være iverksatt.
- Verifikasjon av sikkerhet gjennom test skal utføres av andre personer enn de som har vært med på å utvikle systemet eller personer som drifter systemer.

Sikkerhetsansvarlig har ansvaret for selve gjennomføringen av testen og formidler resultatene tilbake til prosjektet.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-11 Sikkerhetsmal og strategi.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsorganisasjon	Side 1 av 2

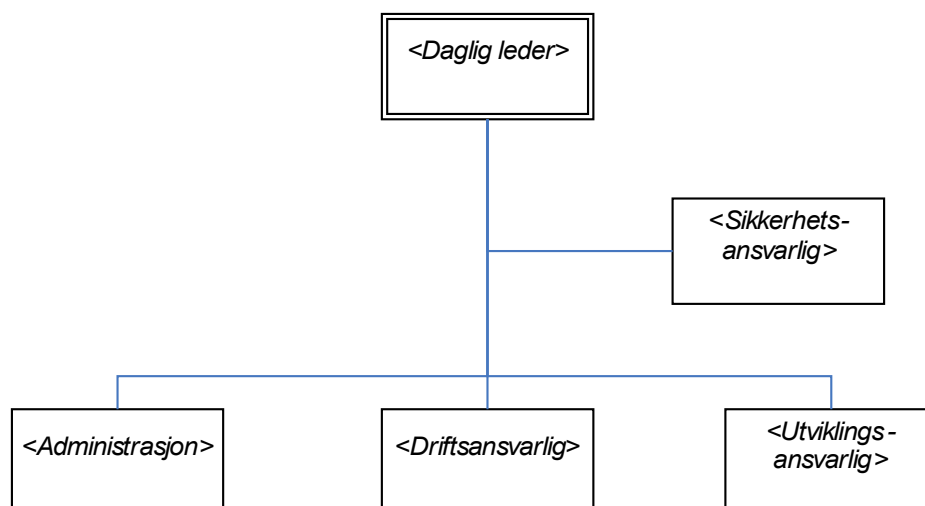
Sikkerhetsorganisasjon

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Diagram

<Fylles ut med eget organisasjonsdiagram>



2 Roller og ansvarlige

<Fylles ut med sikkerhetsrelaterte roller og ansvarlige personer samt eventuell beskrivelse av oppgaver/ansvarsområder for avdelinger>

Sikkerhetsrelatert rolle / Navn / Stilling

Eksempel:

Sikkerhetsansvarlig: NN <Stilling>

Stedfortreder: NN <Stilling>

Driftsansvarlig: NN <Stilling>

Stedfortreder: NN <Stilling>

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-12 Sikkerhetsorganisasjon.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsorganisasjon	Side 2 av 2

Administrasjonen: NN <Stilling>
Stedfortreder: NN <Stilling>

Følgende områder utføres av Administrasjonen:

- *Fysisk sikkerhet*
- *Arkivering og post*
- *Personell og sikkerhet*

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 1-12 Sikkerhetsorganisasjon.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Rutiner for håndtering av personopplysninger	Side 1 av 2

Håndtering av personopplysninger

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Eksempel på tidsfrist for sletting av opplysninger i personalmapper må konkret vurderes av virksomheten før rutine tas i bruk.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

Bruk denne malen for å etablere rutiner for:

- iverksettelse eller opphør av behandling
- overholdelse av melde- og eventuell konsesjonsplikt
- sletting av personopplysninger
- utlevering av personopplysninger til andre
- sikring av kvalitet av personopplysninger
- innhenting og kontroll av samtykke
- oppfyllelse av plikt til informasjon
- innsyn, retting og supplering
- ivaretagelse av eventuell reservasjonsrett
- innsyn i privat epost og private filområder

1 Mal for rutinebeskrivelse

1. Hvorfor skal rutinen utarbeides, hva er hensikten med den
2. Hvem er ansvarlig for å utføre de ulike aktivitetene
3. Hva skal utføres av de ulike ansvarlige
4. Hvordan skal aktivitetene utføres
5. Når skal de ulike aktivitetene utføres (eller under hvilke betingelser)
6. Hva er forventet resultat ved utførelse av rutinen

2 Eksempel - Sletting av personopplysninger

1) Hvorfor skal rutinen utarbeides

Krav i personopplysningsloven §28.

2) Hvem er rutinen rettet mot

- Virksomhetens ledere og saksbehandlere.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-01_Rutiner_for_handtering_av_personopplysninger.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Rutiner for håndtering av personopplysninger	Side 2 av 2

- Arkivpersonale.

3) Hva skal utføres

Hovedregelen er at personopplysninger skal slettes når formålet med behandlingen er oppnådd.

Virksomheten har arkivplikt etter arkivloven, hvilket innebærer at saker virksomheten har hatt til behandling ikke kan slettes. Saker som er eldre enn 10 år skal som hovedregel overleveres til Riksarkivet. Oppbevaring av saker eldre enn 10 år skal ha særlig begrunnelse.

Personopplysninger om ansatte kan oppbevares så lenge opplysningene er relevante for det formål de er opprettet.

Advarsler skal likevel slettes 2 år etter at advarsel ble gitt, med mindre særlige forhold gjør seg gjeldende. Med særlige forhold menes:

- ikke endret adferd,
- nye advarsler eller
- oppsigelsessak eller avskjedssak er innledet.

Ved arbeidsforholdets slutt skal alle personalopplysninger gjennomgå. For videre lagring må det anføres et særskilt grunnlag.

4) Hvordan skal aktivitetene utføres

Behandlingsansvarlig har delegert det daglige sikkerhetsansvaret til sikkerhetsansvarlig.

Sikkerhetsansvarlig gir skriftlig melding til IT driftsansvarlig om hvilke opplysninger som skal slettes og når.

5) Når skal aktivitetene utføres

Ved hver periodisk kontroll eller ved en ansatts fratredelse fra stilling.

6) Resultat

Virksomheten sikrer at personopplysninger ikke oppbevares lenger enn nødvendig.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-01_Rutiner_for_handtering_av_personopplysninger.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Risikovurdering	Side 1 av 2

Risikovurdering

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Rutinebeskrivelse

Mal for rutinebeskrivelse:

1. Hvorfor skal rutinen utarbeides, hva er hensikten med den
2. Hvem er ansvarlig for å utføre de ulike aktivitetene
3. Hva skal utføres av de ulike ansvarlige
4. Hvordan skal aktivitetene utføres
5. Når skal de ulike aktivitetene utføres (eller under hvilke betingelser)
6. Hva er forventet resultat ved utførelse av rutinen

2 Overordnet vurdering av beskyttelsesbehov

<På bakgrunn av hvilket potensial de ulike systemene representerer i forhold til konsekvens, kan vi gjøre en overordnet vurdering av hvilket beskyttelsesbehov som er nødvendig. Systemer hvor katastrofale hendelser kan inntreffe vil normalt, uavhengig av sannsynlighet, ha behov for en bedre beskyttelse enn systemer hvor slike hendelser ikke kan inntreffe.>

	Konfidensialitet	Integritet	Tilgjengelighet
Katastrofal (K=4)			
Stor (K=3)			
Moderat (K=2)			
Liten (K=1)			

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-11 Risikovurdering.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Risikovurdering	Side 2 av 2

3 Hendelsesvurdering

<Først angis hvilke sikkerhetsaspekter som er relevante for hendelsen (konfidensialitet, integritet og / eller tilgjengelighet - KIT). Så gis en vurdering av mulig konsekvens, sannsynlighet for at hendelsen skal inntreffe og risiko som følge av dette. Til slutt gis det en vurdering av om risikoen er akseptabel eller ikke.>

Hendelse	Kategori KIT	Konsekvens	Sannsynlighet	Risiko	Vurderes som akseptabel

4 Beskrivelse av akseptabel risiko

<Tabellen benyttes for å beskrive hendelser man aksepterer risikoen for med gjeldende sikkerhetstiltak (i hvite felt) og hendelser man ikke aksepterer risikoen for (i grå felt). Nye tiltak skal så planlegges og gjennomføres for å redusere risikoen for at uakseptable hendelser skal inntreffe (det vil si flytte hendelsene over fra "grått område" til "hvitt område". Tilsammen vil hendelsene i denne tabellen indikere akseptabelt risikonivå.>

(Forklaring: Hvite felt representerer akseptabel risiko, grå felt uakseptabel.)

Konsekvens: Sannsynlighet:	Liten	Moderat	Stor	Katastrofal
Lav				*
Moderat				
Høy				
Svært høy				

*) Kombinasjonen av katastrofal konsekvens og lav sannsynlighet må sees på som umulig å unngå fordi vi allerede er på den laveste sannsynlighetskategorien, og det kan være umulig å redusere konsekvensen. Derfor er denne kombinasjonen akseptabel, men man bør være bevisst mulige hendelser i denne kategorien og vurdere aktuelle tiltak.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-11 Risikovurdering.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks bruker	Side 1 av 5

Sikkerhetsinstruks bruker

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

Punktene om privat bruk og arbeidsgivers innsyn i e-post og filer bør vurderes konkret for virksomheten. Instruksene må gjøres forutsigbar og konkret for brukeren.

Instruksene bør gjennomgås med tillitsvalgte før den tas i bruk i virksomheten

1 Innledning

Denne instruksjonen beskriver retningslinjer for bruk av IT ved <virksomhet>. Instruksjonen gjelder for alle ansatte og skal være lest og signert, og så leveres til <administrasjonsavdelingen> hvor den blir oppbevart i personalmappen.

Håndtering av dokumenter og informasjon er behandlet i en egen instruks, ref. 8.

2 Bruk av <virksomhet>s informasjonssystem

- Dokumenter som inneholder beskyttelsesverdige opplysninger som kan skade enkeltindivider, kunder eller <virksomhet> hvis de blir kjent av uvedkommende, skal graderes, merkes og håndteres i henhold til rutine for informasjonshåndtering (ref. 8).
- <Virksomhet>s informasjonssystemer er beregnet for jobbrelevante formål. Privat bruk, f.eks. e-post og private filer tillates i begrenset omfang, så lenge det ikke påvirker jobbrelevante oppgaver.
- <Virksomhet> har i utgangspunktet ikke anledning til innsyn i privat e-post eller filer. Unntak gjelder hvis du er ikke-planlagt utilgjengelig i lengre tid, og virksomheten har behov for virksomhetsrelatert informasjon. Det er etablert en egen rutine for slikt innsyn.
- <Virksomhet> har i utgangspunktet ikke anledning til innsyn i privat e-post eller filer. Unntak gjelder ved begrunnet mistanke om straffbare forhold eller ved sikkerhetsmessige behov. Det er etablert en egen rutine for slikt innsyn.
- All prosjektrelatert informasjon skal lagres på prosjektområdene på filservere. Hjemmekatalogen skal primært brukes for informasjon som den enkelte ønsker å ta vare på og som kan benyttes på tvers av prosjekter eller funksjoner som vedkommende utfører.
- Prosjektrelatert informasjon skal ikke lagres på fellesområder.
- Utskrifter skal fjernes fra skriveren så snart utskriftsjobben er ferdig.
- Alle lagringsmedia skal merkes iht. retningslinjer i ref. 8.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-12 Sikkerhetsinstruks bruker.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks bruker	Side 2 av 5

- Prosjektleder er ansvarlig for at tilgang til kunderelatert informasjon følger prinsippet om tilgang i henhold til tjenstlig behov, og gir beskjed til <IT-drift> om tilgangsrettigheter ved opprettelse av nye områder.

2.1 Opplæring

- Før du får tilgang til de aktuelle informasjonssystemene, skal du ha gjennomgått nødvendig opplæring.
- Du er selv ansvarlig for å følge de regler som gjelder for bruk av de forskjellige informasjonssystemene og for behandling av beskyttelsesverdig informasjon i henhold til gjeldende regler, ref. 8.

2.2 Brukernavn, passord og skjermsparer

- Du får tildelt brukernavn og førstegangs passord av <IT-drift>.
- Passord er strengt personlig og skal ikke oppgis til eller lånes ut til andre. Dette er et personlig ansvar.
- Velg et passord som er lett å huske men det skal ikke inneholde navn på familie-medlemmer, fødselsnummer eller andre opplysninger som lett lar seg knytte til brukeren.
- Passordet skal bestå av en kombinasjon av store og små bokstaver og tall/tegn og være på minst 8 tegn. Siste 5 passord skal ikke gjenbrukes.
- Dersom du har mistanke om at passordet har blitt kjent av uvedkommende, skal passordet byttes og hendelsen rapporteres til sikkerhetsansvarlig snarest mulig som et avvik.
- Passordbeskyttet skjermsparer skal benyttes eller kontordør låses når arbeidsplassen forlates i kortere perioder. Maskinen skal også være satt opp med automatisk skjermsparer med aktivering etter 15 minutters inaktivitet.
- Du skal alltid logge ut før du overlater maskinen til andre.

2.3 Oppdatering av antivirusprogram og operativsystem

- Antivirusprogram oppdateres automatisk ved innlogging og deretter hver halve time.
- Operativsystemet oppdateres automatisk for sikkerhetskritiske oppdateringer ved innlogging og en gang om natten.
- Oppdateringer som ikke er kritiske, må godtas av den enkelte bruker.

2.4 Internett

- Alle ansatte har tilgang til å benytte Internett samt sende og motta e-post fra sin lokale arbeidsstasjon/PC.
- Det er ikke tillatt å laste ned utuktig materiale, opphavsrettslig beskyttet materiale (f.eks. musikk, filmer og programvare) eller annet som er i strid med lovverket.
- Tjenester for fildeling og lynmeldinger <virksomhetens eksempler> tillates ikke på grunn av sikkerhetsrisiko knyttet til disse tjenestene.
- Ressurskrevende tjenester, eksempelvis radiolytting og TV/video streaming, skal begrenses for å ikke påvirke negativt jobberelatert trafikk i nettet.
- <Virksomhet> har anledning til å logge informasjon om Internett og e-post trafikk for å sikre alminnelig drift samt for sporing ved eventuelle sikkerhetsbrudd.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-12 Sikkerhetsinstruks bruker.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks bruker	Side 3 av 5

- Det er ikke tillatt å forsøke å forbigå sikkerhetsmekanismer beskrevet i denne sikkerhetsinstruks, for eksempel ved å skjule ikke-tillatte tjenester gjennom andre tjenester.

2.5 E-post

- All e-post (innkommende og utgående) skal gå gjennom <virksomhet>s e-post løsning. Det er derfor ikke tillatt å hente e-post gjennom eksterne POP tjenester eller eksterne web-baserte e-postsystemer.
- Dersom e-post må benyttes for overføring av beskyttelsesverdig informasjon, skal informasjonen sendes som kryptert vedlegg til e-post med godkjent krypteringsprogram. Regler for informasjonshåndtering er beskrevet i ref. 8.
- Brukere er selv ansvarlig for å vurdere hva som er arkivverdig.

2.6 Bærbar PC, PDA og annet portabelt utstyr

- Kontor PC, bærbar PC, PDA og annet portabelt utstyr er i utgangspunktet konfigurert av <IT-drift>. Dette oppsettet skal ikke endres av bruker.
- Beskyttelsesverdig informasjon skal ikke lagres på bærbar PC, PDA eller annet portabelt utstyr med mindre det er installert godkjente sikkerhetsløsninger (normalt med kryptert disk).
- Bærbar PC (Jobb-PC) som benyttes som klient i <virksomhet>-nett, kan benyttes i forbindelse med jobb på reiser og hjemme. Jobb-PC skal ikke benyttes til annet enn jobbrelevante oppgaver.
- Den enkelte bruker er ansvarlig for å håndtere bærbar PC og andre enheter med informasjon i henhold til informasjonens klassifisering, ref. 8.
- La aldri bærbar PC, PDA eller annet bærbart utstyr ligge synlig uten tilsyn.

2.7 Sikkerhetskopiering

- For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelevante informasjon lagres på, eventuelt kopieres til, servere i <virksomhet>-nett.
- For Jobb-PC som benyttes i forbindelse med reiser og hjemmearbeid, må oppdatering mot servere i <virksomhet>-nett gjøres regelmessig, spesielt dersom andre er avhengig av informasjonen.
- Ved behov for gjenoppretting av sikkerhetskopierte informasjon, kontakt <IT-drift>.

2.8 Installasjon av programvare og maskinvare

- Det skal ikke benyttes programvare som avviker fra lisensavtaler til produsenter.
- All lisensiert programvare på maskinen skal godkjennes av <IT-drift>. Dette gjelder både kontor PC, bærbar PC og PDA.
- Dersom du har behov for ytterligere lisensiert programvare, ta kontakt med <IT-drift>.
- All maskinvare og lagringsmedia/harddisk skal være registrert hos <IT-drift>, dersom dette mangler skal <IT-drift> varsles.

2.9 Modem-/bredbåndstilknytninger

- Ekstern tilkopling mot <virksomhet>-nett tillates kun etter godkjenning fra <IT-drift>.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-12 Sikkerhetsinstruks bruker.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks bruker	Side 4 av 5

2.10 Hjemme-PC

- Kunde- eller <virksomhet>-informasjon tillates ikke lagret på privat/hjemme-PC.

2.11 Reparasjon, service og vedlikehold

- Alle feil eller mistanker om feil i informasjonssystemet (både maskinvare og programvare) skal rapporteres til <IT-drift> snarest mulig.
- Det er kun <IT-drift> som kan iverksette arbeid som utføres av eksternt personell på informasjonssystemer og utstyr.

2.12 Håndtering av informasjon og medier

2.12.1 Håndtering

- Dokumenter (papir, foiler etc.) og lagringsmedia, som CD, DVD og disketter, minnepinner etc., skal behandles iht. retningslinjene i ref. 8.

2.12.2 Kassering av medier

- Disker, utstyr som inneholder harddisker og annet lagringsmateriale (f.eks. minnebrikker, backup tape etc.), skal leveres til <IT-drift> for forsvarlig destruksjon.
- Lagringsmedia som CD, DVD, minnepinner og disketter, etc.:
 - Personopplysninger; skal leveres til <IT-drift> for destruksjon.
 - Øvrig klippes/brekkes i biter og kastes i avfall.

3 Fysisk adgang

3.1 Adgangskort

- Dersom du mister nøkkel/nøkkelkort, meld umiddelbart fra til administrasjonen eller sikkerhetsansvarlig.
- Ansatte som slutter eller går ut i permisjon, skal levere nøkkel/nøkkelkort tilbake til administrasjonen.

3.2 Besøkende

Den som mottar besøkende, er ansvarlig for at

- besøkende blir registrert i resepsjonen.
- hentes i resepsjonen og følges tilbake av den som mottar besøket.
- ikke oppholder seg i <virksomhet>s lokaler uten følge av en av de ansatte.

Besøk utenom ordinær arbeidstid skal begrenses.

4 Kontakt med media

Det er kun virksomhetsleder NN eller den hun/han gir ansvaret til, som har myndighet til å uttale seg til presse eller andre media i forbindelse med saker som gjelder IT-sikkerhet, sikkerhetsbrudd eller større hendelser.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-12 Sikkerhetsinstruks bruker.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks bruker	Side 5 av 5

5 Nødhjelp

Brann: Nødnummer 110

Håndslukkingsapparat CO2 og husbrannslange finnes i ◇.

Brannalarm meldes automatisk til ◇ brannvesen.

Ved feil ring ◇ brannvesen telefon ◇.

Politi: Nødnummer 112

Ambulanse: Nødnummer 113

Vann:

Meld fra til administrasjonen.

Stengekran for vann er på rom ◇.

6 Personellsikkerhet

6.1 Sikkerhetsinstruks og taushetserklæring

Ansatte, konsulenter og vikarer skal rette seg etter Sikkerhetsinstruks bruker (dette dokumentet) og underskrive denne, samt taushetserklæring.

6.2 Konsekvenser ved brudd på retningslinjene

Konsekvenser for ansatte som har forårsaket brudd på sikkerhetsreglene, vil bli vurdert i hvert enkelt tilfelle og kan ved alvorlige brudd føre til oppsigelse/avskjed, se virksomhetens reglement.

7 Rapportering og avvik

7.1 Rapportering av sikkerhetsbrudd/hendelser

Meld straks fra til sikkerhetsansvarlig dersom du oppdager sikkerhetsbrudd eller hendelser som kan ha betydning for sikkerheten.

Dersom det oppdages virus/orm/trojaner på diskett/CD-rom, skal <IT-drift> varsles og diskett/CD-rom leveres <IT-drift> umiddelbart.

7.2 Avvikshåndtering

Avvik på denne instruks skal håndteres i henhold til avviksrutine og skal varsles til sikkerhetsansvarlig umiddelbart.

Dersom brukere har prosjektspesifikke behov som avviker fra denne instruks, skal det sendes en anmodning til sikkerhetsansvarlig via avdelingsleder.

8 Referanser

[1] Rutine for informasjonshåndtering

Sikkerhetsinstruksen er lest og akseptert:

Sted og dato: _____

Navn (blokkbokstaver) _____ Signatur: _____

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-12 Sikkerhetsinstruks bruker.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Informasjonshåndtering	Side 1 av 3

Informasjonshåndtering

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

Innledning

Dette dokument er et vedlegg til Sikkerhetsinstruks bruker, ref. .

Klassifisering av informasjon

Informasjon som behandles i <virksomhet> har forskjellig beskyttelsesbehov og er delvis regulert av lovverk. For at brukere skal kunne vite hvordan man skal håndtere informasjonen, gis det i dette dokumentet definisjon av ulike typer informasjon, samt en tabell som viser hvordan den enkelte informasjon skal håndteres.

Følgende beskyttelsesgrader benyttes:

Klassifisering av informasjon	
Beskyttelses-grad	Beskrivelse
ÅPEN ¹	Åpen informasjon er informasjon som er åpent tilgjengelig for alle.
LAV (<Virksomhet> INTERNT)	Informasjon for internt bruk hvor kompromittering, tap eller utilgjengelighet kan føre til: - Uønsket offentliggjøring i media av informasjon som bare skal være tilgjengelig for ansatte - Mindre økonomiske tap - Mindre skade på <virksomhet>s renommé. - Eksempler på informasjon: Interne notater, rundskriv og presentasjoner
MIDDELS	Benyttes dersom det vil kunne <i>skade</i> offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende. Informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til: - At informasjon om <virksomhet> som oppfattes som middels beskyttelsesverdig, kan bli lest/endret av uvedkommende. - Skade på <virksomhet>s renommé. - Risiko for økonomiske tap – under <> kr Eksempler på slik informasjon: - Personopplysninger - Strategier - Adgangskoder
HØY	Benyttes dersom det vil kunne forårsake <i>betydelig skade</i> for offentlige interesser, en bedrift, institusjon eller enkeltperson at informasjonen blir kjent for uvedkommende. Informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til: At informasjon om <virksomhet> som oppfattes som sensitiv, kan bli lest/endret av

¹ Dokumenter med åpen informasjon trenger ikke merkes med beskyttelsesgrad

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-14_ Informasjonshandtering.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Informasjonshåndtering	Side 2 av 3

	uvedkommende. o Alvorlig skade på <virksomhet>s renommé. o Risiko for økonomiske tap – over <> kr Eksempler på slik informasjon: o Sensitive personopplysninger o Sensitive opplysninger om virksomhetens strategi, planer og aktiviteter o Svært sensitiv informasjon om sikkerhetsrelaterte hendelser o Systempassord og andre passord
U.off	Unntatt offentlighet Brukes av offentlige etater. Man må henvise til hvilken paragraf dokumentet unntas etter.

Rutiner for informasjonshåndtering

	ÅPEN	INTERNT) LAV- (VIRKSOMH	Unntatt off.	MIDDELS	HØY
1 Merking					
Dokumenter / informasjon skal være merket med beskyttelsesgrad.		x	x	x	x
Dokumentet / informasjonen skal merkes med hvilken bestemmelse som gir hjemmel for å unnta dokumentet fra offentlighet.			x		
Angi eventuell tidsbegrensning for graderingen					
2 Kopiering					
Dokumenter skal bare kopieres til personer som har autorisasjon for graderingen.		x	x	x	x
3 Oppbevaring					
Ethvert tap eller kompromittering av beskyttelsesverdige dokumenter skal meldes til Sikkerhetsansvarlig og nærmeste linjeleder.		x	x	x	x
Lagres på sikkert område på filsystem hvor kun den/de som skal ha informasjonen har tilgang			x	x	x
Forhindre innsyn fra utenforstående		x	x	x	x
Skal være nedlåst når ikke under oppsyn			x	x	x
Utskrifter					
Utskrifter skal hentes umiddelbart fra skrivere slik at konfidensialitet ("Need to know") i saksbehandlingen opprettholdes			x	x	x
På reise/Hjemme:					
Dokumenter/elektroniske medier skal oppbevares under oppsyn av den ansatte eller avlåst			x	x	x
Lagres kryptert på bærbar PC, eller annet portabelt utstyr			x	x	x
4 Forsendelse/elektronisk håndtering					
Fysiske dokumenter (papir) sendes i posten i lukket konvolutt	x	x	x	x	x
Skal ikke overføres som e-post på Internett					x
Sendes som kryptert fil / kryptert vedlegg til e-post på Internett Sørg for å få kvittering fra mottaker om at e-posten er mottatt.			x	x	
Kan sendes som normal (ukryptert) e-post	x	x			
Tillatt å sende på telefax	x	x			
Informasjonen skal ikke kommuniseres på steder hvor samtale kan overhøres av utenforstående.			x	x	x

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-14 Informasjonshandtering.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Informasjonshåndtering	Side 3 av 3

	ÅPEN	INTERNT/LAV- (VIRKSOMH)	Unntatt off.	MIDDELS	HØY
5 Journalføring					
Føres i journal unntatt offentlighet (ved mottak / forsendelse)			x	x	x
Føres i åpen journal (ved mottak / forsendelse)	x	x	x ²	x ²	
6 Makulering av dokumenter					
Papir legges i egne makuleringsdunker		x	x	x	x
Papir kastes i papiravfall / avfall	x				
7 Håndtering av datalagringsmedia					
Disker, utstyr som inneholder harddisker og annet lagringsmateriale (f.eks. minnebrikker, backuptape etc.), skal leveres til IKT-kontoret for forsvarlig destruksjon.	x	x	x	x	x
Lagringsmedia som CD, DVD og floppy-disker leveres til IKT-kontoret for destruksjon			x	x	x
Lagringsmedia som CD, DVD og floppy-disker klippes/brekkes i biter og kastes i avfall	x	x			
Reparasjon / Service:					
Datautstyr sendes IKT-kontoret	x	x	x	x	x

Referanser

- [1] Personopplysningsloven m. forskrifter
<http://www.lovdata.no/all/nl-20000414-031.html>
- [2] Sikkerhetsinstruks - brukere for <virksomhet>

² Hvis det føres offentlig journal, kan disse føres i åpen journal i stedet for journal unntatt offentlighet dersom journalføringen ikke røper fortrolige opplysninger. Nøytrale kjennetegn, utelatelser eller overstrykninger skal benyttes i kopi av journal som legges frem for publikum for å unngå at fortrolig informasjon røpes

²

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-14 Informasjonshandtering.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sjekkliste nyansatt / slutter	Side 1 av 2

Sjekkliste nyansatt / slutter

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

Denne malen dekker kun sikkerhetsaspektene ved tiltredelse for nyansatt og når arbeidsforhold opphører for ansatt.

Navn: _____

1 Sjekkliste - nyansatt

<Fylles ut av administrasjon og oppbevares sammen med andre personaldata.>

Eksempel:

Sjekkpunkter:	Ok Dato:
<Virksomhets> taushetserklæring underskrevet 1. arbeidsdag.	
Sikkerhetsinstruks for <Virksomhet> delt ut 1. arbeidsdag.	
Kontornøkler og adgangskort med begrenset adgang utlevert 1. arbeidsdag.	
Sikkerhetsinstruks for <Virksomhet> gjennomgått og signert (i løpet av de første 2 uker.	

2 Sjekkliste - opphør av arbeidsforhold

<Fylles ut av administrasjon og oppbevares sammen med andre personaldata.>

Eksempel:

Sjekkpunkter:	Ok Dato:
Kundeinformasjon inkl. e-post og filer er gjennomgått med avdelingsleder og overlevert.	
Privat e-post og private filer er slettet.	
Graderte/firma sensitive dokumenter er levert administrasjon for makulering eller arkivering.	

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-15 Sjekkliste nyansatt slutter.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sjekkliste nyansatt / slutter	Side 2 av 2

<i>Arkivskap, hyller og reoler er ryddet og tømt.</i>	
<i>Datalagringsmedia, PC og mobiltelefon er levert IT-drift.</i>	
<i>Sikkerhetssamtale med sikkerhetsansvarlig er gjennomført i forbindelse med avtalt taushetsløfte. Kopi av taushetserklæringer leveres ved ønske.</i>	
<i>Adgangskort og nøkler er levert administrasjonen</i>	
<i>Adgangskort er sperret.</i>	

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-15 Sjekkliste nyansatt slutter.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Taushetserklæring	Side 1 av 3

Taushetserklæring

NB! Innholdet i denne malen må tilpasses egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

Jeg forplikter meg herved til ikke å bruke, åpenbare, utlevere eller på annen måte gjøre tilgjengelig for uvedkommende informasjon om data og bedrifts- eller forretningshemmeligheter, personopplysninger, eller bedrifts- eller forretningsmessig know-how som jeg har fått kjennskap til i mitt arbeid ved bedriften.

Jeg vil også vise aktsomhet i omtale av andre forhold som jeg blir kjent med eller erfarer under mitt arbeid.

Jeg har lest de lovbestemmelser som er anført på de neste sidene av denne erklæring. Jeg er dermed klar over straffelovens §145, §294 og §405a samt markedsføringslovens §7 og §8. Brudd på disse bestemmelsene kan medføre straffeansvar, oppsigelse eller avskjed.

Jeg er også klar over at denne taushetserklæring gjelder etter opphør av ansettelsesforholdet eller oppdraget i henhold til lovene referert i avsnittet ovenfor.

....., den

Sted Dato

.....

Underskrift

.....

Navn i blokkbokstaver

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-16 Taushetserklaering.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Taushetserklæring	Side 2 av 3

AVSKRIFT AV DE VIKTIGSTE LOVBESTEMMELSER SOM VIL KUNNE
KOMME TIL ANVENDELSE VED UBERETTIGET BRUK OG ÅPENBARING AV
DATA og BEDRIFTSHEMMELIGHETER

Lov nr 10 av 22. mai 1902: Almindelig borgerlig Straffelov (Straffeloven).

§ 294. Med Bøder eller Fængsel indtil 6 Maaneder straffes den, som

1. ved at fremkalde eller styrke en Vildfarelse retsstridig forleder nogen til en Handling, hvorved der voldes denne eller nogen, paa hvis Vegne han handler, Formuestab, eller som medvirker hertil, eller
2. uberettiget enten selv gjør Brug af en Forretnings- eller Driftshemmelighed vedkommende en Bedrift, hvori han er eller i Løbet af de 2 sidste Aar har været ansat, eller hvori han har eller i Løbet af de 2 sidste Aar har havt Del, eller aabenbarer en saadan i Hensigt at sætte en anden i stand til at gjøre Brug af den, eller som ved Forledelse eller Tilskyndelse medvirker hertil, eller
3. uberettiget gjør bruk av en bedrifts forretnings- eller bedriftshemmelighet som han har fått kjennskap til eller rådighet over i egenskap av teknisk eller merkantil konsulent for bedriften eller i anledning et oppdrag fra den, eller uberettiget åpenbarer en slik hemmelighet i den hensikt å sette andre i stand til å gjøre bruk av den, eller som ved forledelse eller tilskynding medvirker til dette.

Offentlig Paataale finder alene Sted, naar det begjæres af fornærmede og findes paakrævet af almene Hensyn.

§ 405a. Med bøter eller fengsel inntil 3 måneder straffes den som på urimelig måte skaffer seg eller søker å skaffe seg kunnskap om eller rådighet over en bedriftshemmelighet.

LOV 1972-06-16 nr 47: Lov om kontroll med markedsføring og avtalevilkår (markedsføringsloven).

§ 7. *Bedriftshemmeligheter.*

Den som har fått kunnskap om eller rådighet over en bedriftshemmelighet i anledning av et tjeneste-, tillitsvervs- eller forretningsforhold, må ikke retsstridig utnytte hemmeligheten i næringsvirksomhet.

Det samme gjelder den som har oppnådd kunnskap om eller rådighet over en bedriftshemmelighet gjennom noens brudd på taushetsplikt eller gjennom noens rettsstridige handling ellers.

§ 8. *Tekniske hjelpemidler.*

Den som er blitt betrodd tekniske tegninger, beskrivelser, oppskrifter, modeller eller liknende tekniske hjelpemidler i anledning av et tjeneste-, tillitsvervs- eller forretningsforhold, må ikke retsstridig utnytte dem i næringsvirksomhet.

Det samme gjelder den som har oppnådd rådighet over tekniske tegninger, beskrivelser, oppskrifter, modeller og liknende tekniske hjelpemidler gjennom noens rettsstridige handling.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-16 Taushetserklaering.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Taushetserklæring	Side 3 av 3

Lov 2005-04-08 nr 16 Lovtiltak mot datakriminalitet (Straffeloven)

§ 145. Den som uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer, straffes med bøter eller med fengsel inntil 6 måneder eller begge deler.

Det samme gjelder den som uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler.

Voldes skade ved erverv eller bruk av slik uberettiget kunnskap, eller er forbrytelsen forøvet i hensikt å skaffe noen en uberettiget vinning, kan fengsel inntil 2 år anvendes.

Medvirkning straffes på samme måte.

Offentlig påtale finner bare sted når allmenne hensyn krever det.

Endret ved lover 16 feb 1979 nr. 3, 12 juni 1987 nr. 54, 8 april 2005 nr. 16.

§ 145a. Med bøter eller fengsel inntil 6 måneder straffes den som

1. ved hjelp av hemmelig lytteapparat avlytter telefonsamtale eller annen samtale mellom andre, eller forhandlinger i lukket møte som han ikke selv deltar i, eller
2. ved hjelp av lydbånd eller annen teknisk innretning hemmelig gjør opptak av samtale som foran nevnt eller av forhandlinger i lukket møte som han enten ikke selv deltar i, eller som han har skaffet seg adgang til ved falske foregivender eller ved å snike seg inn, eller
3. anbringer lytteapparat, lydbånd eller annen teknisk innretning i øyemed som foran nevnt.

Medvirkning straffes på samme måte.

Offentlig påtale finner bare sted når det kreves av almene hensyn.

Tilføyd ved lov 12 des 1958 nr. 1.

§ 145b. Den som uberettiget gjør tilgjengelig for andre passord eller andre data som kan gi tilgang til et datasystem, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler.

Grov spredning av tilgangsdata straffes med fengsel inntil 2 år. Ved avgjørelsen av om spredningen er grov, skal det særlig legges vekt på om dataene kan gi tilgang til sensitive opplysninger, om spredningen er omfattende og om handlingen for øvrig skaper fare for betydelig skade.

Medvirkning straffes på samme måte.

Tilføyd ved lov 8 april 2005 nr. 16.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-16 Taushetserklæring.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks - leder	Side 1 av 2

Sikkerhetsinstruks - leder

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Innledning

<Virksomhet> er underlagt Personopplysningsloven og tilhørende krav til informasjonssikkerhet. Dette dokumentet inneholder sikkerhetsinstruks for ledere med personalansvar i <Virksomhet>. Denne kommer i tillegg til generelle brukerrelaterte rutiner (se ref. -).

2 Sikkerhetsinstruks

2.1 Ansettelse

Sjekkliste for ansettelse av fast ansatte:

- 1) Taushetserklæring leses og underskrives av den ansatte.
- 2) Sikkerhetsinstruks leses og underskrives av den ansatte.
- 3) Rutine for informasjonshåndtering skal leses av den ansatte.
- 4) Utlevere eventuelle nøkler, nøkkeltast, koder e.l.
- 5) Punktene 1-5 over skal gjennomføres før brukertilganger gis. Leder skal deretter informere <IT-avdelingen> om behov for brukertilganger. Vær spesielt oppmerksom på hvor lenge det er behov for tilgangen samt nivå på tilgang. Benytt <felles> autorisasjonsskjema for de ulike systemer. Disse finnes på <Virksomhet>s Intranettsider.

Sjekkliste for bruk av konsulenter og andre midlertidige ansatte:

- 1) Taushetserklæring leses og underskrives.
- 2) Sikkerhetsinstruks skal leses og underskrives.
- 3) Rutine for informasjonshåndtering skal leses.
- 4) Dersom det er behov for autorisasjon til informasjonssystemet, skal dette avklares med systemeier, eventuelt sikkerhetsansvarlig, før autorisasjonsskjema sendes <IT-avdelingen>.
- 5) Utlevere eventuelle nøkler, nøkkeltast, koder e.l.
- 6) Punktene 1-5 over skal gjennomføres før brukertilganger gis. Ledere skal deretter informere <IT-avdelingen> om behov for brukertilganger. Vær spesielt oppmerksom på hvor lenge det er behov for tilgangen og nivå på tilgang.

Leder er ansvarlig for å oppbevare en kopi av underskrevet erklæring og instruks samt autorisasjonsskjema for alle som inngår i personalansvaret. Original autorisasjonsskjema sendes i tillegg til <IT-avdelingen>.

2.2 Regelmessig verifikasjon av brukerkonti og brukertilganger

<IT-avdelingen> vil regelmessig sende ut oversikt over relevante definerte brukere og brukertilganger til leder med personalansvar.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-17 Sikkerhetsinstruks leder.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks - leder	Side 2 av 2

Leder skal så snart som praktisk mulig etter mottak, verifisere at oversikten er korrekt, dvs reflekterer ansvar og organisasjonsmessig tilhørighet. Eventuelle feil og mangler skal formidles <IT-avdelingen> på e-post eller fax. Leder skal oppbevare kopi av alle meldte endringer.

2.3 Endring av arbeidsforhold/ansvar

Ved endringer av ansvar eller organisasjonsmessig tilhørighet internt i <Virksomhet> skal brukerens tilganger i informasjonssystemet vurderes. <IT avdelingen> skal informeres om eventuelle relevante endringer i behov for tilgang på informasjonssystemene. Leder skal oppbevare kopi av alle meldte endringer.

2.4 Hendelser med betydning for sikkerheten

Sikkerhetsrelaterte hendelser av alvorlig karakter skal rapporteres til <Sikkerhetsansvarlig>.

2.5 Konsekvenser ved brudd på retningslinjene

Brudd på <Virksomhet>s sikkerhetsregler er å betrakte som tjenesteforsømmelse, og skal vurderes i det enkelte tilfelle.

2.6 Permisjoner eller andre typer midlertidige arbeidsopphold

Leder skal vurdere innlevering av nøkler/adgangskort/utlånt utstyr samt påse at sensitiv informasjon er nedlåst.

2.7 Avslutning av arbeidsforhold

Leder skal verifisere at arbeidstaker har levert <Virksomhet>s eiendeler:

- Mobiltelefon
- Bærbar Pc
- Nøkler
- Adgangskort

Leder skal:

- verifisere at arbeidstaker har signert for levering <Virksomhet> eiendeler og rydding i dokumentasjon og filer, ref skjema
- gi beskjed til <IT-avdelingen> om sperring av brukerkonti med brukertilganger.
 - Oppbevare kopi av beskjed til <IT-avdelingen>

Referanser

- [1] Sikkerhetsinstruks - bruker
 [2] Informasjonshåndteringsrutine
 [3] Taushetserklæring

Sikkerhetsinstruksen er lest og akseptert:

Sted og dato: _____

Navn (blokkbokstaver) _____ Signatur: _____

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-17 Sikkerhetsinstruks leder.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Sikkerhetsinstruks - sikkerhetsansvarlig	Side 1 av 1

Sikkerhetsinstruks - sikkerhetsansvarlig

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Innledning

Sikkerhetsansvarlig rapporterer til Daglig leder/Administrerende direktør og er nærmeste overordnede for følgende roller:

Administrasjonen; med håndtering av:

- Fysisk sikkerhet
- Arkivering og post
- Personell og sikkerhet

2 Sikkerhetsinstruks

Sikkerhetsansvarlig har følgende ansvarsområder:

- Utarbeide og vedlikeholde regime for Internkontroll.
- Ansvarlig for vedlikehold av dokumentet **Oversikt over personopplysninger**.
- Påse at de gjeldende sikkerhetsbestemmelse, instruks og rutiner blir fulgt.
- Påse at underlagte sikkerhetsledd har klart definerte oppgaver/forhold for å utøve sine funksjoner, og virkelig utøver disse.
- Ansvar for at administrasjonen utøver sitt ansvarlig for fysisk sikkerhet, personell og sikkerhet og dokumentsikkerhet.
- Utføre ikke anmeldte inspeksjoner på dag- eller nattid på kontorer, møterom og andre lokaler han/hun finner grunn til å inspisere.
- Påtale mislighold muntlig eller skriftlig, avhengig av misligholdets karakter.
- Sørge for at alle ansatte har kjennskap til regimet for Internkontroll og tilhørende sikkerhetsbestemmelser, instruks og rutiner .
- Ha sikkerhetssamtaler ved ansettelse og ved avslutning av et ansettelsesforhold.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-19_Sikkerhetsinstruks_sikkerhetsansvarlig.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Beskrivelse av informasjonssystemet	Side 1 av 5

Beskrivelse av informasjonssystemet

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Arkitektur

1.1 Funksjonell arkitektur

<Overordnet tegning med støttende beskrivelse av hvordan de ulike elementene i IT-infrastrukturen spiller sammen for å oppnå hensikten med løsningene for brukerne av tjenestene.>

1.2 Sikkerhetsarkitektur

<Overordnet tegning med støttende beskrivelse av hvordan de ulike elementene i sikkerhetskonseptet spiller sammen for å oppnå beskyttelse av personopplysningene og beskyttelse av tjenestene til brukerne i overensstemmelse med akseptabelt risikonivå.>

2 Grensesnitt ut av / inn til virksomheten

2.1 Logiske grensesnitt

2.2 Fysiske forbindelser

3 Internt ruter / IP-nett

3.1 Adresseplan

3.2 Nettverkstjenester

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 21 Beskrivelse av informasjonssystemet.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Beskrivelse av informasjonssystemet	Side 2 av 5

4 Nettverkskomponenter

4.1 Rutere

4.2 Svitsjer

4.3 Brannmurer

5 Overvåking

5.1 Driftsovervåking

5.2 Nettverksovervåking

6 Logging

<Beskrivelse av loggfunksjoner, formater og loggfiler>

7 Andre sikkerhetstiltak

<Henvisning til besluttede sikkerhetstiltak etter risikoanalyse med hensyn på konfidensialitet, integritet og tilgjengelighet.>

7.1 Redundans

7.2 Tilgjengelighetsovervåking

7.3 Tilgangskontroll

7.4 Kryptering

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 21 Beskrivelse av informasjonssystemet.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Beskrivelse av informasjonssystemet	Side 3 av 5

7.5 Integritetsovervåking

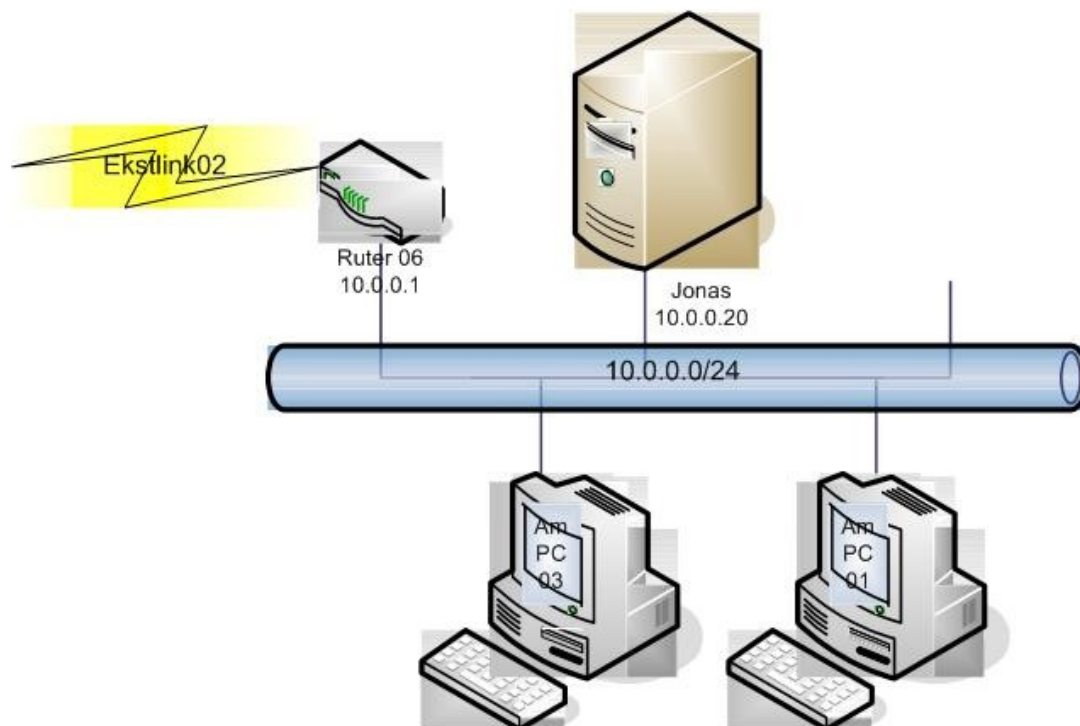
8 Vedlegg

8.1 Konfigurasjonskart

8.1.1 Nettverkstegning

Nettverkstegning med beskrivelse av

- navn på nettverksutstyr,
- IP-nettadresser (eventuelt adresseområder) og nettverksmasker og
- IP-adresser for sentrale servere.



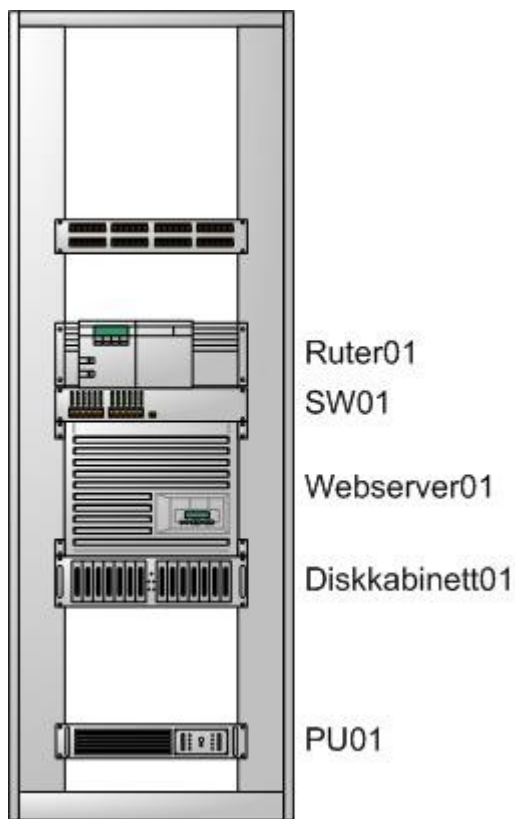
8.1.2 Konfigurasjon - Nettverk

<Utskrift av oppsett av utstyr og programvare eller kopi av oppsett til elektronisk fil som inngår i sikkerhetskopiering>

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 21 Beskrivelse av informasjonssystemet.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Beskrivelse av informasjonssystemet	Side 4 av 5

8.1.3 Fysisk montering (skap)



8.2 Beskrivelse av informasjonssystem <navn>

8.2.1 Tjenester / applikasjoner / sluttbrukere

8.2.2 Personopplysninger

<Referanse til Oversikt over personopplysninger>

8.2.3 Programvare / plattform

<Opplisting eller tabellbeskrivelse av programvare som inngår i konfigurasjonen med minimum beskrivelse av

- "Navn" eller identitet i IT infrastrukturen
- Produsent
- Type
- Versjon>

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 21 Beskrivelse av informasjonssystemet.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Beskrivelse av informasjonssystemet	Side 5 av 5

8.2.4 Maskinvare / plattform

<Opplisting eller tabellbeskrivelse av utstyr som inngår i konfigurasjonen med minimum beskrivelse av

- "Navn" eller identitet i IT infrastrukturen
- Produsent
- Type
- Versjon>

8.2.5 Oppsett av maskinvare og programvare

<Utskrift av oppsett av maskinvare og programvare eller kopi av oppsett til elektronisk fil som inngår i sikkerhetskopiering>

8.2.6 Nettverk / evt. eksterne grensesnitt

8.2.7 Sikkerhetstiltak

<Henvisning til beskyttelsesbehov for systemet og hva som er implementert iht. krav/kategorier med hensyn til konfigurasjon/integritet og tilgjengelighet

8.2.7.1 Tilgangskontroll

<Benytt henvisning hvis tilgangskontroll er standardisert i virksomheten og beskrevet i hoveddokumentet>

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 21 Beskrivelse av informasjonssystemet.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Driftsrutiner	Side 1 av 1

Driftsrutiner

<I denne malen plasseres alle driftsrutiner som er aktuelle for virksomheten for internkontroll og informasjonssikkerhet som følge av krav i Veileder - internkontroll og informasjonssikkerhet.

Dette gjelder rutiner som er nødvendige utover rutinene beskrevet i dokumentet Rutiner for informasjonssikkerhet.

Bruk denne malen for rutiner som eksempelvis:

- Sikkerhetskopiering
- Test av sikkerhetskopiering
- Gjennomgang av brukertilganger
- Oppdatering av programvare og operativsystem
- Endringer i informasjonssystemet
- Kontroll av informasjonssystemet (feillogger, lagringsplass, etc)
- Test av nødstrøm>

1 <Driftsrutine 1>

1.1 Rutinebeskrivelse

Mal for rutinebeskrivelse:

1. Hvorfor skal rutinen utarbeides, hva er hensikten med den
2. Hvem er ansvarlig for å utføre de ulike aktivitetene
3. Hva skal utføres av de ulike ansvarlige
4. Hvordan skal aktivitetene utføres
5. Når skal de ulike aktivitetene utføres (eller under hvilke betingelser)
6. Hva er forventet resultat ved utførelse av rutinen

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-22_Driftsrutiner.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Overordnet IT beredskapsplan	Side 1 av 7

Overordnet IT beredskapsplan

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Eksemplet er tilpasset virksomheter med et vesentlig behov for å sikre tilgjengelighet.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Innledning

1.1 Generelt

Hensikten med beredskapsplanlegging 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 ref. [1] ”Sikkerhetsmål og -strategi”.

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

1.2 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

1.3 Omfang

Beredskapsplanen gjelder for de systemer, tjenester og infrastruktur som behandler elektronisk informasjon som tilhører <Virksomhet>. Systemer som skal omfattes av

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 23 Overordnet IT beredskapsplan.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Overordnet IT beredskapsplan	Side 2 av 7

beredskapsplanen må klassifiseres i henhold til beskyttelsesbehov (Konfidensialitet, Integritet og tilgjengelighet).

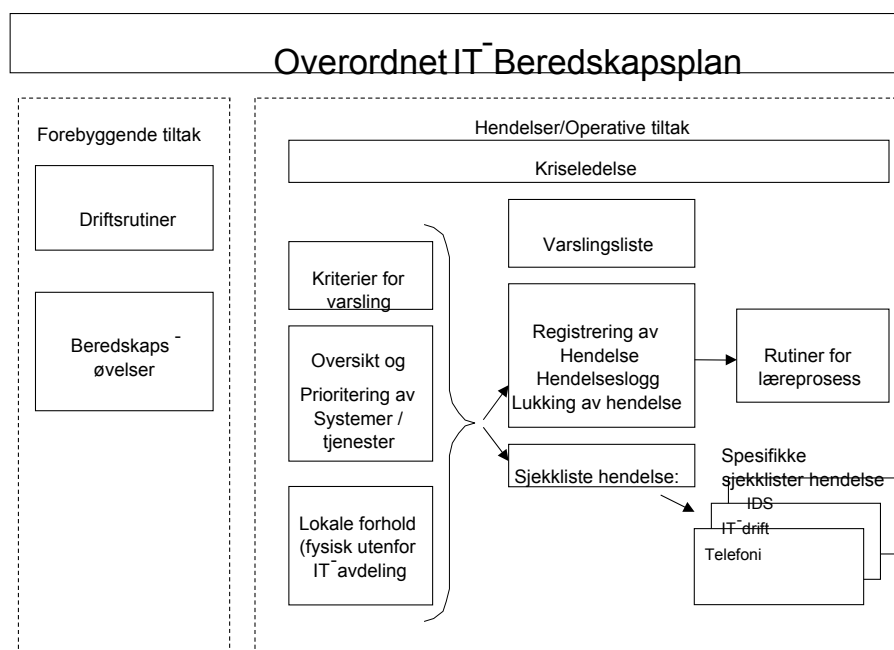
Beredskapsplanens detaljeringsgrad gjenspeiler de ulike systemenes beskyttelsesbehov (for eksempel Meget høyt, Høyt, Middels og Lavt).

2 Struktur IT beredskapsplan

<Virksomhet>'s IT beredskapsplan 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 IT beredskapsstrukturen bestå av organisering og et antall underliggende dokumenter og rutiner som inngår i operativ beredskapsplan.

Figur 1 viser overordnet struktur med dokumentasjon og roller.



Figur 1 Struktur beredskapsplaner <Virksomhet>

2.1 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

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-23 Overordnet IT beredskapsplan.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Overordnet IT beredskapsplan	Side 3 av 7

	• 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.

2.2 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 IT beredskapsplan. Ansvarlig for oppdatering og vedlikehold av driftsrutinene er IT-avdeling ved IT driftsansvarlig. Det utøvende ansvar er delegert til hver enkelt avdelingsleder.

2.3 Hjelpemidler ved hendelse

Beredskapsplanen omfatter et antall roller, rutiner og dokumenter som er gruppert i "hjelpemidler ved hendelse" (se Figur 1). Disse hjelpemidlene utgjør den operative delen av IT beredskapsplanen til <Virksomhet> internt. Følgende roller og rutiner kan inngå:

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

3 Ansvar og roller

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

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.	

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-23 Overordnet IT beredskapsplan.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Overordnet IT beredskapsplan	Side 4 av 7

Rolle	Beskrivelse av ansvar	Kommentar
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> 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.	

Tabell 1 - Oversikt over IT beredskapsplanens roller og ansvar

4 Organisering

4.1 Hendelseshåndtering ved <Virksomhet>

Beskrivelse av blant annet:

- Hvordan brukerhenvendelser og IT relaterte hendelser håndteres.
- 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).

4.2 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 xx.xx - xx.xx).
- Mottak av meldinger om alvorlige hendelser.
- Oversikt over varslingskjeden.

4.3 Rutiner for kriseledelse

Beskrivelse av blant annet

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-23 Overordnet IT beredskapsplan.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Overordnet IT beredskapsplan	Side 5 av 7

- informasjon til brukere med status på hendelseshåndtering, forventet tid for feilretting osv.

Rolle	Ansvar	Kommentar
Kriseleder	(Blant annet:) - 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.	

Tabell 2 – Kriseleders ansvar

Figur kan vise hvilke parter som normalt er involvert ved håndtering av alvorlige hendelser/kriser.

Figur x Skjematisk framstilling av involverte parter i krisehåndtering

4.3.1 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 av uvedkommende og
- alle hendelser som medfører mistanke om at informasjon er blitt kjent av uvedkommende inkludert alle hendelser hvor sensitive personopplysninger har kommet eller mistenkes å ha kommet uvedkommende i hende.

4.4 Verktøykasse for håndtering av alvorlige hendelser

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

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

4.5 Læreprosess/Avvikshåndtering

Systematisk læreprosess, både etter hendelser og etter beredskapsøvelser, kan beskrives.

5 Forebyggende administrative tiltak

- Oppfølging av hendelser.
- Endringskontroll og konfigurasjonsstyring.
- Avtaler med leverandører.
- Trusselvurdering.
- Beredskapsøvelser / tester.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 23 Overordnet IT beredskapsplan.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Overordnet IT beredskapsplan	Side 6 av 7

6 Forebyggende tekniske tiltak for systemer og tjenester

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

		Systemer/tjenester med krav til tilgjengelighet				Merknad
Krav til:		Lavt	Middels	Høyt	Meget høyt	
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 egenkontroll/ 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 varslings 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

Tabell 3 – Generelle IT beredskapstiltak

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 23 Overordnet IT beredskapsplan.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Overordnet IT beredskapsplan	Side 7 av 7

7 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 IT sikkerhetsansvarlig. Planene skal revideres/oppdateres ved behov, eksempelvis

- <...>

8 Referanser

[1] Sikkerhetsmål og -strategi

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2- 23 Overordnet IT beredskapsplan.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Fysisk sikkerhet	Side 1 av 1

Fysisk sikkerhet

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Beskyttede områder

<Her beskrives fysiske områder av virksomheten og/eller hele bygninger som skal beskyttes som følge av behandling av personopplysninger.>

2 Adgangskontroll

<Her beskrives rutiner og tekniske tiltak for adgangskontroll til beskyttede områder.>

3 Tiltak mot innbrudd, vannskade og brann

<Her beskrives rutiner og tekniske tiltak for å forhindre og redusere eventuelle skader ved innbrudd, vanninntrengning og brann.>

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 2-24_Fysisk_sikkerhet.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Avvikshåndtering og egenkontroll	Side 1 av 5

Avvikshåndtering og egenkontroll

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Avvikshåndtering

Hva er et avvik: Enhver hendelse eller tilstand som bryter med <Virksomhet>s internkontroll.

1.1 Behandling av hendelser

Hendelser kan defineres inn i følgende kategorier:

- Avvik fra gjeldende rutiner
- Hendelser som kan ha sikkerhetsmessig konsekvens
- Utført av ansatte, som brudd på sikkerhetsbestemmelser
- Utført av eksterne, som fysisk innbrudd, elektroniske angrep
- Beredskapshendelser

1.2 Hensikt

Rutiner for rapportering av hendelser og håndtering av avvik skal sikre at man har mulighet til å gjøre forbedringer i internkontrollen og at eventuelle sikkerhetsbrudd rapporteres til ansvarlig person. På denne måten kan organisasjonen lære av avvik, og sette i gang tiltak for å forbedre tilstanden i virksomheten.

1.3 Utførelse

Alle ansatte er ansvarlig for å rapportere avvik fra gjeldende rutiner og andre hendelser til den som er ansvarlig for det aktuelle området eller sikkerhetsansvarlig. Feil i programvare og maskinvare rapporteres til IT-drift.

Sikkerhetshendelser og beredskapshendelser krever ofte en rask reaksjon og må rapporteres omgående, muntlig eller helst som e-mail.

Avvik håndteres av linjeleder eller sikkerhetsansvarlig avhengig av avvikets art. Avviket registreres i det verktøyet som er formålstjenlig, men på en slik måte at det er enkelt å få oversikt over status på avvik og korrigerende tiltak.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-01 Avvikshandtering og egenkontroll.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Avvikshåndtering og egenkontroll	Side 2 av 5

1.4 Sikkerhetshendelser

1.4.1 Utført av ansatte

1.4.1.1 Bevisste sikkerhetsbrudd

Dersom det avdekkes tegn på bevisste sikkerhetsbrudd som f eks:

- Misbruk av virksomhetens IKT-systemer
- Tyveri av virksomhetens eiendom
- Tilsiktet spredning av ondsinnet programvare
- Forsøk på å sende sensitive personopplysninger i e-post/vedlegg

Sikkerhetsansvarlig skal varsle personalansvarlig og disse skal sammen avgjøre tiltak.

1.4.1.2 Brudd på generell taushetsplikt

Brudd på den generelle taushetsplikten fra ansatte eller tidligere ansatte skal rapporteres til sikkerhetsansvarlig som vurderer hvilke tiltak som skal iverksettes.

1.4.2 Utført av eksterne

Alle innbrudd og forsøk på innbrudd skal politianmeldes.

Alle elektroniske angrep som medfører økonomiske konsekvenser for virksomhet, skal vurderes anmeldt til Politiet.

1.5 Beredskapshendelser

IT-drift skal håndtere alle beredskapshendelser og rapportere dette på utarbeidet skjema.

1.6 Avviksliste og rapportering

Avviksliste skal holdes løpende oppdatert og kan inneholde:

- Dato
- Beskrivelse
- Kilde
- Avdeling/systemområde
- Alvorlighet
- Status
- Ansvarlig for oppfølging
- Frist for neste oppfølgingspunkt
- Kommentar / korrektivt tiltak

Sikkerhetsansvarlig er ansvarlig for at det utarbeides en årlig rapport fra avviksbehandling til Ledelsens gjennomgang.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-01 Avvikshandtering og egenkontroll.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Avvikshåndtering og egenkontroll	Side 3 av 5

2 Egenkontroll

2.1 Plan

Sikkerhetsansvarlig er ansvarlig for at det opprettes og vedlikeholdes en plan over egenkontrollaktiviteter.

<Planen bør dekke et tidsrom på minimum ett år men kan løpe over flere år. Det kan være ønskelig å gjøre en grundig kontroll av noen områder eller avdelinger i virksomheten sjeldnere enn en gang pr. år men det skal fremgå av planen at alle aktuelle områder eller avdelinger dekkes i løpet av 2 - 5 år.>

Eksempel:

Egenkontrolltiltak	Eier av aktivitet	Frekvens	Resultat
Test av uautorisert fysisk adgang til virksomhets lokaler og kontorer	Eiendom og Sikkerhet	Årlig	
Brukeres tilgangsrettigheter. Avdelingsleder sjekker liste tilsendt fra IT-avdeling og kvitterer denne. IT-drift gjør nødvendige oppdateringer	IT-drift	Halvårlig	
Gjennomgang av privilegerte brukers tilgangsrettigheter – administrator rettigheter	IT-drift, telefoni og system	Halvårlig	
Bekreft skifte av administratorpassord.	IT-drift, telefoni og system	Årlig / når driftspersonel l slutter	
Verifikasjon og evt oppdatering av konfigurasjonskart - Nettverk	IT-drift	Halvårlig/ved endringer	
Kontroll av liste over IT-utstyr og lagringsmedia	IT-drift	Årlig / ved endringer	
Gjennomgå status på oppdatering av antivirusprogram på hver enkelt PC/server	IT-drift	Kvartal/stikkprøver	
Gjennomføring av sikkerhetstester (virksomhetskritiske applikasjoner og infrastruktur)	Sikkerhetsansvarlig	Ved endringer	
Sikkerhetsovervåking IDP (Intrusion Detection Prevention) av kritiske servere samt eksterne forbindelser.	IT-drift	Kontinuerlig	
Bekreft regelsett i IDP	IT-drift	Årlig /ved endringer	

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-01 Avvikshandtering og egenkontroll.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Avvikshåndtering og egenkontroll	Side 4 av 5

Periodisk måling av opptid på viktige og prioriterte systemer.	IT drift og telefoni	Periodisk	
Bekreftelse herding av nettverksenheter, inklusiv sjekk av sikkerhetskopi av svitsje/ruterkonfigurasjon	IT-drift	Årlig	
Bekreftelse herding av servere	IT-drift	Årlig / ved endringer	
Bekreftelse av fungerende sikkerhetskopi. For de systemer der dette er gjort som en del av vanlig drift, kreves ikke egen separat egenkontroll aktivitet	IT-drift og telefoni	Årlig / ved endringer	
Bekreftelse av kjennskap -håndteringsrutiner	sikkerhetsansvarlig	Årlig	
Verifikasjon av etterlevelse -håndteringsrutiner	sikkerhetsansvarlig	Årlig	

2.2 Rutine

Egenkontroll gjennomføres i henhold til dokumentert plan av enheten som "eier" aktiviteten.

Sikkerhetsansvarlig har ansvar for å følge opp at planlagte aktiviteter blir gjennomført.

2.3 Rapportering

Resultater fra egenkontrollaktiviteter skal dokumenteres og rapporteres til sikkerhetsansvarlig.

Avvik som avdekkes i forbindelse med egenkontroll, varsles/rapporteres som beskrevet i kapittel 1.

Sikkerhetsansvarlig er ansvarlig for at det utarbeides en årlig rapport fra egenkontroll til Ledelsens gjennomgang.

3 Gjennomgang av rutiner

Rutiner for håndtering av personopplysninger og for informasjonssikkerhet bør gjennomgås periodisk for å sikre at rutinene er

- oppdaterte i henhold til interne og eksterne forhold,
- hensiktsmessige og
- tilstrekkelige.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-01 Avvikshandtering og egenkontroll.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Avvikshåndtering og egenkontroll	Side 5 av 5

Periodisk gjennomgang bør inngå i egenkontrollplan, ref. kapittel 2. I tillegg kan det være behov for gjennomgang og oppdatering utover dette ved betydelige endringer i interne eller eksterne forhold.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-01 Avvikshandtering og egenkontroll.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Avviksskjema	Side 1 av 1

Avviksskjema

<Se veilederen Internkontroll og informasjonssikkerhet for veiledning til utfylling.>

Avviksskjema	Virksomhet: XX	Sendes til: Sikkerhetsansvarlig	Saksident: xxxx
Formål: Skjemaet skal sikre at alle brudd og antatte brudd på håndteringsrutiner eller sikkerhetsrutiner blir registret og behandlet på forsvarlig måte.			
Beskrivelse av avviket: xxxxxxx xxxxxxx vedlegg:			
Beskrivelse av midlertidig tiltak: xxxxxxx xxxxxxx vedlegg:			
Melderens registrering	Navn: XXXXXXXXXX	utstyr/ident: XXXXXXXXXX	dato/ kl: XXXXXXXXXX
Analyse av årsak: xxxxxxx xxxxxxx Vedlegg:			
Beskrivelse av iverksatte tiltak: xxxxxxx xxxxxxx Henv:			
Sikkerhetsansvarliges Behandling	Klassifikasjon: XXXXXXXXXX	Rapport sendes Datatilsynet: JA / NEI	dato / underskrift: NN
Evaluert dato:			

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-02_Avviksskjema.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Egenkontrollskjema	Side 1 av 1

Egenkontrollskjema

<Se veilederen Internkontroll og informasjonssikkerhet for veiledning til utfylling og for eksempler.>

Egenkontrolltiltak	Eier av aktivitet	Frekvens	Resultat	Kommentarer/ tiltak

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-03_Egenkontrollskjema.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Rapport fra avvikshåndtering og egenkontroll - forslag til tiltak	Side 1 av 2

Rapport fra avvikshåndtering og egenkontroll - forslag til tiltak

NB! Innholdet i denne malen må tilpasses til egen virksomhet. Det kan medføre utfylling av ytterligere informasjon og/eller sletting av ikke relevant informasjon.

Det gjøres oppmerksom på at eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven.

1 Oppsummering siste år

<Et sammendrag av viktigste avvik og funn fra egenkontroll i året som er gått siden siste Ledelsens gjennomgang. Oppsummering av forslag til tiltak for å forbedre internkontroll, forventende resultater av tiltak, tidsplan og kostnader for gjennomføring.>

2 Viktigste avvik

Liste over viktigste avvik siste år som kan inneholde:

- Tidspunkt / tidsrom avviket skjedde
- Beskrivelse
- Årsak
- Avdeling/systemområde
- Alvorlighet
- Status
- Gjennomførte, eventuelt midlertidige, tiltak.
- Eventuelle foreslåtte tiltak, vise til kapittel 4.

3 Viktigste funn ved egenkontroll

Liste over viktigste funn siste år som kan inneholde:

- Tidspunkt / tidsrom
- Beskrivelse
- Årsak
- Avdeling/systemområde
- Alvorlighet
- Status
- Gjennomførte, eventuelt midlertidige, tiltak.
- Eventuelle foreslåtte tiltak, vise til kapittel 4.

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-04_Rapport_fra_avvikshandtering_og_egenkontroll-forslag_til_tiltak.odt	

Internkontroll <Virksomhet>	Dato: xx.xx.200x Versjon: x.xx
Rapport fra avvikshåndtering og egenkontroll - forslag til tiltak	Side 2 av 2

4 Forslag til tiltak

Prioritert liste over forslag til tiltak til forbedring av internkontroll som kan inneholde:

- Forslag til tiltak
- Forventende resultat
- Tidsplan
- Kostnader for gjennomføring

Vedlegg 1 Fullstendig avviksliste

Vedlegg 2: Fullstendig liste over funn ved egenkontroll

Dokumentref:	Dokumentansvarlig: NN
Filnavn: 3-04_Rapport_fra_avvikshandtering_og_egenkontroll-forslag_til_tiltak.odt	