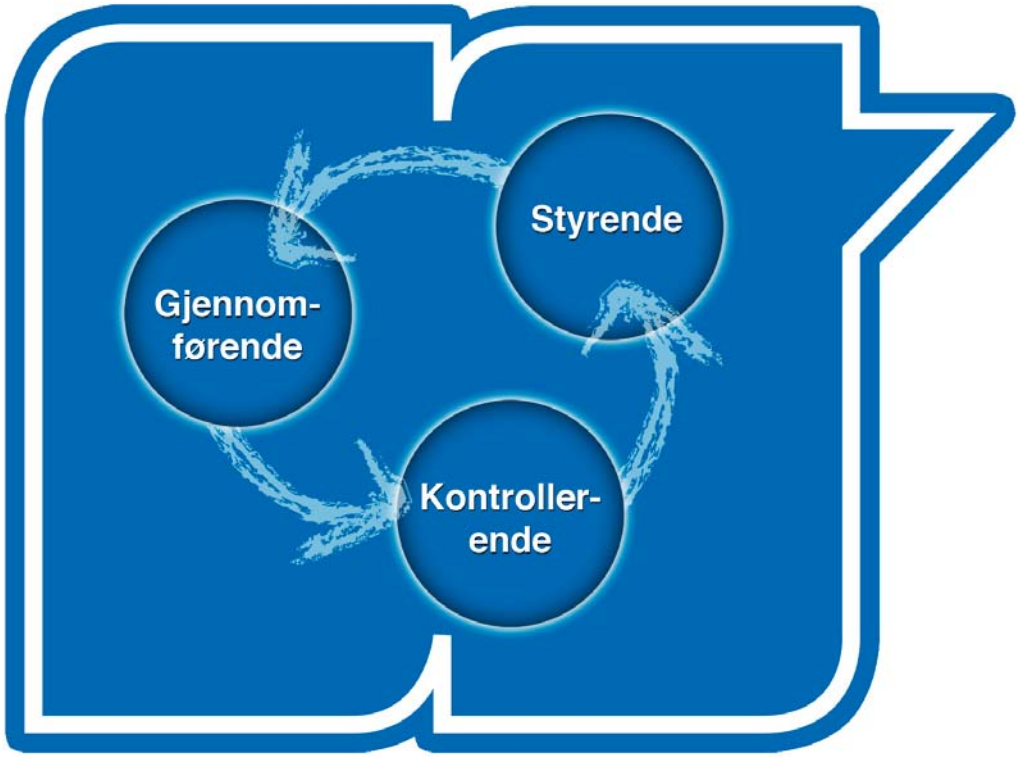
Datatilsynet

Internkontroll i mindre virksomheter - eksempel

Veileder 07/02b (del 2 av 2)

Publisert 15.02.2007



Datatilsynet

Gateadresse: Tollbugata 3, Oslo

Postadresse: postboks 8177, dep

0034 Oslo

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50

Dette dokumentet er et eksempel på internkontroll for mindre virksomheter. Dokumentet hører sammen med dokumentet "Internkontroll i mindre virksomheter - introduksjon".

Eksempelet på internkontroll må gjennomgås og tilpasses til virksomheten din. Sett inn riktig verdi for <virksomhet>, <navn> etc. og tilpass bruken av blant annet roller og avdelinger som sikkerhetsansvarlig, personalsjef, daglig leder og IT-avdeling. Gi dokumentet din egen tittel.

Det forutsettes at virksomheten kun behandler typer personopplysninger om egne ansatte og kunder (som beskrevet i kapittel 1). Dersom virksomheten behandler personopplysninger utover dette, må den generelle veilederen "Internkontroll og informasjonssikkerhet" med tilhørende maler benyttes.

Vær oppmerksom på at også andre regelverk enn personopplysningsloven og personopplysningsforskriften kan stille krav til hvordan personopplysninger skal behandles.

Denne teksten kan slettes før dokumentet tas i bruk i virksomheten.

Innholdsfortegnelse

1 Styrende dokumentasjon 5

2 Gjennomførende dokumentasjon 8

2.1 Rutiner for håndtering av personopplysningene 8

2.2 Rutiner relatert til registrert person 10

2.3 Informasjonssikkerhet 14

3 Kontrollerende dokumentasjon 15

Vedlegg 1 - Sikkerhetsinstruks bruker *17*

Vedlegg 2 - Taushetserklæring *22*

Lov nr 10 av 22. mai 1902: Almindelig borgerlig Straffelov (Straffeloven). 23

LOV 1972-06-16 nr 47: Lov om kontroll med markedsføring og avtalevilkår (markedsføringsloven). 23

Vedlegg 3 - Konfigurasjonsbeskrivelse *25*

Vedlegg 4 - Resultat av risikovurdering *27*

Vedlegg 5 - Driftsrutiner og sikkerhetstiltak *29*

Vedlegg 6 - Avviksrapport *30*

Vedlegg 7 - Utdrag fra forskriftstekst *31*

§ 7-7 Kunde-, abonnent- og leverandøropplysninger 31

§ 7-11 Aktivitetslogg i edb-system eller datanett 31

§ 7-16 Personalregistre mv. 31

1 Styrende dokumentasjon

Personopplysningsloven stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak. Tiltakene skal oppfylle kravene i eller i medhold av personopplysningsloven, herunder sikre personopplysningenes kvalitet. Dette kan beskrives som:

- Rutiner for oppfyllelse av virksomhetens plikter og de registrertes rettigheter.
- Rutiner og tekniske tiltak for informasjonssikkerhet.

<Virksomhet> behandler personopplysninger for å administrere forholdet til sine ansatte (personaladministrasjon) og forholdet til sine kunder. Virksomhetens leder, <navn>, (den behandlingsansvarlige) er ansvarlig for at behandlingen av personopplysninger foregår etter personopplysningslovens bestemmelser.

Virksomheten behandler opplysninger om ansatte med hjemmel (behandlingsgrunnlag) i personopplysningslovens:

- § 8 ved at det er fastsatt i lov (arbeidslivslovgivningen, samt lønns- og ligningsopplysninger).
- § 8 ved at det innhentes samtykke fra den ansatte.
- § 8 a) for å oppfylle avtale med den registrerte.
- § 8 b) for å ivareta en rettslig forpliktelse.
- § 8 f) for å ivareta tungtveiende interesser.
- § 9 f) for å ivareta arbeidsrettslige plikter og rettigheter.

Virksomheten behandler opplysninger om kunder med hjemmel (behandlingsgrunnlag) i personopplysningslovens:

- § 8 a) for å oppfylle avtale med den registrerte (nødvendige administrasjon av kundeforholdet).
- § 8 ved at det innhentes samtykke (utover det som dekkes av forrige punkt).
- § 8 ved at det er fastsatt i lov (regnskapsopplysninger som inkluderer kundeopplysninger).

Opplysningene om ansatte håndteres i lønns- og personalsystemet. Opplysningene om kunder håndteres i kunde- og ordrebehandlingssystemet. Den daglige håndteringen av opplysningene utføres av personalsjef for opplysninger om ansatte og av salgssjef for kundeopplysninger.

<Virksomhet> skal kun behandle nødvendige opplysninger om ansatte og kunder. De som registreres hos oss skal alltid være klar over at det blir gjort, og om nødvendig skal vi be om samtykke for dette. Alle i virksomheten skal vite hvordan personopplysningene skal håndteres, og om nødvendig kan de søke hjelp hos sin nærmeste leder. Virksomheten skal alltid kunne svare på spørsmål, både fra publikum og de som er registrert, om behandlingene av personopplysninger.

Sikkerhetsmål:

Personopplysninger om kunder og ansatte skal

- ikke være tilgjengelige for personer som ikke har behov for opplysningene i arbeidet sitt.
- være tilgjengelige og oppdaterte i henhold til behov.

Personopplysninger om kunder må ikke komme på avveie av hensyn til kundene det gjelder, og av hensyn til egen virksomhet.

Personopplysningene om ansatte skal kun være tilgjengelige internt i virksomheten for medarbeidere med tjenstlig behov, eksempelvis avdelingsleder og personalansvarlig.

Opplysningene i virksomheten skal sikres med hensyn til konfidensialitet (uvedkommende får ikke tilgang på opplysningene), integritet (opplysningene endres ikke uautorisert eller utilsiktet), og tilgjengelighet (opplysningene er tilgjengelige når vi trenger dem).

Eksempler på hendelser vi ønsker å beskytte oss mot:

- Felles hendelser for brudd på konfidensialitet, integritet og tilgjengelighet.
    - innbrudd i virksomhetens lokaler eller nettverk.
    - uvedkommendes bruk av brukerkonti.
    - angrep av virus eller andre ondsinnede program.
- Brudd på konfidensialitet (personopplysninger kommer på avveie).
    - tap av bærbart utstyr.
    - tap av lagringsmedium.
    - utskrift liggende på skriver.
    - utilsiktet utlevering av ansattopplysninger via e-post.
- Brudd på integritet (personopplysninger blir endret).
    - ulike versjoner av dokumenter.
    - feilregistrering.
- Brudd på tilgjengelighet (personopplysninger er utilgjengelige).
    - Nettverk eller system ute av drift.
    - Brann, vannskade og strømsvikt.
    - Hærverk.
    - Tjenestenekteangrep (Denial of Service).

Sikkerhetsstrategier:

- Det skal utpekes en sikkerhetsansvarlig i virksomheten.
- Uvedkommende skal ikke kunne få fysisk tilgang til personopplysningene, eller utstyr disse er lagret på.
- Ved behov for prioritering, har beskyttelse av personalopplysninger høyere prioritet enn kundeopplysninger.
- Tilgangskontroll skal sikre at tilgang til opplysninger om ansatte og kunder skal begrenses til de som har behov for det.
- Virksomhetens nettverk skal beskyttes mot inntrengning fra eksterne nettverk med brannmur som kun slipper gjennom nødvendig datatrafikk.
- Virksomhetens nettverk skal beskyttes mot uvedkommendes bruk, eksempelvis ved sikring av trådløst nettverk.
- *<virksomhetens beskrivelse av hvordan den forholder seg til IT-teknisk kompetanse - intern eller ekstern>*

Ekstra tiltak, utover tiltak med utgangspunkt i sikkerhetsstrategiene ovenfor, skal iverksettes for spesielt beskyttelsesverdige opplysninger som:

- *<sykmeldinger>*

- <*opplysninger rundt tilrettelegging av arbeidsplassen*>
- <*vurderinger av den ansatte*>
- <*merknader og advarsler*>

Organisering:

Personalsjef, <navn>, har rollen som sikkerhetsansvarlig. Sikkerhetsansvarlig skal vedlikeholde en oversikt over behandlinger av personopplysninger med formål og behandlingsgrunnlag, og skal sørge for at virksomheten har de nødvendige rutiner for å gjøre behandlingen forsvarlig. Sikkerhetsansvarlig skal årlig forberede, kalle inn til og dokumentere resultatene fra ledelsens gjennomgang av internkontroll og informasjonssikkerhet.

IT-driftsansvarlig, <navn>, er ansvarlig for for IT-infrastruktur og informasjonssystemene. IT-driftsansvarlig skal sørge for at IT-infrastruktur og informasjonssystemene ivaretar krav til sikkerhet basert på vedtatte rutiner og tekniske sikkerhetstiltak. Dette omfatter tiltak som:

- Sikre IKT-utstyr mot tyveri, hærverk, brann og strømutfall.
- Holde oversikt over virksomhetens IT-utstyr.
- Sikre at IT-utstyr er klassifisert i henhold til type opplysninger det behandler.
- Sørge for sikkerhetskopiering og sikker lagring av kopier.

Andre parter:

Parter som behandler personopplysninger på vegne av <virksomhet>, er virksomhetens databehandlere. Den behandlingsansvarlige skal inngå avtale med databehandlere. Avtalen skal regulere hvordan databehandleren skal håndtere og sikre personopplysningene.

<virksomhet> har <databehandler> som databehandler for sitt regnskapssystem. Avtalen er signert den xxx og er arkivert med referansenummer yyy.

<virksomhet> har <driftspart> som driftskonsulent for informasjonssystemet. Avtalen er signert den xxx og er arkivert med referansenummer yyy.

Parter som har tilgang til, eller en rolle i forhold til, <virksomhets> informasjonssystem, skal signere taushetserklæring. Den behandlingsansvarlige eller sikkerhetsansvarlig skal avtale forholdet med slike parter.

2 Gjennomførende dokumentasjon

2.1 Rutiner for håndtering av personopplysningene

Ny behandling, opphør av behandling og overholdelse av melde-/konsesjonsplikt

Rutinen er kun relevant når virksomheten endrer behandlingene den utøver. Se styrende del, 2. avsnitt.

Ved oppstart av en ny behandling av personopplysninger, skal sikkerhetsansvarlig bekrefte gyldig behandlingsgrunnlag. Melding, alternativt konsesjonssøknad, skal sendes Datatilsynet dersom behandlingen ikke er unntatt fra dette. Sikkerhetsansvarlig skal sørge for fornyelse av melding hvert tredje år. Oppstart av nye behandlinger vil medføre behov for endringer i internkontrollen.

Melde- og konsesjonsplikt

Virksomheten har følgende unntak fra melde– og konsesjonsplikten:

- Kundeopplysninger er unntatt meldeplikt etter personopplysningslovens § 31 jf. personopplysningsforkriftens § 7-7.
- Personalopplysninger er unntatt melde- og konsesjonsplikt etter personopplysningslovens § 31 og § 33 jf. personopplysningsforkriftens § 7-16.
- Opplysninger i datalogger er unntatt meldeplikt etter personopplysningslovens § 31 jf. personopplysningsforkriftens § 7-11.

Bestemmelsene om unntak beskriver håndteringen av opplysningene, og er gjengitt i vedlegg 7, Utdrag fra forskriftstekst.

Virksomheten har ingen meldepliktige behandlinger.

Virksomheten har ingen konsesjonspliktige behandlinger.

Innsyn i behandling av personopplysninger

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger som foretas i <Virksomhet> (ref. §18 i personopplysningsforskriften).

"Enhver kan kreve å få følgende informasjon om en bestemt type behandling:

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,

b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,

c) formålet med behandlingen,

d) beskrivelser av hvilke typer personopplysninger som behandles,

e) hvor opplysningene er hentet fra, og

f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om

a) hvilke opplysninger om den registrerte som behandles, og

b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i første ledd bokstav a - f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.

…"

Henvendelser om innsyn skal formidles til sikkerhetsansvarlig (personalsjef) som er ansvarlig for at henvendelser besvares fortløpende, og senest innen 4 uker ved ferieavvikling.

Sletting av personopplysninger

Personopplysninger skal slettes når det ikke lenger er saklig behov for å oppbevare dem i virksomheten. Sikkerhetsansvarlig er ansvarlig for dette hvis det er endringer ved virksomheten som tilsier at opplysningene skal slettes.

Rutine for sletting:

<Det er viktig at virksomheten konkret vurderer frister for sletting, også i forhold til krav i andre lover om oppbevaring. Rutinen er kun et eksempel.>

1) Salgssjef er ansvarlig for personopplysninger om kunder. Salgssjef skal:

- sørge for at personopplysninger relatert til kundeforholdet slettes etter 3 års inaktivitet i kundeforholdet. Dette gjelder med mindre skriftlig samtykke til fortsatt lagring er innhentet fra kunden,
- påse at det ikke lagres flere personopplysninger om kunder enn nødvendig for formålet,
- holde en oversikt over når det sist var aktivitet i de ulike kundeforholdene og
- gi IT-driftsansvarlig beskjed om hvilke opplysninger som skal slettes når.

Rutinen gjelder ikke opplysninger i virksomhetens regnskap. Disse gjennomgås når oppbevaringsplikten utløper.

2) Personalsjef er ansvarlig for personopplysninger om ansatte. Personalsjef skal :

- fjerne unødvendige opplysninger etter gjennomføring av personalsamtale,
- fjerne unødvendige opplysninger ved avslutning av arbeidsforholdet,
- gjennomføre ny vurdering av behov for fortsatt lagring et år etter avlutning av arbeidsforholdet,
- påse at det ikke lagres personopplysninger om ansatte som ikke er relevante for administrasjon av arbeidsforholdet og
- gi IT-driftsansvarlig beskjed om hvilke opplysninger som skal slettes når.

Rutinen gjelder ikke opplysninger i virksomhetens regnskap. Disse gjennomgås når oppbevaringsplikten utløper.

Rutine for utlevering av personopplysninger til andre

Utlevering betyr at personopplysninger overlates til annen behandlingsansvarlig. Dette er en ny behandling, og det kreves et eget behandlingsgrunnlag. Dersom ikke annet behandlingsgrunnlag finnes, må det innhentes samtykke fra den registrerte.

Opplysninger om egne ansatte kan utleveres til offentlige myndigheter i overensstemmelse med lovpålagte krav. Ved tvil om hjemmel for dette, bes det om at myndighetsorganet beskriver hjemmelen for å kreve opplysningene.

Utlevering av personopplysninger til 3. part forøvrig skal godkjennes av behandlingsansvarlig. Selve utleveringsoppgaven gjennomføres av IT-drift.

Sikring av kvalitet av personopplysninger

Den behandlingsansvarlige har overordnet ansvar for at opplysningene er så korrekte og oppdaterte som mulig i forhold til formålet med behandlingen. Personalsjef er ansvarlig for at personalopplysninger bekreftes korrekte av den ansatte årlig i forbindelse med personalsamtale. Salgssjef er ansvarlig for at kundeopplysninger er korrekte. Hver selger er ansvarlig for at kontaktinformasjon til kundene som de er ansvarlige for, til enhver tid er oppdaterte.

2.2 Rutiner relatert til registrert person

Innhenting og kontroll av samtykke

Kunder kan abonnere på et nyhetsbrev som sendes med e-post fra virksomheten.

Kunden skal på forhånd gi samtykke til at virksomheten kan sende nyhetsbrev til ham/henne. Slikt samtykke kan gis pr. telefon eller e-post. Kunden kan trekke sitt samtykke tilbake når som helst ved hjelp av beskjed pr. telefon eller e-post. Salgssjef er ansvarlig for at distribusjonsliste for nyhetsbrev er oppdatert.

Oppfyllelse av informasjonsplikt

Stillingssøkere og andre aktuelle kandidater for ansettelse informeres under intervju med personalsjef om virksomhetens politikk og hvilke opplysninger som kan lagres om den ansatte under arbeidsforholdet, om innsynsrett og rett til å få rettet og supplert data. Kunder informeres om lagring av personopplysninger i kjøpsavtale og har mulighet til å reservere seg mot slik lagring etter at oppgjør er gjennomført. Kjøpsavtale beskriver også kundens krav på innsyn i opplysninger som er laget om ham/henne og på retting og supplering av opplysninger.

Innsyn

Rett til innsyn i personopplysninger er beskrevet i personopplysningsloven § 18:

"Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,

b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,

c) formålet med behandlingen,

d) beskrivelser av hvilke typer personopplysninger som behandles,

e) hvor opplysningene er hentet fra, og

f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om

a) hvilke opplysninger om den registrerte som behandles, og

b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten.

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i første ledd bokstav a - f i den grad dette er nødvendig for at den registrerte skal kunne vareta egne interesser.

Retten til informasjon etter annet og tredje ledd gjelder ikke dersom personopplysningene behandles utelukkende for historiske, statistiske eller vitenskapelige formål og behandlingen ikke får noen direkte betydning for den registrerte."

Plikt til å informere når det samles inn opplysninger fra den registrerte. Dette er beskrevet i personopplysningsloven § 19:

"Når det samles inn personopplysninger fra den registrerte selv, skal den behandlingsansvarlige av eget tiltak først informere den registrerte om

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,

b) formålet med behandlingen,

c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,

d) det er frivillig å gi fra seg opplysningene, og

e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28.

Varsling er ikke påkrevd dersom det er på det rene at den registrerte allerede kjenner til informasjonen i første ledd."

Plikt til å informere når det samles inn opplysninger fra andre enn den registrerte, er beskrevet i personopplysningsloven § 20:

"En behandlingsansvarlig som samler inn personopplysninger fra andre enn den registrerte selv, skal av eget tiltak informere den registrerte om hvilke opplysninger som samles inn og gi informasjon som nevnt i § 19 første ledd så snart opplysningene er innhentet. Dersom formålet med innsamling av opplysningene er å gi dem videre til andre, kan den behandlingsansvarlige vente med å varsle den registrerte til utleveringen skjer.

Den registrerte har ikke krav på varsel etter første ledd dersom

a) innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov,

b) varsling er umulig eller uforholdsmessig vanskelig, eller

c) det er på det rene at den registrerte allerede kjenner til informasjonen varselet skal inneholde.

Når varsling unnlates med hjemmel i bokstav b, skal informasjonen likevel gis senest når det gjøres en henvendelse til den registrerte på grunnlag av opplysningene."

Virksomheten skal ha rutine for behandling av forespørsel om innsyn fra registrert.

Eksempel - Generell rutine for behandling av forespørsel om innsyn:

Ansatte gis innsyn i, og på forespørsel utskrift av, alle opplysninger som er lagret om seg selv ved henvendelse til personalsjef. Kunder får på henvendelse til selger eller salgssjef oversendt utskrift av alle opplysninger som er lagret om seg selv. Slikt innsyn og/eller utskrift skal gis uten unødig opphold og senest innen 30 dager fra forespørsel er mottatt. Forespørsel kan være muntlig, men personalsjef og salgssjef kan be om skriftlig forespørsel dersom de ønsker det, for å kunne dokumentere svartid.

Retting og supplering

Personopplysninger om ansatte og kunder skal være tilstrekkelige og relevante for formålet med behandlingen. Kravet til relevans trekker opp en ytre grense for hvilke personopplysninger som kan tas med i behandlingen, og kan ikke fravikes gjennom samtykke fra den registrerte. Kravet til tilstrekkelighet innebærer at man må ha nok opplysninger for å kunne ivareta formålet med behandlingen.

Det kan også være behov for retting i henhold til lovens §27. Bestemmelsen slår blant annet fast: *"Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på begjæring av den registrerte rette de mangelfulle opplysningene."*

Eksempel - Rutine for behandling av forespørsel om retting og supplering:

- Mottak av forespørsel om retting eller supplering for ansatt eller kunde.
- Formidling av forespørsel til henholdsvis personalsjef eller salgssjef.

- Mottakeren av forespørselen skal verifisere korrekthet av forespurte endringer av opplysninger.

- Hvis endringene er verifisert, utstede arbeidsordre for oppdatering av system(er).

- Bekrefte skriftlig til den som forespør endringer.

Innsyn i private e-poster og private filområder

Det vises til Vedlegg 1, Sikkerhetsinstruks, den ansattes plikter i forbindelse med bruk av <Virksomhet>s e-postsystem.

Det er ikke adgang for <Virksomhet> å gjøre innsyn i ansattes personlige e-postkasse og filer på personlig filområde med visse unntak. I følgende situasjoner kan innsyn likevel være aktuelt:

A) Ved fravær dersom

- det er god grunn til å tro at det er kommet virksomhetsrelaterte meldinger i e-postkassen som arbeidsgiver trenger av driftshensyn.
- den ansatte samtykker eller virksomheten har skriftlige retningslinjer som de ansatte er kjent med og som klart og tydelig sier hvilke fraværsituasjoner som kan innebære innsyn.

B) Ved opphør av arbeidsforholdet dersom

- det er behov for å sortere ut virksomhetsrelatert e-post før innholdet slettes og e-postkassen avsluttes i tråd med skriftlige retningslinjer.
- dette er avtalt med den enkelte.

C) Ved begrunnet mistanke om at

- e-post har et innhold som er straffbart.
- e-post som inngår som et ledd i gjennomføringen av en straffbar handling.
- det sendes e-post som medfører et grovt brudd på plikter som følger av arbeidsforhold, reglement eller annet skriftlig regelverk knyttet til ansettelsesforholdet.

Hvis et av vilkårene i punkt C er oppfylt, kan det også gjøres innsyn i privat e-post på den personlige e-postkassen, ellers ikke.

Utfyllende informasjon rundt dette finnes på www.datatilsynet.no. Regelverket på dette området er under endring.

Rutine for innsyn i e-post:

A) Arbeidstakeren skal så sant mulig varsles før innsyn.

B) Disse to punktene skal i tillegg gjennomføres:

- Arbeidstakeren må få tilbud om å være tilstede ved åpningen selv, eller selv få utpeke en representant som kan være tilstede.

- Innsynet skal dokumenteres (hvorfor innsynet ble foretatt, hvem som fattet beslutningen, hvem som var tilstede, metode for innsyn og resultatet).

Rutinene gjelder også for innsyn i personlige filer og hjemmeområde.

2.3 Informasjonssikkerhet

Veiledning for å utarbeide denne dokumentasjonen, finner du i del 1, "introduksjon", under kapittel 3 "Informasjonssikkerhet". Dersom drift av informasjonssystemet er satt bort til en leverandør, skal leverandøren bidra med denne dokumentasjonen.

Tilgang til sikkerhetsdokumentasjon skal begrenses til de som har behov for det. Sikkerhetsdokumentasjon er derfor ført i vedlegg som ikke gis ut til enhver ansatt.

Brukere ved <virksomhet> benytter informasjonssystemet slik det fremgår av vedlegg 1, Sikkerhetsinstruks bruker.

Sikkerhetsansvarlig ved <virksomhet> har dokumentert informasjonssystemets konfigurasjon i vedlegg 3. Tilgang til vedlegget begrenses.

Sikkerhetsansvarlig ved <virksomhet> har gjennomført risikovurdering av informasjonssystemet og dokumentert denne i vedlegg 4. Tilgang til vedlegget begrenses.

Rutiner for drift av informasjonssystemet og beskrivelse av sikkerhetstiltak er dokumentert i vedlegg 5, Driftsrutiner og sikkerhetstiltak. Tilgang til vedlegget begrenses.

3 Kontrollerende dokumentasjon

Håndtering av uønskede hendelser

Ansatte som oppdager uønskede hendelser skal snarest rapportere om dette til nærmeste overordnede eller sikkerhetsansvarlig. Ledere som oppdager uønskede hendelser eller blir informert av underordnede, skal snarest rapportere dette til sikkerhetsansvarlig.

Håndtering av uønskede hendelser skal gjennomgås i møte mellom personalsjef, salgssjef, IT-driftssjef og sikkerhetsansvarlig månedlig. I møtet skal det besluttes eventuelle rutinemessige eller tekniske tiltak for å forhindre at uønskede hendelser gjentar seg.

Egenkontroll

To ganger pr. år, i mars og september måned, skal rutiner og tekniske tiltak beskrevet i dette dokument gjennomgås for å bekrefte at de fungerer etter hensikten. Sikkerhetssjef er ansvarlig for å gjennomføre egenkontrollen og dokumentere resultatet.

Avvikshåndtering

Ansatte som oppdager avvik fra rutiner, skal rapportere om dette i avviksskjema som sendes til sikkerhetsansvarlig. Se vedlegg 1, Avviksskjema. Avvik skal behandles i møte mellom personalsjef, salgssjef, IT-driftssjef og sikkerhetsansvarlig månedlig. Møtet skal beslutte eventuelle rutinemessige eller tekniske tiltak for å forhindre at avvik gjentar seg.

Ledelsens gjennomgang

Ledelsen skal årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Ledelsen skal kontrollere at disse er i samsvar med virksomhetens behov og eventuelt oppdatere mål, strategi og organisering.

Ved ledelsens gjennomgang deltar virksomhetsleder, personalsjef/sikkerhetssjef , salgssjef og IT-driftsleder.

Praktisk organisering av gjennomgangen, utarbeidelse av rapport samt iverksetting av eventuelle tiltak, er sikkerhetsansvarligs ansvar.

I ledelsens gjennomgang av informasjonssystemet skal bl.a. følgende vurderes:

- Resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet.
- Endringer med betydning for drift av informasjonssystemet eller for informasjonssikkerheten, herunder:
    - Endringer i offentlige sikkerhetskrav.
    - Endringer i de personopplysninger virksomheten skal behandle.

  - Endringer trusselbildet som bl.a. beskrevet i rapport fra utførte risikovurderinger.

- Om informasjonssystemet bør endres, eksempelvis som følge av ønske om ny funksjonalitet.

- Overordnet behandling av alvorlige hendelser og avvik.

Vedlegg 1 - Sikkerhetsinstruks bruker

Innledning

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

Bruk av <Virksomhet>s IKT-systemer

- <Virksomhet>s informasjonssystemer er beregnet for jobbrelaterte formål. Privat bruk, f.eks. e-post og private filer tillates i begrenset omfang, så lenge det ikke påvirker jobbrelaterte 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.

Opplæring

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

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 er blitt kjent av andre, skal passordet byttes og hendelsen rapporteres til sikkerhetsansvarlig snarest mulig som et avvik.
- Passordbeskyttet skjermsparer skal benyttes og/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, samt ved arbeidstidens slutt.

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/applikasjoner, eksempelvis radiolytting og TV/video streaming, skal begrenses for å ikke påvirke negativt jobbrelatert 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.
- Det er ikke tillatt å forsøke å forbigå sikkerhetsmekanismer og denne sikkerhetsinstruks, for eksempel ved å skjule disse gjennom andre tjenester.

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 web-baserte e-postsystemer <*virksomhetens eksempler*>.
- Dersom e-post må benyttes for overføring av beskyttelsesverdig informasjon, skal informasjonen sendes som kryptert vedlegg til e-post med godkjent krypteringsprogram.
- Brukere er selv ansvarlig for å vurdere hva som er arkivverdig.

Bærbar PC, PDA og annet portabelt utstyr

- Kontor PC, bærbar PC (Jobb-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 som benyttes som klient i <virksomhet>-nett, kan benyttes i forbindelse med jobb på reiser og hjemme. Slike skal ikke benyttes til annet enn jobbrelaterte oppgaver.
- La aldri bærbar PC, PDA eller annet bærbart utstyr ligge synlig uten tilsyn.

Sikkerhetskopiering

- For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på eller 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 sikkerhetskopiert informasjon, kontakt IT-drift.

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.

Modem-/bredbåndstilknytninger

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

Hjemme-PC

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

Reparasjon, service og vedlikehold

- Alle feil eller mistanker om feil i IT-systemet (både maskin- og programvare) skal rapporteres til IT-drift snarest mulig.
- Det er kun IT-drift som kan iverksette arbeid som utføres av eksternt personell på IKT-systemer og utstyr.

Håndtering av informasjon og medier

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

Fysisk adgang

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.

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.

Kontakt med media

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

Nødhjelp

Brann: Nødnummer 110

Håndslukkingsapparat CO2 og husbrannslange finnes i <>.

Rømningsveier er merket med nødlys.

Brannalarm meldes automatisk til <> brannvesen.

Ved feil ring <> brannvesen telefon <>.

Møt opp på utsiden bygningen når brannalarmen går.

Politi: Nødnummer 112

Ambulanse: Nødnummer 113

Vann: Meld fra til administrasjonen.

Stengekran for vann er på rom <>.

Personellsikkerhet

Taushetserklæring

Ansatte, konsulenter og vikarer skal underskrive taushetserklæring.

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.

Rapportering og avvik

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.

Avvikshåndtering

Avvik fra 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.

Sikkerhetsinstruksen er lest og akseptert:

Sted og dato: _____

Navn (blokkbokstaver) _____ Signatur: _____

Vedlegg 2 - Taushetserklæring

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

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 Paatale 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 rettsstridig 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 rettsstridig 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.

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.

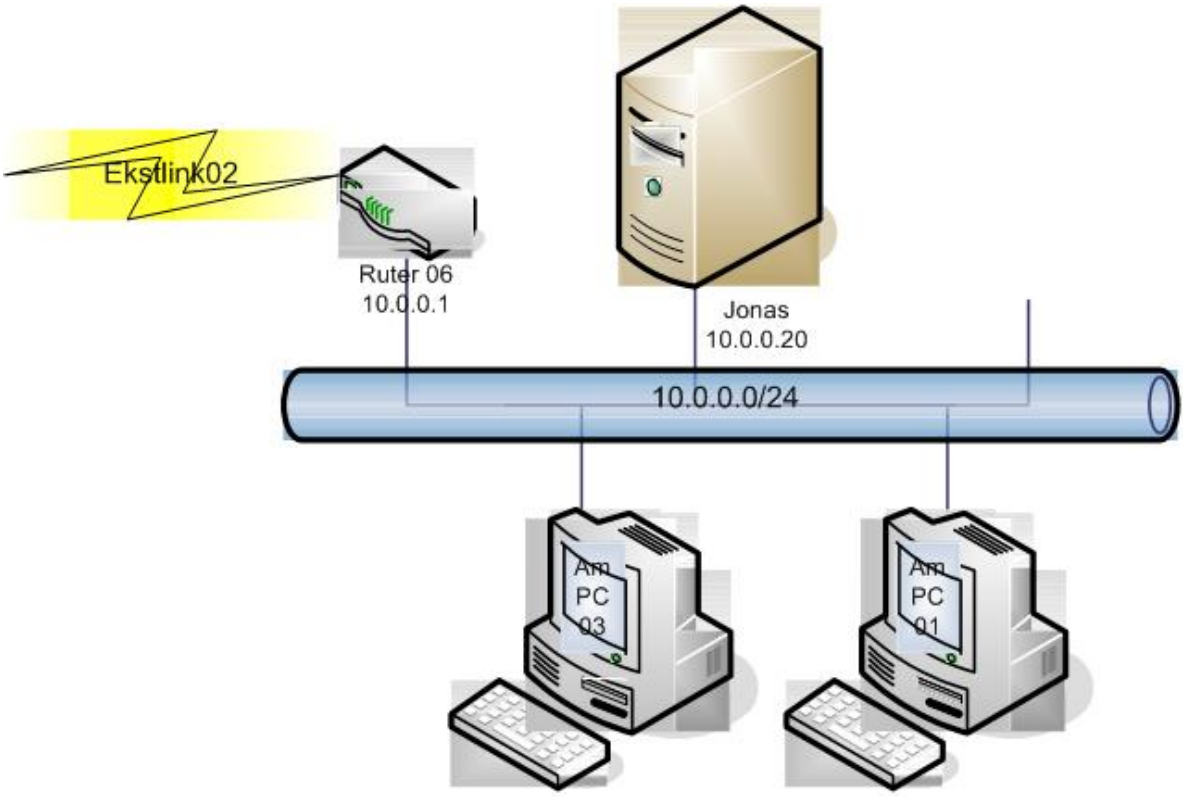
Tilføyd ved lov 8 april 2005 nr. 16.

Vedlegg 3 - Konfigurasjonsbeskrivelse

3.1 Nettverkstegning

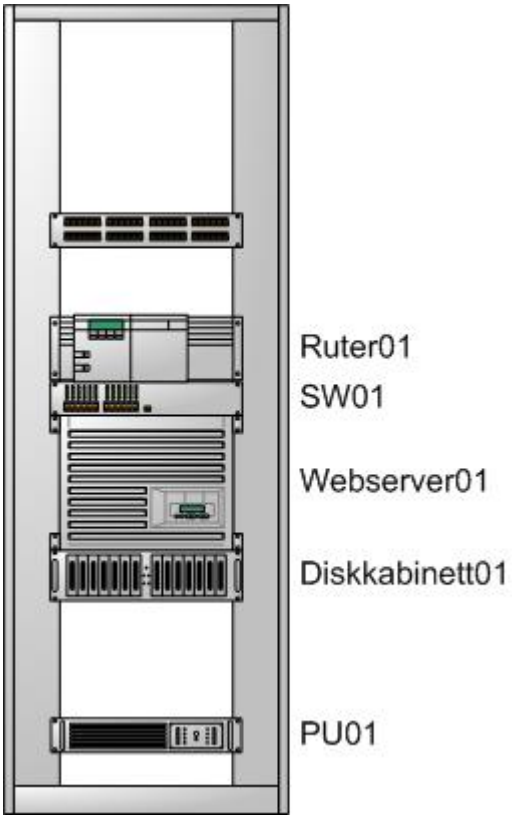
Nettverkstegning med beskrivelse av

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



Figur 1 Nettverkstegning

3.2 Fysisk montering (skap)



3-1Tegning av Skap

3.3 Beskrivelse av utstyr og programvare

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

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

3.4 Oppsett av utstyr

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

Vedlegg 4 - Resultat av risikovurdering

4.1 Analyse av hendelser

Hendelse	**Kategori K I T**	**Konsekvens**	**Sannsynlighet**	**Vurdering**
1. Utenforstående får tilgang til lokalene gjennom innbrudd, tyveri av PC'er og servere.	K, T	Kan medføre uopprettelig økonomisk tap ved tilgang til kundeopplysninger. - Tap av omsetning og kunder under nedetid.	Det er lav sannsynlighet for innbrudd grunnet alarm tilknyttet vaktselskap.	**Akseptabel**
2. Ansatte får tilgang til andre ansattes personalmapper ved å låse seg inn på kontoret til personalansvarlig.	K, I	Kan føre til tap av anseelse eller integritet for den enkelte ansatte.	Kan med letthet gjennomføres ved bruk av standard kontornøkler.	**Ikke akseptabel**
3. Utilgjengelighet av personalsystem i 24 timer.	T	Kan medføre økonomisk tap for de ansatte ved forsinket utbetaling - reparerbart.	Moderat sannsynlighet. Frafall av Internett eller nedetid i informasjonssystem.	**Akseptabel**
4. Brann i virksomhetens lokaler.	T	Kan medføre økonomisk tap ved tap av omsetning og kunder.	Sannsynlig med tap og betydelige skader på grunn av manglende sikkerhetskopier utenfor huset, brannvarsling med linje til brannvesenet og brannsikring i datarom.	**Ikke akseptabel**
5. Vannskade	T	Kan medføre økonomisk tap ved tap av omsetning og kunder.	Lav sannsynlighet for vannskader grunnet ingen vannrør umiddelbart over datarom, metalldeksler over servere og fordi bygningen ikke er flomutsatt.	**Akseptabel**

4.2 Tiltak for å redusere risiko

Hendelser som er identifisert med en ikke-akseptabel risiko:

Hendelse nr.	**Tiltak**	**Ansvar**	**Frist**
2	Skaffe låsbart arkivskap til personalansvarlig og revidere rutine for håndtering av personalsaker.	Sikkerhets-ansvarlig	1. juni 2007
4	4.1 Ta daglig sikkerhetskopi med lagring hver uke utenfor bygning..	IT-driftsansvarlig	1. april 2007
4	4.2 Brannvarslingssystem med linje direkte til brannvesen.	Sikkerhets-ansvarlig	1. juli 2007
4	4.3 Brannslukningsanlegg i datarom.	Sikkerhets-ansvarlig	1. juli 2007

Vedlegg 5 - Driftsrutiner og sikkerhetstiltak

Sikkerhetskopiering

Personopplysninger skal sikkerhetskopieres for å sikre integritet og tilgjengelighet. IT-driftssjef er ansvarlig for at denne rutine følges.

Brukere er ansvarlige for at personopplysninger de endrer eller på annen måte har ansvar for, skrives eller kopiere til diskområde hvor de blir sikkerhetskopiert.

Rutine for sikkerhetskopiering:

IT-driftssjef er ansvarlig for at

- det tas daglig sikkerhetskopi av minimum endringer av data.
- det tas ukentlig sikkerhetskopi av alle data.
- det lagres sikkerhetskopi av alle data utenfor bygning med database hver annen uke.
- all sikkerhetskopiering logges.
- logger for sikkerhetskopiering sjekkes for korrekthet hver morgen - mandag til fredag.

Test av tilbakelegging av data fra sikkerhetskopi til filer og database skal gjennomføres minimum hvert kvartal under oppsyn av sikkerhetsansvarlig.

Vedlegg 6 - Avviksrapport

Eksempel på avviksrapport.

Avviksrapport	Virksomhet: XX	Sendes til: Sikkerhetsansvarlig	Saksident: xxxx
Formål: Rapporten 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: Xxxxxxxxx	Utstyr/ident: xxxxxxxx	Dato/ kl: xxxxxxxxx
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:			

Vedlegg 7 - Utdrag fra forskriftstekst

§ 7-7 Kunde-, abonnent- og leverandøropplysninger

Behandling av personopplysninger om kunder, abonnenter og leverandører er unntatt fra meldeplikten etter personopplysningsloven § 31 første ledd. Det samme gjelder opplysninger om tredjeperson som er nødvendig for gjennomføring av kontraktsforpliktelser.

Unntak fra meldeplikt gjelder bare dersom personopplysningene behandles som ledd i administrasjon og gjennomføring av kontraktsforpliktelser.

§ 7-11 Aktivitetslogg i edb-system eller datanett

Behandling av personopplysninger som følge av registrering av aktiviteter (hendelser) i et edb-system, samt behandling av personopplysninger om disposisjoner til ressurser i systemet, er unntatt fra meldeplikten etter personopplysningsloven § 31 første ledd.

Unntak fra meldeplikt gjelder bare dersom behandlingen har som formål

a) å administrere systemet, eller

b) å avdekke/oppklare brudd på sikkerheten i edb-systemet.

Personopplysninger som fremkommer som følge av behandlinger etter annet ledd, kan ikke senere behandles for å overvåke eller kontrollere den enkelte.

§ 7-16 Personalregistre mv.

Arbeidsgivers behandling av ikke-sensitive personopplysninger om nåværende eller tidligere ansatte, personale, representanter, innleid arbeidskraft samt søkere til en stilling er unntatt meldeplikt etter personopplysningsloven § 31 første ledd.

Dersom det behandles sensitive personopplysninger, er behandlingen unntatt fra konsesjonsplikten etter personopplysningsloven § 33 første ledd, men underlagt meldeplikten etter § 31 første ledd. Unntak fra konsesjonsplikt gjelder under forutsetning av at:

a) den registrerte har samtykket i behandlingen eller behandlingen er fastsatt i lov,

b) opplysningene er knyttet til arbeidsforholdet, og

c) personopplysningene behandles som ledd i personaladministrasjonen.

Meldeplikt etter andre ledd gjelder likevel ikke behandling av

a) opplysninger om medlemskap i fagforeninger som nevnt i personopplysningsloven § 2 nr. 8 bokstav e,

b) nødvendige fraværsopplysninger og opplysninger som er registreringspliktige i henhold til lov 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven) § 5-1,

c) opplysninger som er nødvendige for å tilrettelegge arbeidssituasjonen på grunn av helseforhold.