Veiledning i informasjonssikkerhet

for kommuner og fylker

TV-202:2005

Forord

Veileder i informasjonssikkerhet for kommuner og fylkeskommuner ble første gang gitt ut i 1998, og er nå tilpasset dagens regelverk.

En kommunes behandlinger av personopplysninger er regulert i personopplysningsloven og helseregisterloven, hvor henholdsvis § 13 og § 16 stiller krav til sikring av personopplysningene. De to bestemmelsene er relativt likelydende, og personopplysningslovens begreper benyttes i denne veileder. Utfyllende bestemmelser for informasjonssikkerhet er gitt i personopplysningsforskriftens 2. kapittel.

Når denne veilederen ble skrevet første gang gjaldt personregisterloven. Personopplysningsloven som trådte i kraft 1. januar 2001 gir i større grad den behandlingsansvarlige frihet til å bestemme sikkerhetsnivå gjennom å velge akseptkriterier og utføre risikovurderinger. Den reviderte utgaven har tilpasset teksten til nytt lovverk, mens de opprinnelige prinsippene i veilederen er beholdt.

Oslo 26. januar 2005

Sammendrag

Dette dokument veileder kommuner og fylkeskommuner ved etablering av tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Veiledningen angir anbefalinger for å oppfylle personopplysningslovens §13 og herunder personopplysningsforskriftens kapittel 2.

I Del I defineres sentrale begreper, samtidig som formålet med dokumentet beskrives.

Del II beskriver ledelsens ansvar og gir eksempler på mål og strategi for informasjonssikkerheten. Det vises også hvordan man kan utarbeide oversikt over og klassifisere de personopplysninger som behandles. Med utgangspunkt i risikovurderinger vises det hvordan informasjonssikkerheten vedlikeholdes ved bruk av sikkerhetsrevisjon og ledelsens gjennomgang.

Del III angir organiseringen av informasjonssystemet. Organisering av ansvar og myndighetsforhold beskrives. Konfigurasjonskontroll og eksempler på rutinebeskrivelser viser hvordan arbeidet med informasjonssystemet bør utføres i henhold til dokumenterte rutiner.

Veiledning for bruk av partnere og leverandører er beskrevet i Del IV.

Del V angir nødvendige sikkerhetstiltak med hensyn på personellsikkerhet, fysisk sikkerhet, systemteknisk sikkerhet - herunder tilgangskontroll og sikker datakommunikasjon - og dokumentsikkerhet.

Utarbeidelse av dokumentasjon er beskrevet i Del VI.

I denne veiledningen er brukt en rekke konkrete eksempler for å utdype de anbefalinger som beskrives. Slike illustrerende eksempler er markert ved
innrykk og en egen skrifttype.

INNHOLD

FIGURER

Del I Innledning

1 Definisjoner

Personopplysningslovens § 2 gir følgende førende definisjoner:

1) Personopplysning	-	opplysninger og vurderinger som kan knyttes til enkeltperson
2) Behandling av personopplysninger	-	enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksområder
3) Personregister	-	registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen
4) Behandlingsansvarlig	-	den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes
5) Datatbehandler	-	den som behandler personopplysninger på vegne av den behandlingsansvarlige
6) Registrert	-	den som en personopplysning kan knyttes til
7) Samtykke	-	en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv
8) Sensitive personopplysninger	-	Opplysninger om: a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller relgiøs oppfatning b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling c) helseforhold d) seksuelle forhold e) medlemsskap i fagforeninger

Videre defineres følgende sentrale begreper i dette dokumentet:

Datakommunikasjon	–	elektronisk kommunikasjon av data i et informasjonssystem. Datakommunikasjon der overføringsmedium er utenfor virksomhetens kontroll betegnes *ekstern datakommunikasjon.*

Demilitarisert sone (DMZ)	–	en sone hvor brukere utenfor virksomheten kan gis tilgang, men som er skilt fra virksomhetens øvrige informasjonssystem ved hjelp av en sikkerhetsbarriere.
Eksternt nettverk	–	datanettverk som benyttes av flere virksomheter.
Internt nettverk	–	fellesbegrep for de ulike nettverk som finnes i en virksomhet til bruk for de ansatte.
Område	–	del av virksomheten adskilt fra virksomheten for øvrig ved hjelp av fysiske innretninger og med adgangskontroll.
Sone	–	de deler av informasjonssystemet som kan kommunisere ved hjelp av datakommunikasjon. Soner opprettes etter analyse av behovet for tilgang og datakommunikasjon mellom enkelte enheter i informasjonssystemet.
Teknisk sikkerhetsbarriere	–	utstyr og program benyttet for tilgangskontroll mellom virksomhetens informasjonssystem og eksterne nettverk, eller mellom forskjellige soner internt i virksomhetens informasjonssystem.
Virksomhet	–	Den behandlingsansvarliges virksomhet (eksempelvis kommune, fylkes kommune, bydel eller KS), eller annen virksomhet det samarbeides med.

2 Formål

Personopplysningslovens § 13 med utfyllende bestemmelser i personopplysningsforskriftens 2. kapittel gir forventninger om tilfredsstillende sikring av informasjonssystemet med grunnlag i en risikovurdering. Helseregisterlovens § 16 gir tilsvarende føringer for behandlinger av helseopplysninger i helseforvaltningen.

Veiledningen angir metoder for å etablere tilfredsstillende informasjonssikkerhet ved:

- elektronisk behandling av personopplysninger i virksomhetens informasjonssystem
- tilkobling av virksomhetens informasjonssystem til eksterne datanett
- ekstern datakommunikasjon - herunder ekstern datakommunikasjon av sensitive personopplysninger.

I veiledningen er ordet *kommune* benyttet som fellesbetegnelse for kommune og fylkeskommune. Veiledningen inneholder en rekke eksempler. Disse er angitt med egen skrifttype, og er ment som illustrasjoner for å utdype de anbefalinger som beskrives.

Del II Ledelsens ansvar

3 Ansvar

Behandlingsansvarlig, normalt representert ved den administrative ledelse, er ansvarlig for at sikkerhetsbestemmelsene i personopplysningslovens § 13 og personopplysningsforskriftens kapittel 2 følges.

Ansvaret omfatter også at det årlig avsettes tilstrekkelige ressurser, både personalmessige og økonomiske, slik at tilfredstillende informasjonssikkerhet opprettholdes.

Den behandlingsansvarlige må etablere klare ansvars og myndighetsforhold slik at det er klart hvem som har fått delegert hvilke oppgaver.

4 Sikkerhetsmål

Kommunen bør som del av øvrige målbeskrivelser angi formålet med elektronisk behandling av personopplysninger.

Kommunal virksomhet dekker et vidt spekter av tjenester og fagområder som innebærer behandling av ulike personopplysninger. Moderne informasjonsteknologi muliggjør forskjellige former for behandling - som innsamling, bearbeiding, lagring og utlevering - av både sensitive og ikke-sensitive personopplysninger. I denne veiledningen anbefales sikkerhetsløsninger ved:

- elektronisk behandling av personopplysninger i virksomhetens informasjonssystem; målet med slik behandling kan være harmonisert (lik) saksbehandling av høy kvalitet
- datakommunikasjon mellom forskjellige kommunale enheter; målet ved slik behandling kan være tilgjengelighet og rask saksbehandling
- tilkopling til eksterne datanett; målet ved slik behandling kan være å oppnå bedre grunnlag for saksbehandling og bedre tilgang til informasjon for brukerne av virksomhetens tjenester
- datakommunikasjon; målet med datakommunikasjon kan være effektiv samhandling med andre samfunnssektorer eller forvaltningsnivå.
- bruk av hjemmekontor og telependling som del av virksomhetens elektroniske behandling av personopplysninger.

Eksempel på overordnet mål:

"Kommunens målsetting er å yte innbyggerne tjenester med høy kvalitet og samtidig å utnytte kommunens ressurser optimalt. Bruk av moderne informasjonsteknologi gjør det mulig å løse kommunale oppgaver best mulig. Samtidig vil bruk av slik teknologi introdusere trusler overfor de opplysninger som behandles. Kommunens overordnede mål ved elektronisk behandling av personopplysninger er derfor sikker og effektiv saksbehandling".

Virksomhetens ledelse skal utarbeide mål for informasjonssikkerheten i virksomheten. Sikkerhetsmålet skal angi overordnede krav til personopplysningenes konfidensialitet, integritet og tilgjengelighet. Sikkerhetsmålet skal ta utgangspunkt i lovpålagte krav til informasjonssikkerhet.

Eksempel på sikkerhetsmål:

"Ved elektronisk behandling av personopplysninger skal opplysningene sikres tilstrekkelig:

- konfidensialitet, slik at opplysningene ikke blir kjent for uvedkommende
- tilgjengelighet, slik at alle medarbeidere med tjenstlig behov kan utføre pålagte oppgaver, og brukerne av kommunens tjenester gis tilfredsstillende informasjon
- integritet, slik at opplysningene ikke utilsiktet endres ved behandlingen

Kommunen skal ha et bevisst forhold til de risikoer som gjelder ved elektronisk behandling av personopplysninger. Sikkerhetstiltak skal baseres på etablerte og velprøvde løsninger som gir god margin i forhold til sikkerhetsbehovet. Ved behandling av sensitive personopplysninger skal krav til konfidensialitet ikke vike til fordel for krav til tilgjengelighet.

Informasjonssikkerheten i kommunen skal kontinuerlig etterprøves og forbedres. Kommunens medarbeidere skal ha tilstrekkelig kompetanse og gis nødvendig opplæring slik at tilfredsstillende informasjonssikkerhet opprettholdes.

Kommunen er underlagt krav om forholdsmessig sikring av informasjonssystemet etter personopplysningsloven, krav om profesjonsbestemt taushetsplikt, og krav om taushetsplikt etter forvaltningsloven. Elektronisk behandling av personopplysninger skal være i samsvar med disse".

Virksomhetens sikkerhetsmål skal dokumenteres og undertegnes av representant for virksomhetens ledelse.

5 Sikkerhetsstrategi

Virksomheten skal beskrive valg og prioriteringer i sikkerhetsarbeidet i en sikkerhetsstrategi.

Sikkerhetsstrategien skal ha sikkerhetsmålet som utgangspunkt, og på overordnet nivå beskrive ansvars- og myndighetsforhold, valg og prioriteringer, forholdet til partnere og leverandører, samt organisatoriske og tekniske sikkerhetstiltak.

Eksempel på sikkerhetsstrategi:

"Arbeidet med informasjonssikkerhet inngår som en integrert del av de oppgaver som påhviler kommunens enkelte etater/seksjoner. Etatsledere/seksjonssjefer skal påse at tilfredsstillende informasjonssikkerhet oppnås ved behandling av personopplysninger innen den enkeltes myndighetsområde.

Driftstekniske oppgaver i tilknytting til informasjonssystemet påhviler i første rekke kommunens sentrale IT-avdeling. Vedlikehold og feilretting utføres av leverandører i kontraktfestet forhold.

Sensitive personopplysninger skal føres i dedikerte informasjonssystemer uten tilkopling til kommunens øvrige informasjonssystem eller eksterne datanett."

Eksempel på sikkerhetsstrategi knyttet til organisering av informasjonssystemet:

"Overordnet operativt ansvar for drift av informasjonssystemet er tillagt IT-driftsleder med arbeidsoppgaver som angitt i stillingsbeskrivelse. Overordnet operativt ansvar for informasjonssikkerheten er tillagt kommunens sikkerhetsansvarlig med arbeidsoppgaver som beskrevet i stillingsbeskrivelse. IT-driftsleder og Sikkerhetsansvarlig rapporterer direkte til Rådmannen.

Det er utpekt kontaktpersoner for informasjonssikkerhet og for drift av informasjonssystemet for de deler av virksomheten som er etablert utenfor kommunens sentrale lokalisering.

All bruk av informasjonssystemet utføres i samsvar med på forhånd fastlagte rutiner. Det påhviler den enkelte medarbeider å rapportere avvik eksempelvis i form av sikkerhetsbrudd, til nærmeste overordnede og til kommunens sikkerhetsansvarlig.

Kommunens informasjonssystem skal være konfigurert i samsvar med konfigurasjonskart. Kun utstyr eller program eiet/disponert av kommunen skal inngå i informasjonssystemet."

Eksempel på sikkerhetsstrategi for partnere og leverandører:

"Kommunens bruk av partnere og leverandører reguleres av kontrakter, hvor også bestemmelser om informasjonssikkerhet inngår.

Ved valg av partner eller leverandør vurderes ikke bare pris, leveringsdyktighet og leveransekvalitet, men også partneren/leverandørens mulighet for å følge opp og vedlikeholde leveransen over tid.

I den grad personell hos partner eller leverandør gis adgang til utstyr eller programmer hvor sensitive personopplysninger behandles, gis tilgang til selve opplysningene eller til informasjon om sikring av slike opplysninger, har kommunen oversikt over hvilket personell dette gjelder. Kommunen skal sørge for at angjeldende personell er informert om den taushetsplikt som gjelder."

Eksempel på sikkerhetsstrategi for personellsikkerhet:

"Medarbeidere med tjenstlig adgang til informasjonssystemet skal ha tilstrekkelig kunnskaper om bruk av informasjonssystemet og nødvendig kompetanse i informasjonssikkerhet.

Medarbeidere gis kun tilgang til personopplysninger i den grad dette er nødvendig for å utføre pålagte oppgaver. Alle medarbeidere er informert om den taushetsplikt som gjelder."

Eksempel på strategi for fysisk sikkerhet:

"Utstyr benyttet for behandling av personopplysninger er sikret mot uautorisert adgang. Utstyr benyttet for å behandle sensitive personopplysninger er plassert i egne områder fysisk sikret i forhold til kommunens øvrige informasjonssystem. Tilsvarende gjelder for utstyr som inngår i sikkerhetsbarrierer mellom informasjonssystemets forskjellige soner, og mellom kommunens informasjonssystem og eksterne datanett."

Eksempler på sikkerhetsstrategi for systemteknisk sikkerhet:

"Kommunens informasjonssystem er inndelt i soner som gjenspeiler skillet mellom behandling av sensitive og "ikke-sensitive" personopplysninger. De deler av informasjonssystemet hvor sensitive personopplysninger behandles, er videre inndelt i samsvar med formålet med behandlingen av personopplysninger/tjenester kommunen leverer.

Brukere i sikrede soner gis begrenset tilgang til tjenester i de øvrige deler av kommunens informasjonssystem, men ikke til tjenester i eksterne datanett.

På hjemmekontor benyttes kun utstyr og program eiet/disponert av kommunen og som inngår i konfigurasjonskontrollen. Hjemmekontor benyttes kun for å utføre pålagte oppgaver. Utstyr benyttet for behandling av sensitive personopplysninger på hjemmekontor vil ikke på noe tidspunkt direkte eller indirekte tilkobles eksterne datanett."

Eksempel på sikkerhetsstrategi for dokumentsikkerhet:

"Ved merking fremgår det klart hvorvidt dokumenter inneholder sensitive personopplysninger og strategi, eller tiltak for sikring av slike opplysninger."

Virksomhetens sikkerhetsstrategi skal dokumenteres og undertegnes av representant for virksomhetens ledelse.

Sikkerhetsstrategien gir premissene for hva som er akseptabel risiko i virksomheten. Hvorvidt de valgte sikkerhetstiltak gir tilfredstillende sikkerhet måles gjennom risikovurderinger.

6 Personopplysninger

Virksomheten skal utarbeide og holde oppdatert en oversikt over hvilke behandlinger av personopplysninger som foretas, og hvilke opplysninger som inngår i disse.

Oversikten danner grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og –strategi. Dessuten benyttes den som underlag ved risikovurderinger.

Oversikten over personopplysninger som behandles skal gi kortfattet informasjon om:

- hvilke opplysninger som lagres og formålet med behandlingen,
- hjemmelsgrunnlag for å behandle opplysningene
- klassifikasjon av hvorvidt personopplysningene er sensitive eller ikke
- teknologiske sikkerhetstiltak med angivelse av sone eller nettverk
- hvor opplysningene lagres og om de overføres via eksterne media
- registerets omfang

Eksempel på oversikt over personopplysninger som behandles:

Informasjon Formål	**Hjemmel**	**Melding/ Konsesjon**	**Klassifikasjon**	**Sikrings-tiltak**	**Lagring og kommunikasjon**	**Opplysningenes omfang**
Lønn og personal: -lønnsopplysn. - personalopplysn.	Person-opplysnings-loven, § 8	Unntatt i forskriften	Person-opplysninger	internt nettverk	Felles datarom kommunikasjon til teknisk etat	ca. ..... ansatte
Barnevern: -vurdering og tiltak	Barnevern-loven, § 3-1	Meldt 14.01.2004	Sensitive opplysninger	isolert nettverk	På etaten - ingen ekstern kommunikasjon	ca ..... barn og foresatte
Helse opplysninger: - pasientjournal	Helse-personelloven § 39 flg.	Meldt 14.01.2004	Sensitive Opplysninger	Sikret sone, kryptering	Felles datarom kommunikasjon til legesenter	ca. ..... pasienter
Sosial omsorg: - klient økonomi - sosiale ytelser	Sosialtjeneste-loven § 2-1	Meldt 14.01.2004	Sensitive Opplysninger	Sikret sone, sosial-kontor	Felles datarom ingen ekstern kommunikasjon	ca. ..... klienter
Elevadministrasjon - elever / foresatte - lærere	Opplærings-loven § 13-5		Person Opplysninger	internt nettverk	Felles datarom ekstern kommunikasjon til skolene.	ca. ..... søkere
Hendelsesregister: - logg over brudd	Person-opplysnings-loven, § 13	Unntatt i forskriften	Sensitive sikkerhetsoppl.	Sikret teknisk sone	Felles datarom ingen ekstern kommunikasjon	Ca. .....
Sikkerhetsorg. - ansatte og oppg.	Person-opplysnings-loven, § 13		Person Opplysninger	Sikret teknisk sone	Felles datarom ingen ekstern kommunikasjon	Ca. .....

7 Risikovurdering

Virksomheten skal gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel endringer i informasjonssystemet eller endringer i trusselbildet. Risiko betegner forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse.

Formålet med risikovurdering er å undersøke hvorvidt den risiko som avdekkes er innenfor de akseptkriterier virksomheten har fastlagt. Risikovurderingen danner grunnlag for iverksetting av nødvendige sikkerhetstiltak, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten.

Eksempler på elementer som inngår i risikovurdering:

- planlegging og oppstart
- beskrivelse og avgrensing av analyseobjekt
  - identifisering av hvor personopplysningene befinner seg i informasjonssystemet
  - identifisering av tiltak for sikring av personopplysningene
- beskrivelse av trusler mot informasjonssikkerheten med hensyn til:
  - konfidensialitet
  - tilgjengelighet
  - integritet
- årsaksanalyse dvs. vurdering av hvordan en uønsket hendelse kan inntreffe
- konsekvensanalyse dvs. vurdering av de følger en uønsket hendelse kan medføre
- frekvensanalyse dvs. vurdering av sannsynlighet for at en uønsket hendelse kan inntreffe
- beskrivelse av risiko
- vurdering av hvorvidt den avdekkede risiko er innefor akseptkriteriene
- vurdering av sikkerhetstiltak.

Risikovurdering skal gi følgende resultat:

- oversikt over identifiserte trusler
- angivelse av sannsynlighet for at en uønsket hendelse kan inntreffe
- angivelse av konsekvenser av en uønsket hendelse
- resultat fra analyse av sikkerhetstiltakenes effekt i forhold til risiko.

Virksomhetens ledelse har ansvar for iverksetting av risikovurdering. Resultat fra analysen rapporteres til virksomhetens ledelse.

I arbeidet med risikovurdering vises det til Datatilsynets veileder ”Risikovurdering av informasjonssystem” og standarden NS 5814 Krav til risikoanalyser.

8 Sikkerhetsrevisjon

Virksomheten skal periodisk kontrollere arbeidet med informasjonssystemet og informasjonssikkerheten.

Formålet med sikkerhetsrevisjon er å sikre at besluttet sikkerhetsmål, -strategi og organisering etterleves i hele virksomheten. Resultat av sikkerhetsrevisjon danner grunnlag for eventuelle endringer i sikkerhetsmål, -strategi og organisering, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten.

Sikkerhetsrevisjon skal gjennomføres slik at alle deler av virksomheten kontrolleres

innenfor et 12 måneders intervall. Kontroll av informasjonssystemets enkelte deler kan med fordel fordeles jevnt i dette intervallet slik at informasjonssystemets drift forstyrres minst mulig.

Ved gjennomføring av kontrollen skal bl.a. følgende elementer gjennomgås:

- ansvars- og myndighetsforhold
- utførelse av arbeidsoppgaver i tilknytting til informasjonssystemet
- sikkerhetstiltak, herunder utprøving av tekniske sikkerhetsløsninger
- gjennomgang av avvik registrert siden forrige kontroll.

Eksempel på elementer som inngår i sikkerhetsrevisjon:

- "kontrollplan med angivelse av hva som skal kontrolleres og tidspunkt for den enkelte kontroll.
- varsling av kontrollen slik at berørt personell er tilstede og forberedt
- utarbeidelse av spørsmål/sjekkliste omfattende de elementer som skal gjennomgås
- rapportering."

Eksempel på kontrollplan:

Kontrollobjekt	Kontrollsted	jan. feb.	mars april	mai juni	juli aug	Sept Okt	nov Des
Sosialtjenesten	Sosial Kontoret				*1 aug* *1 sept*		
Barneverntjenesten	Barnevern- kontoret				*15 aug* *1 sept*		
PP-tjenesten	PPT- kontoret				*15 aug* *1 sept*		
Legesentre	Legesenteret					*1 sept.* *15 sep*	
Helseinstitusjoner	Institusjon a Institusjon b					*1 sept.* *15 sept*	
Barnehager	Barnehage a Barnehage b					*1 okt.* *15 okt*	
Skoler	Skole a Skole b					1 okt. 15 okt	
Intern driftsløsning (servere, nett)	EDB-avd						*1 nov* 15 nov
Intern tilkopling (intern brannmur/ruter)	EDB-avd						1 nov 15 nov
Ekstern tilkopling, (ytre brannmur)	EDB-avd						15 nov 1 des

Planen angir dato med frist for kontroll og dato for iverksetting av korrigerende tiltak.

Virksomhetens ledelse har ansvar for iverksetting av sikkerhetsrevisjon. Sikkerhetsrevisjoner kan ledes av sikkerhetsansvarlig. Gjennomføringen bør utføres slik at den som leder kontrollen ikke selv er ansvarlig for den del av virksomheten som kontrolleres. Resultat fra sikkerhetsrevisjon rapporteres til virksomhetens ledelse. Eventuelle avvik avdekket i sikkerhetsrevisjon, behandles i samsvar med virksomhetens system for avvikshåndtering.

9 Ledelsens gjennomgang

Ledelsen skal årlig gjennomgå sikkerhetsmål, strategi og organisering av informasjonssystemet. Ledelsen skal kontrollere at disse er i samsvar med virksomhetens behov.

Formålet med ledelsens gjennomgang er at ledelsen gis mulighet til å vurdere status for

sikkerheten i den elektroniske behandlingen av personopplysninger i virksomheten. Videre skal gjennomgangen danne grunnlag for nødvendig revisjon av sikkerhetsmål og sikkerhetsstrategi.

Ved ledelsens gjennomgang deltar representanter fra virksomhetens øverste ledelse sammen med sikkerhetsansvarlig og IT-driftsleder. Praktisk organisering av gjennomgangen, utarbeidelse av rapport, iverksetting av eventuelle tiltak, kan med fordel legges til sikkerhetsansvarlig.

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 / utvidet bruk.

Eksempel på rapport fra ledelsens gjennomgang av informasjonssystemet og av informasjonssikkerheten:

Rapport fra ledelsens gjennomgang 2004	Virksomhet: Kommunen	Skrevet av: JBL	dato: 1.12.2004	arkivref: xx.yyyy
Deltagere: Rådmann Sikkerhetsansvarlig IT-driftsleder Etatssjefer med operativt ansvar for behandling av personopplysninger				
Distribusjon: Møtedeltakerne				

Saknr.	Sak	Aksjon	Ansvarlig / frist
1/04	Rapporter fra utførte sikkerhetsrevisjoner. - Rapportene fra sikkerhetsrevisjoner ble lagt fram uten merknader		
2/04	Behandling av registerte sikkerhetsbrudd og logger. - Innbrudd på sosialkontoret bør gi endret sikkerhetsstrategi	Det innhentes bistand til endring.	IT-driftsleder, 15.12.04
3/04	Behandling av foreslåtte nye løsninger. - Prosjektforslaget for bruk av hjemmekontor ble godkjent.		

Del III Organisering

10 Organisasjon

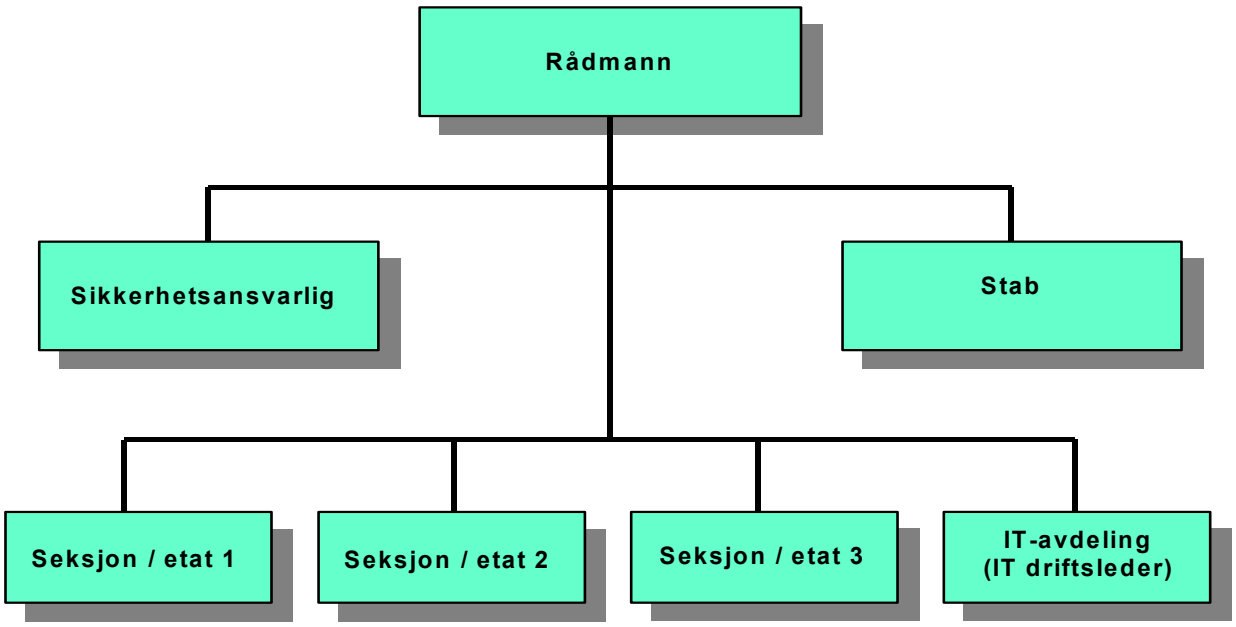
Arbeidet med informasjonsbehandlingen skal organiseres slik at tilfredsstillende informasjonssikkerhet oppnås. Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.

Organiseringen av sikkerhetsarbeidet skal være en del av virksomhetens ordinære organisering. Virksomheten bør unngå å opprette en egen "sikkerhetsorganisasjon" på siden av normale organisasjoner. Virksomhetens ledelse skal delegere overordnet operativt ansvar for informasjonssikkerheten til en av virksomhetens medarbeidere. Videre skal overordnet operativt ansvar for drift av informasjonssystemet delegeres til en av virksomhetens medarbeidere. Disse to funksjoner skal rapportere til virksomhetens ledelse og bør delegeres til to forskjellige medarbeidere. I mindre virksomheter vil delegering til to forskjellige medarbeidere ikke alltid være praktisk mulig.

Dersom virksomheten er etablert på flere geografiske steder skal det på hvert sted utpekes personell med ansvar for drift og informasjonssikkerhet. Disse rapporterer til sikkerhetsansvarlig og driftsleder.

Ansvar og myndighetsforhold skal være avklart og dokumentert slik at

- brukere kjenner og følger de fastlagte rutiner som gjelder for bruk av informasjonssystemet, herunder gjennomføre de sikkerhetstiltak brukeren selv er ansvarlig for
- medarbeidere og innleid personell som utfører drift og vedlikehold, utfører arbeidet i samsvar med fastlagte rutiner.



FIGUR 1: Eksempel på organisering av sikkerhet og IT-drift:

Organisasjonskartet angir funksjoner. I mindre virksomheter kan det være nødvendig å gi samme person ansvaret for flere funksjoner.

11 Konfigurasjon

11.1 Konfigurasjonskontroll

Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås. Kun utstyr eller program eiet / disponert av virksomheten skal inngå i konfigurasjonen. Dette gjelder også utstyr eller program benyttet på hjemmekontor eller til telependling.

Det skal være fastlagte rutiner for hvordan utstyr som har vært frakoplet skal koples til informasjonssystemet.

Formålet med konfigurasjonskontrollen er å sikre at utstyr og program fungerer sammen som forutsatt, samt at virksomhetene til enhver tid har en oppdatert oversikt over informasjonssystemets konfigurasjon, bl.a. til bruk ved risikovurderinger, sikkerhetsrevisjon, ledelsens gjennomgang av informasjonssystemet og av informasjonssikkerheten mv.

Konfigurasjonen skal dokumenteres i en oversikt, eksempelvis i form av konfigurasjonskart og støttende beskrivelse, som angir:

- koblinger mellom utstyr og program
- inndeling av informasjonssystemet i soner
- kommunikasjonspunkt for tikopling til ekstern datakommunikasjon.

Eksempel på overordnet konfigurasjonskart, se fig. 5 i kap. 18

Videre skal utstyr eller programmer med betydning for informasjonssikkerheten, herunder tekniske sikkerhetsbarrierer, dokumenteres. Slik dokumentasjon bør omfatte:

- navn eller modellbetegnelse, og serienummer eller versjonsnummer
- sikkerhetsfunksjoner med opplysninger om oppsett/innstilling av utstyr/program
- når utstyret ble tatt i bruk, eller når utstyret ble tatt ut av bruk
- opplysninger om vedlikehold, skade, funksjonsfeil, reparasjoner.

Dokumentasjon av sikkerhetsløsning skal omfatte de kravene som er inntatt i kapittel 18.

Arbeidet med å utarbeide og holde oppdatert konfigurasjonsoversikt og beskrivelser av utstyr/programmer, kan delegeres virksomhetens IT-driftsleder.

11.2 Konfigurasjonsendring

Endringer i informasjonssystemets konfigurasjon skal utføres planmessig og systematisk, og bare etter godkjenning fra virksomhetens ledelse.

Formålet er å sikre at konfigurasjonsendringer er i samsvar med besluttet sikkerhetsstrategi, og at informasjonssystemet fungerer som forutsatt også etter at endringen er gjennomført.

Sentrale elementer ved endring av konfigurasjonen er:

- behovs- og kompatibilitetsanalyse

- risikovurdering dersom endringen vil kunne få innvirkning på informasjonssikkerheten
- utprøving og testing.

Endringer av informasjonssystemets konfigurasjon besluttes av virksomhetens ledelse. Arbeidet med selve gjennomføringen av endringen kan delegeres virksomhetens IT-driftsleder.

12 Administrative og tekniske rutiner

Informasjonssystemet skal benyttes i samsvar med fastlagte rutiner. I den grad det er nødvendig for å oppnå tilfredsstillende informasjonssikkerhet, skal rutiner utarbeides for bruk, drift og vedlikehold av det enkelte utstyr eller program.

Arbeidet med informasjonssystemet er basert på rutiner for å sikre at alle aktiviteter med betydning for informasjonssikkerhet gjennomføres, og at arbeidsoppgaver utføres likt hver gang de repeteres.

Rutiner skal ha en detaljeringsgrad tilpasset virksomhetens behov, og angi:

- ansvar for at arbeidsoppgaven utføres, og ansvar for utarbeidelse/vedlikehold av rutinen
- tidspunkt for utførelse av arbeidsoppgaven
- hvilke aktiviteter som skal gjennomføres
- hvilke resultat som skal oppnås og hvordan disse formidles/rapporteres i organisasjonen.

I tillegg til de rutiner som dette dokument stiller krav om er det aktuelt å utarbeide rutiner for en rekke andre forhold:

Eksempler på rutiner:

- mottak, installasjon og utprøving av utstyr og program
- oppgradering og vedlikehold av utstyr og program
- brukerstøtte.

Rutiner kan utarbeides av de medarbeidere som er best kjent med/skal utføre arbeidsoppgavene. Ansvaret for å godkjenne rutiner kan delegeres virksomhetens sikkerhetsansvarlig / IT-driftsleder.

13 Beredskapsplanlegging

13.1 Planlegging for utilsiktet avbrudd

Dersom virksomheten vurderer det som nødvendig, skal det ved avbrudd i driften av informasjonssystemet etableres alternativer til normal behandling av personopplysningene.

Formålet med beredskapsplanlegging er å sikre nødvendig behandling av personopplysninger også ved avbrudd i normal drift, samt at alternativ behandling utføres planmessig.

Elementer som skal inngå i beredskapsplaner er:

- ansvar for å utarbeide beredskapsplaner og ansvar for å iverksette alternativ drift
- vurdering av avbruddets virkning på informasjonssystemet og for informasjonssikkerheten
- alternativ behandling, herunder beskrivelse av utstyr, program og manuell behandling
- verifisering av informasjonssystemet og metode for gjenskaping av normal drift etter korreksjon
- utprøving og øving av beredskapsplaner.

Beredskapsplaner kan utarbeides av virksomhetens IT-driftsleder, som også kan delegeres ansvaret for å iverksette alternativ behandling av personopplysninger.

13.2 Sikkerhetskopiering

Virksomheten skal sikkerhetskopiere data inneholdende de personopplysninger som behandles. Videre skal programmene som benyttes i behandlingen, og programmer med betydning for informasjonssikkerheten kopieres. Sikkerhetskopier av programmer skal også omfatte oppsett og innstilling.

Formålet med sikkerhetskopiering er å gjøre det mulig å gjenopprette normal drift av informasjonssystemet etter avbrudd eller feil, herunder etablere tekniske sikkerhetsløsninger på nytt, samt gi tilgang til de personopplysninger som behandles.

Rutine for sikkerhetskopiering skal angi:

- ansvar for å beskrive hvordan sikkerhetskopiering skal utføres og ansvar for selve kopieringen
- hvilke data som skal kopieres
- kopieringstidspunkt og intervall
- metode for verifisering av reservekopi
- lagring av reservekopi, herunder angivelse av lagringsmedium og sikring av dette, samt metode for gjennomretting av normal drift av informasjonssystemet ved bruk av sikkerhetskopier.

Sikkerhetskopiering, herunder valg av tidspunkt, intervall, lagringsmedia og sikring av lagringsmedia bør tilpasses ulike feilsituasjoner. Sikkerhetskopier til bruk ved feil hvor konsekvensene for personopplysningene er liten bør være enkelt tilgjengelig, for eksempel

i nærheten av det utstyr hvor personopplysningene eller programmet normalt befinner seg. Sikkerhetskopier til bruk ved feil hvor konsekvensen for personopplysningene er store skal lagres på et annet sted enn der personopplysningene eller programmet normalt benyttes.

Eksempler på valg av kopieringsintervall, lagringsmedium og lagringssted ved sikkerhetskopiering:

Komponent som skal kopieres	**Nærkopi på datarom:** **- intervall** **- kopieringmåte** **- medium**	**Fjernkopi i annen bygning:** **- intervall** **- kopieringsmåte** **- medium**
Basisprogramvare til brannmurer, servere og annet utstyr	- Ved hver ny versjon - En komplett kopi - Disk, CD-rom mv.	- Ved hver ny versjon - En komplett kopi - Disk, CD-rom mv.
Konfigureringer og innstillinger for brannmurer, servere og annet utstyr	- Ved hver ny konfigurering - En endringskopi - Disk / tape.	- Ved hver ny versjon - En komplett kopi - Tape mv.
Sensitive personopplysninger	- Daglig - Rullerende kopi i 5 gen. - Disk / tape.	- Ukekopi - En komplett kopi - Tape mv.
Personopplysninger	- Daglig - Rullerende kopi i 5 gen. - Disk / tape.	- Ukekopi - En komplett kopi - Tape mv.
Andre data	ved behov	ved behov

Virksomheten bør også ha rutiner som sørger for at det ikke oppbevares unødvendige sikkerhetskopier, og at sikkerhetskopiene slettes tilfredstillende når formålet er oppfylt.

Rutiner for sikkerhetskopiering kan utarbeides av virksomhetens IT-driftsleder, mens medarbeidere som behandler personopplysninger eller bruker de aktuelle programmene, kan utføre selve sikkerhetskopieringen.

14 Avviksbehandling

Dersom informasjonssystemet benyttes i strid med fastlagte rutiner, ved brudd på informasjonssikkerhet, samt mistanke om sikkerhetsbrudd, skal virksomheten iverksette avviksbehandling.

Formålet med avviksbehandling er å bringe avviket til opphør, gjenopprette normal tilstand, og hindre gjentagelse. Dersom det ikke er samsvar mellom fastlagte rutiner og hvordan informasjonssystemet faktisk benyttes, skal resultatet fra avviksbehandling benyttes som grunnlag ved gjennomgang og endring av de aktuelle rutiner. Avviksbehandling består av:

- deteksjon av avviket
- rapportering; normalt utføres dette av den medarbeider som oppdager avviket. Avviket rapporteres til virksomhetens i henhold intern organisering.
- iverksetting av strakstiltak bl.a. med det formål å avgrense eventuelle følgeskader. Strakstiltakene kan utføres av den medarbeider som oppdager avviket, eventuelt av den medarbeider som betjener eller har ansvar for den berørte del av informasjonssystemet.
- iverksetting av korrigerende tiltak for permanent å gjenopprette normal tilstand. Dette utføres normalt av virksomhetens IT-driftssjef.

- vurdering, etter noe tid, av hvorvidt det korrigerende tiltak fungerer etter sin hensikt. Vurderingen utføres av virksomhetens IT-driftssjef, eventuelt av sikkerhetsansvarlig ved gjennomføring av ledelsens gjennomgang.

Eksempler på situasjoner som gjør det nødvendig å iverksette avviksbehandling:

- ved utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering
- når medarbeidere benytter informasjonssystemet uten autorisasjon
- når medarbeidere benytter informasjonssystemet uten den opplæring som er forutsatt.
- ved feil i utstyr eller program som kan ha innvirkning på informasjonssikkerheten eller driften av informasjonssystemet.

Avviksbehandling skal dokumenteres i en rapport som inneholder opplysninger om selve avviket, strakstiltak som er utført, korrigerende tiltak som er iverksatt, resultater fra evaluering av det korrigerende tiltakets effekt over tid samt opplysninger om hvilke medarbeidere som har vært involvert i behandlingen av avviket.

Rapportering av avvik utføres normal av de medarbeidere som oppdager avviket, eventuelt av den medarbeider som betjener eller har ansvar for den berørte del av informasjonssystemet. Korrigerende tiltak iverksettes av virksomhetens IT-driftssjef. Vurdering av det korrigerende tiltakets effekt over tid utføres av virksomhetens IT-driftssjef, evt. av sikkerhetsansvarlig ved gjennomføring av ledelsens gjennomgang.

Dersom avviket har medført en uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.

Eksempel på avviksrapport.

<table>
<tr><td>Avviksrapport</td><td>Virksomhet: Kommunen</td><td>sendes til: Sikkerhetsansv.</td><td>saksident: xxxx</td></tr>
<tr><td colspan="4">Formål: Rapporten skal sikre at alle brudd og antatte brudd på sikkerhetsrutinene blir registret og behandlet på forsvarlig måte.</td></tr>
<tr><td colspan="4">Beskrivelse av avviket:
xxxxxxx
xxxxxxx
vedlegg:</td></tr>
<tr><td colspan="4">Beskrivelse av midlertidig tiltak:
xxxxxxx
xxxxxxx
vedlegg:</td></tr>
<tr><td>Melderens registrering</td><td>Navn:
Xxxxxxxxx</td><td>utstyr/ident:
xxxxxxxx</td><td>dato/ kl:
xxxxxxxxx</td></tr>
<tr><td colspan="4">Analyse av årsak:
xxxxxxx
xxxxxxx
Vedlegg:</td></tr>
<tr><td colspan="4">Beskrivelse av iverksatte tiltak:
xxxxxxx
xxxxxxx
Henv:</td></tr>
<tr><td>Sikkerhetsansvarliges Behandling</td><td>Klassifikasjon:
Xxxxxxxxxx</td><td>Rapport sendes Datatilsynet:
JA / NEI</td><td>dato / underskrift:
JBL</td></tr>
<tr><td>Evaluert dato:</td><td></td><td></td><td></td></tr>
</table>

Del IV Sikkerhet hos andre virksomheter

15 Sikkerhet hos andre virksomheter

Virksomheter som utfører behandlinger av personopplysninger på vegne av den behandlingsansvarlige betegnes databehandlere, og forholdet til disse reguleres gjennom en databehandleravtale hvor informasjonssikkerheten vil utgjøre en del.

Det skal også inngås avtaler med øvrige virksomheter som gjennomfører sikkerhetstiltak eller gis tilgang til utstyr eller program hvor det behandles personopplysninger.

Ved valg av partner eller leverandør skal det, i tillegg til å vurdere leveransepris, tid og kvalitet, også vektlegges partnerens eller leverandørens kompetanse og evne til å vedlikeholde leveransen over tid.

Kontraktsregulering av forholdet til partnere og leverandører har som formål å avklare ansvarsdelingen med hensyn til informasjonssikkerhet, samt å utstyre virksomheten med et styringsverktøy overfor partner eller leverandør. For databehandlere skal det reguleres hvordan disse skal behandle personopplysninger.

Eksempler på partnere eller leverandører hvor det er aktuelt å inngå kontrakt med sikkerhetsvilkår:

- databehandlere
- leverandører som gjennomfører sikkerhetstiltak
- firma med konsulentoppdrag i tilknytting til informasjonssystemet
- firma som utfører vedlikehold av utstyr eller program, eller som utfører arbeid i områder hvor utstyr eller program befinner seg
- renholdsfirma
- vikarbyrå.

Av de sikkerhetskrav som fremgår av retningslinjene for informasjonssikkerhet skal det i kontrakten spesielt legges vekt på:

- om partneren eller leverandørens personell er informert om den taushetsplikt som gjelder og at slikt personell skal undertegne taushetserklæring
- at det etableres oversikt over hvilke av partnerens eller leverandørens personell som skal gis tilgang til informasjonssystemet eller adgang til områder eller utstyr
- hvordan virksomhetens kontroll av sikkerhet hos partner og leverandør skal utføres.

Eksempel på vilkår som kan inngå i kontrakt mellom virksomheten og partner/leverandør:

Ansvar Leverandøren er ansvarlig for sikkerhetsbrudd for eget personale og brudd som har oppstått gjennom tilkopling av leverandørens utstyr. Leverandøren kan ikke engasjere en tredjepart (underleverandør) til å utføre arbeidsoppgaver som følger av denne avtalen, uten at oppdragsgiver har godkjent dette og leverandøren har inngått kontrakt med tredjepart som har tilsvarende sikkerhetsbestemmelser.
Taushetsplikt Leverandørens personale skal undertegne taushetserklæring. De som undertegner taushetserklæring skal gjøres kjent med hva dette innebærer. Leverandøren kan kun benytte de personer til oppdraget som oppdragsgiver på forhånd har godkjent og er informert om. Taushetsplikten gjelder også etter at avtalen er opphørt, og etter at leverandørens personale har sluttet hos leverandøren.
Sikkerhetsløsning Leverandøren skal til enhver tid ha en organisatorisk og teknisk sikkerhetsløsning som tilfredsstiller personopplysningsforskriften og den behandlingsansvarliges krav til tilfredstillende informasjonssikkerhet. Dette skal kunne dokumenteres overfor den behandlingsansvarlige.
Samarbeid Leverandøren skal ved behov samarbeide med oppdragsgiver om de sikkerhetsbrudd som kan tilskrives leverandøren. Som ledd i virksomhetens sikkerhetsrevisjon bør det være et møte for å gjennomgå leverandørens organisatoriske og tekniske sikkerhetstiltak

Kontraktsvilkår fastsettes av virksomhetens ledelse. Valg av partner og leverandør, og inngåelse av kontrakt, kan utføres av virksomhetens innkjøpsfunksjon, eventuelt av IT-driftsansvarlig.

Del V Sikkerhet

16 Personellsikkerhet

16.1 Kompetansekrav

Alle medarbeidere som bruker, administrerer, vedlikeholder eller utvikler informasjonssystemene, eller på annen måte påvirker informasjonssikkerheten, skal ha nødvendig kompetanse til å utføre sine oppgaver. Medarbeidere med overordnet operativt ansvar for drift av informasjonssystemet eller med informasjonssikkerheten, skal kunne dokumentere nødvendig kompetanse relevant for den teknologi virksomheten benytter i informasjonssystemet.

Virksomheten skal utarbeide rutiner som sørger for at kompetanse vedlikeholdes og utvikles. Sentrale elementer i slike rutiner består av:

- oversikt over den enkelte medarbeiders kompetanse
- oversikt over kompetansekrav for de ulike oppgaver og funksjoner
- årlige planer for kompetanseutvikling.

De årlige medarbeidersamtalene er et godt utgangspunkt for å drøfte status og videreutvikling av kompetanse hos medarbeidere.

16.2 Taushetsplikt

Medarbeidere som har tilgang til sensitive personopplysninger eller til informasjon om sikring av slike opplysninger, skal ha taushetsplikt og undertegne taushetserklæring.

Medarbeiderne skal informeres om taushetspliktens omfang og varighet, samt om konsekvenser dersom den brytes.

16.3 Autorisasjon

Det skal bare gis adgang til områder eller tilgang til personopplysninger i den grad det er nødvendig for å utføre pålagte oppgaver i henhold til vedtatt sikkerhetsstrategi.

Formålet med autorisasjonsrutinen er å sikre at de som får adgang til områder og utstyr, og tilgang til soner, data og programmer, til enhver tid har den autorisasjon som er nødvendig i forhold til tjenstlige behov.

Rutine for autorisasjonstildeling skal omfatte:

- autorisasjon av nytilsette, vikarer og partnere med henhold til tjenstlige behov
- behov for endringer ved forandring av oppgaver, herunder sletting av autorisasjon når tjenstlige behov ikke lenger er tilstede, for eksempel når en medarbeider slutter i virksomheten
- kontroll med at tildelte autorisasjoner fungerer etter forutsetningene.

17 Fysisk sikkerhet

Virksomheten skal sørge for at lokaler og utstyr den benytter er forsvarlig sikret, med spesiell vekt på de rom hvor det er plassert utstyr benyttet for behandling av sensitive personopplysninger, eller for sikring av slike (eksempelvis tjenermaskin, kommunikasjons- og nettverksenheter).

Den fysiske sikringen av behandling av sensitive personopplysninger er en vesentlig del av det totale sikkerhetskonseptet. Trusler som kan utløses ved for dårlig fysisk sikring kan bl.a. være:

- at uvedkommende får tilgang til utstyr hvor sensitive personopplysninger behandles
- tyveri av PC-er eller sikkerhetskopier på dagtid eller ved innbrudd utenom arbeidstiden
- sabotasje eller hærverk mot vitale deler av informasjonssystemet.

Selv om ingen kan sikre seg 100% mot uautorisert adgang, må de sikkerhetsløsninger som velges være slik at forsøk på inntrenging faktisk blir oppdaget. De bør også være gode nok til at et forsøk forsinkes tilstrekkelig til at respons på utløst alarm kan ha mulighet til å avverge eller begrense konsekvensene av sikkerhetsbrudd.

17.1 Adgangskontroll

Adgang til lokaler og utstyr hvor personopplysninger behandles skal kontrolleres. Det gjelder spesielle sikringstiltak der hvor det behandles sensitive personopplysninger eller der man har informasjon om sikring av slike opplysninger,.

Virksomheten må vurdere behovet for å innføre fysisk områdeinndeling av lokaler, slik at det er entydig hvilke områder som trenger spesiell beskyttelse. Denne sikringen kan gjennomføres ved bruk av adgangskontroll til lokaler eller bruk av spesielle sikringsmekanismer knyttet til bruk av selve utstyret.

For eksempel vil virksomheter hvor publikum har adgang nødvendigvis måtte definere hvor det benyttes adgangskontroll og hvor en må benytte sikring på bruk av utstyret.

17.1.1 Adgang til område

Ved bruk av områdesikring med adgangskontroll der sensitive personopplysninger behandles, skal det kontrolleres at kun autorisert personell har selvstendig adgang til disse. Dette innebærer følgende:

- områder der sensitive personopplysninger behandles skal være kontrollert av adgangskontrollsystem
- før nøkkelansvarlig tildeler den enkelte nøkler og koder for adgang, skal skriftlig autorisasjon mottas
- tildelte adgangsrettigheter skal begrenses til det som er nødvendig ut fra tjenstlig behov, og skal alltid fjernes når arbeidsforholdet opphører
- besøkende skal alltid følges av medarbeider som er autorisert for adgang til området, og skal aldri etterlates alene i slike områder.

17.1.2 Adgang til utstyr

Ved bruk av mekanismer for sikring av adgang til utstyr for behandling av sensitive personopplysninger, skal mulig bruk av utstyret begrenses til de som har tjenstlig behov for dette.

Det utstyret som benyttes ved behandling av sensitive personopplysninger (arbeidsstasjoner og skrivere, kopimaskiner, telefaks etc.) må innrettes slik at tilgangen begrenses til de som har tjenstlig behov. Dette gjennomføres ved bruk av betryggende rutiner og teknisk sikring for å hindre uautorisert bruk at utstyret, samt egnede tiltak mot innsyn.

17.1.3 Fysisk sikkerhet i andre lokaler

Utstyr benyttet på hjemmekontor skal fysisk sikres ved bruk av normal bygningsmessig sikkerhet. Videre bør det innskjerpes at avlåsing og lukking av vinduer blir gjort når lokalene ikke er i bruk.

18 Systemteknisk sikkerhet

Tilgang til tjenester og informasjon i nettverk skal kun gis etter tjenstlig behov. Som utgangspunkt skal alle tjenester være sperret. Mulig sikkerhetsarkitektur vil i prinsippet omfatte enkle løsninger der det er et fysisk skille mellom risikoutsatte tjenester og sensitive personopplysninger, og stadig mer omfattende løsninger der det er behov for en mer integrert nettverksløsning for bruk av ulike opplysninger.

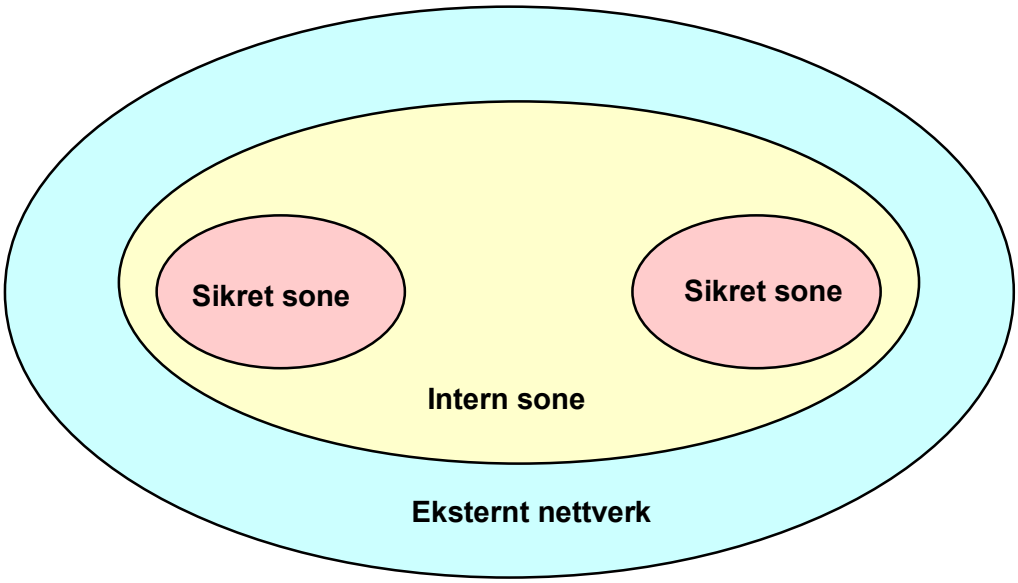
Hvorvidt man har mulighet til å iverksette en tilstrekkelig sikkerhetsløsning vil være bestemmende for graden av integrasjon og funksjonalitet i informasjonssystemet.

18.1 Sikkerhetsarkitektur. Inndeling i soner.

Soner benyttes som et grunnleggende prinsipp i sikkerhetsarkitekturen. En sone er de deler av et informasjonssystem som tillates å kommunisere ved datakommunikasjon. Soner opprettes etter analyse av behovet for tilgang og datakommunikasjon. For å begrense tilgangen til personopplysninger, benyttes følgende soner internt i en virksomhet (ref. figur 2):

- Sikret sone hvor sensitive personopplysninger behandles (ved behov opprettes flere sikrede soner i virksomheten). Den enkelte sikrede sone er sikkerhetsmessig atskilt fra resten av det interne nettverk og eventuelle andre sikrede soner, foruten mot eksterne nettverk.
- Intern sone hvor ikke sensitive personopplysinger behandles, denne kan også omfatte andre opplysninger i virksomheten som ikke skal eksponeres eksternt.

Eksterne nettverk som virksomheten benytter men som ikke kontrolleres av virksomheten er tegnet inn på figuren, da interne informasjonssystemer også kan kommunisere med slike.

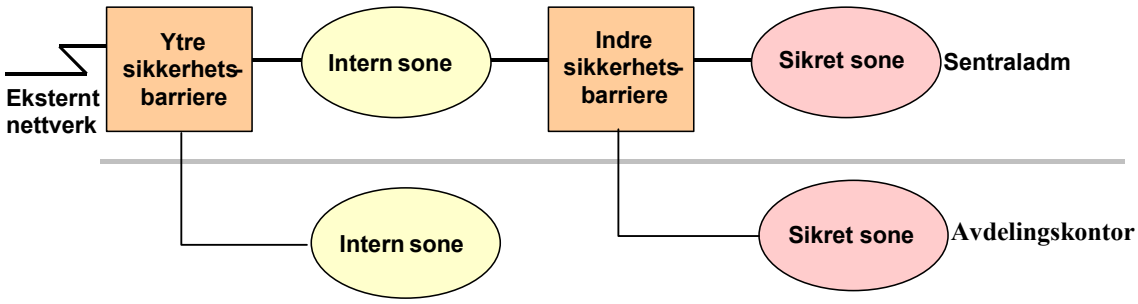


FIGUR 2: **Sikkerhetsarkitektur – inndeling i soner**

Sikkerhetsarkitekturen skal videre ivareta følgende:

- Sensitive personopplysninger skal behandles og lagres i sikrede soner hvor kun autoriserte brukere gis tilgang. En virksomhet kan opprette flere sikrede soner avhengig av behovet.
- Skillet mellom sikret sone og intern sone skal gjennomføres slik at det ikke er mulig for brukere å overstyre innlagte begrensninger. Det må som minimum være én teknisk sikkerhetsbarriere mellom sikret sone og intern sone.
- Skillet mellom eksterne nettverk og sikret sone skal utgjøres av to tekniske sikkerhetsbarrierer.
- Ingen tjenester skal kunne initieres fra andre soner og inn i sikret sone med mindre særskilte tekniske sikkerhetstiltak er iverksatt.
- Ved ekstern formidling av sensitive personopplysninger samt informasjon om sikring av slike opplysninger skal data krypteres.
- Krypteringsnøkler for systemer(eksempelvis VPN) skal håndteres minst like sikkert som opplysningene krypteringen er ment å beskytte, og tilgang til disse skal reguleres av tjenestlig behov.

18.2 Tilgangskontroll



FIGUR 3: **Soneinndeling ved behandling av ulik informasjon**

Figuren viser soneinndeling ved behandling av ulik informasjon. Systemteknisk sikkerhet ivaretas ved sikkerhetsbarrierer som beskrevet nedenfor. Funksjonelle krav til de ulike sikkerhetsbarrierene beskrives fra kap. 18.2.1. Sentraladministrasjonen eller virksomhetens hovedkontor behandler både sensitive personopplysninger, alminnelig intern informasjon og er tilknyttet eksternt nettverk:

- ytre sikkerhetsbarriere som sikkerhetsløsning mellom eksternt nettverk og intern sone
- indre sikkerhetsbarriere som sikkerhetsløsning mellom internt nettverk og sikret sone.

På et avdelingskontor der noen medarbeidere er autorisert for tilgang til sensitive personopplysninger, mens andre behandler øvrig informasjon, benyttes følgende løsning:

- sikret sone tilkoples sentraladministrasjonens indre sikkerhetsbarriere via kryptert forbindelse for tilgang til sensitive personopplysninger
- intern sone tilkoples sentraladministrasjonens ytre sikkerhetsbarriere for tilgang til øvrig informasjon.

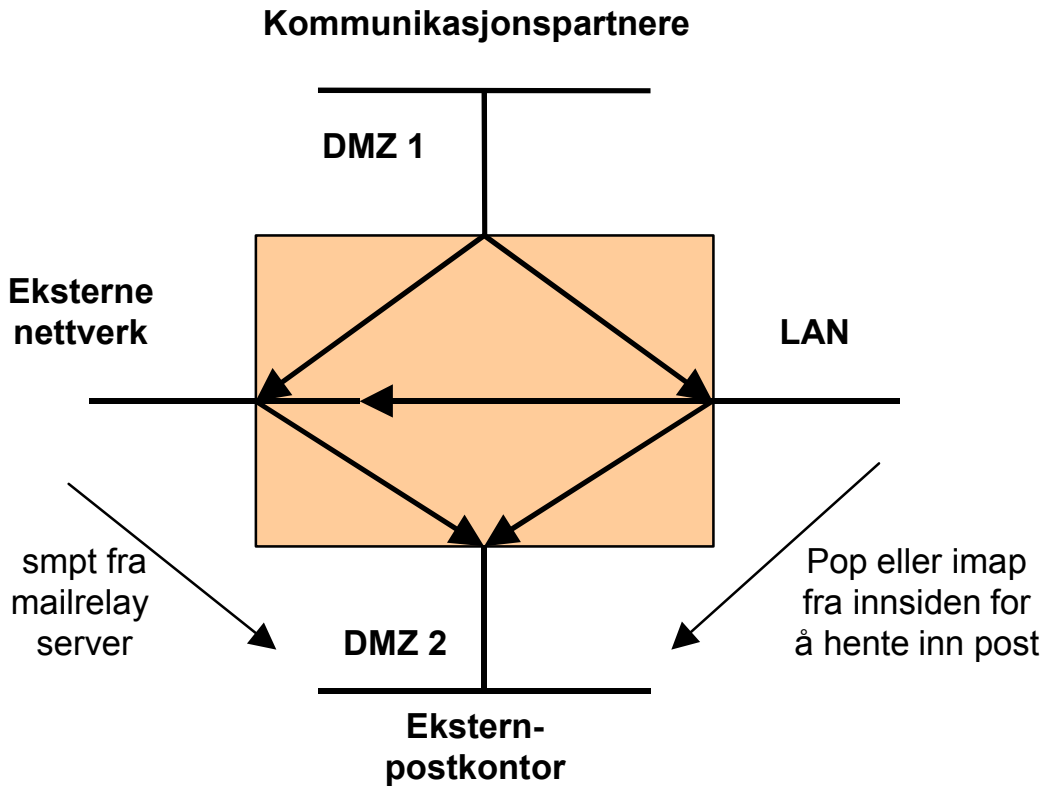
Dersom et avdelingskontor kun har behov for en sone, realiseres dette med den sonen det er behov for.

18.2.1 Sikkerhetsbarrierer

Tilgang fra sikret sone, hvor sensitive opplysninger behandles, til eksternt nettverk skal gå gjennom to sikkerhetsbarrierer.

En løsning hvor det er et fysisk skille mellom sikret sone og intern sone krever ingen ytterligere systemtekniske tiltak for å skille mellom sonene. For begrensning av tilgang til sensitive personopplysninger innen sikret sone, se avsnitt 18.2.2.

Konfigurering av sikkerhetsbarriere



FIGUR 4: **Anbefalt konfigurering av hvor informasjon og tjenester bør tillates gjennom sikkerhetsbarriere.**

Sikkerhetsbarrieren skal inneholde funksjoner for:

- nettverkskontroll; som regulerer informasjonsflyten mellom eksternt nettverk og virksomhetens ulike soner, herunder hvilke nettverks- og applikasjonsprotokoller som kan benyttes
- applikasjonskontroll; som muliggjør kontroll og begrensning på applikasjonsnivå med formål å:
  - verifisere at det er den tillatte tjenesten som faktisk benyttes
  - hindre at tjenesten benyttes for initiering av aktiviteter som ikke er tillatt og ikke er del av tjenesten selv
  - kontrollere og begrense funksjonaliteten i tjenestene etter behov
  - forhindre utnyttelse av kjente svakheter i tjenestene

  - kontrollere og filtrere ut komplekse datastrukturer slik at datadrevne angrep og tilstedeværelse av ødeleggende program hindres (f.eks. Active X komponenter, viruskontroll)
  - ivareta autentisering og autorisering av brukeren før tjenesten aktiveres
- redusere virkningen av "denial of service" angrep, dvs uautorisert utilgjengeliggjøring av tjenester.

Sikkerhetsbarrierer kan realiseres med bruk av brannmur, postkontor, viruskontroll mv. hvor funksjonalitet utføres fordelt på ulike komponenter slik at samlet sikkerhetsfunksjonalitet blir ivaretatt. Løsningen skal videre omfatte verktøy for analysering av registreringer. Løsningen skal ha et robust og strukturert brukergrensesnitt som gir enkel oversikt over oppsett og innstilling.

Sikkerhetsbarrieren skal generere alarmer når kritiske hendelser som indikerer mulige sikkerhetsbrudd inntreffer. Sikkerhetsrelevante hendelser skal registreres i et hendelsesregister, se kap. 23 for detaljer. Ansvar for oppfølging og implementering av nye versjoner av sikkerhetsoppdateringer må være entydig plassert.

18.2.2 Funksjonelle krav til indre sikkerhetsbarriere

Ved modellen for soneinndeling i figur 3 foran konfigureres indre sikkerhetsbarriere med følgende spesielle funksjonalitet:

- kun tillate tjenester initiert fra sikret sone til intern sone (stenging av FTP-trafikk fra intern til sikret sone)
- tjenester som ikke eksplisitt er tillatt er forbudt
- hver sikret sone etableres på et eget nettverkssegment
- tjenester kan tillates initiert mellom to sikrede soner (det kreves kryptering hvis disse sonene benytter eksterne forbindelser for datakommunikasjon)
- kun bruk av Java og Active X med opphav anerkjent av virksomheten
- det gis ikke tilgang til Internett-tjenester når bruker er innlogget på sikret sone
- e-post som inneholder sensitive personopplysninger må hentes inn til sikret sone ved hjelp av POP, IMAP eller lignende og virus sjekkes på sikret sone.
- ekstern overføring av sensitive personopplysninger krever kryptering fra sikret sone i en virksomhet til tilsvarende sikret sone hos annen virksomhet
- oppdatering av sikkerhetspatcher
- brukerprofil i sikkerhetsbarriere
- autentisering av brukere i sikkerhetsbarrieren.

18.2.3 Funksjonelle krav til ytre sikkerhetsbarriere

Ved løsning som er skissert i figur 3 foran benyttes ytre sikkerhetsbarriere med følgende spesielle funksjonalitet (se generell konfigurering av sikkerhetsbarriere foran):

- ingen trafikk tillates initiert fra eksterne nettverk og direkte inn på virksomhetens interne nettverk.
- tjenester som ikke eksplisitt er tillatt er forbudt
- autentisering av brukere i sikkerhetsbarrieren
- brukerprofil i sikkerhetsbarriere
- "Network Address Translation" (NAT) benyttes så sikkerhetsbarrieren på denne måten skjuler ressursene på innsiden overfor det eksterne datanettet
- kun bruk av Java og Active X med opphav anerkjent av virksomheten
- oppdatering av sikkerhetspatcher

- ekstern e-post skal mottas via DMZ på følgende måte, se figur 5 (DMZ 2)
  - smtp fra mail-relay server og til mail-server
  - pop, IMAP eller tilsvarende fra innsiden og inn på intern mail-server på henholdsvis sikker og intern sone
- hvis ekstern Web-server installeres på innsiden av virksomhetens informasjonssystem, må dette implementeres som beskrevet i 18.4.1
- kjente eksterne innringte forbindelser må implementeres som vist i figur 5.

18.2.4 Tilgang til sensitive personopplysninger

For å kunne begrense tilgang til de sensitive personopplysninger når man er inne på sikret sone legges følgende begrensninger og kontroller med tilgang til informasjon og applikasjoner på sikret sone:

- Tilgang til alle tjenester og informasjon er i utgangspunktet sperret.
- Tilgangskontrollen skal benytte individuelle passord og skal sørge for at brukere kun autoriseres for tilgang til informasjon og tjenester etter tjenstlige behov.
- Virksomheten skal angi krav til minimum lengde, sammensetning og varighet av passord.
- Virksomheten skal angi krav til maksimalt tillatt tidsrom uten aktivitet fra en bruker før det kreves ny autentisering.
- Sperring av brukerkonti som ikke har vært benyttet de siste to mnd, alternativt når passord skulle ha vært skiftet.
- Sikkerhetsrelevante hendelser skal registreres i hendelsesregister, se kap. 23 for detaljer for
  - krav til hvilke hendelser og hva som skal registreres
  - automatisk og manuell håndtering av hendelsesregister
  - ansvarlig for gjennomgang av hendelsesregister.

En løsning med fysisk skille mellom sikret sone og intern sone krever bare innføring av tilgangskontroller som nevnt over.

For løsninger med nettverksforbindelse gjelder i tillegg følgende:

- Det må benyttes et operativsystem eller 3. part sikkerhetsløsning som tilfredsstillende skiller mellom brukeres rettigheter til henholdsvis intern og sikret sone. Dette må skille mellom brukere/brukergruppers (identitet/passord) rettigheter til filsystem/nettverksressurser.
- Brukere i sikret sone må konfigureres med to alternative brukerprofiler hvis tilgang til eksterne nettverk skal gis til disse brukerne. De to brukerprofilene kan ha følgende tilgjengelige tjenester:
  - kun tilgang til tjenester og informasjon i sikret sone
  - tilgang til tjenester og informasjon i eksterne nettverk, inkludert eventuell tilgang til intern sone.
- Teknisk sikkerhetsløsning hos bruker skal bidra til å hindre uautorisert utlevering av sensitive personopplysninger ved utilsiktet overføring av data mellom program, eksempelvis ved bruk av "klipp og lim"-funksjon
- Dersom det skal lagres sensitive personopplysninger på utstyr som bringes ut av sikker sone, skal harddisken på disse maskinene automatisk krypteres.
- Hvis bruker i sikret sone også skal ha tilgang til tjenester på det intern sone eller eksterne tjenester, må det ikke være mulig å lagre ukrypterte sensitive

personopplysninger lokalt på arbeidsstasjonen. (Forutsetninger for ekstern overføring av sensitive personopplysninger, se kap. 18.3.2.).

18.3 Datakommunikasjon

18.3.1 Intern datakommunikasjon

Intern datakommunikasjon kan kun skje via medier som virksomheten har fysisk kontroll med. Dette omfatter datakommunikasjon innenfor virksomhetens bygninger og områder hvor virksomheten har kontroll. I utgangspunktet kan sensitive personopplysninger overføres innen sikrede soner, mens annen informasjon kan overføres på virksomhetens interne nettverk.

18.3.2 Ekstern datakommunikasjon

Ekstern datakommunikasjon innebærer oversendelse av informasjon via media hvor virksomheten ikke har kontroll med tilgang til mediet. Dette omfatter også overføring til virksomhetens ulike avdelinger / kontorer på forskjellige steder. Ved bruk av f.eks. egen nedgravd fiber vil det i hvert tilfelle måtte vurderes om virksomheten har kontroll med denne.

Oversendelse av sensitive personopplysninger betinger følgende:

- Utveksling av sensitiv informasjon skal kun gjøres til tilsvarende sikrede soner, dvs virksomhetens andre sikrede soner, eller sikrede soner hos partnere.
- Ved overføring av sensitive personopplysninger og informasjon om sikring av slike skal data krypteres. Dette inkluderer kryptering av passord før oversendelse over eksterne forbindelser.
- Kryptering av data skal skje ende-til-ende mellom to sikrede soner, dvs at kryptering/dekryptering skjer i sikret sone.
- All post hentes inn av virksomheten slik at gjennomgående forbindelser ikke etableres, eksempelvis ved bruk av POP, IMAP eller lignende.

Kommunikasjon med eksterne parter og leverandører skal skje gjennom dedikerte tilkoplinger, som i DMZ eller ved bruk av VPN, slik at disse ikke kan misbrukes.

Den ytre sikkerhetsbarrieren vil hindre all tilgang til virksomhetens interne nettverk. Det vil derfor ikke være mulig å foreta selvstendig initiering fra eksterne nettverk for uthenting av sensitive personopplysninger. Mellom kjente parter hvor det er avtalt prosedyrer og realisert nødvendige tekniske løsninger kan utveksling av sensitive personopplysninger etter anmodning fra utsiden av virksomheten skje på følgende måte:

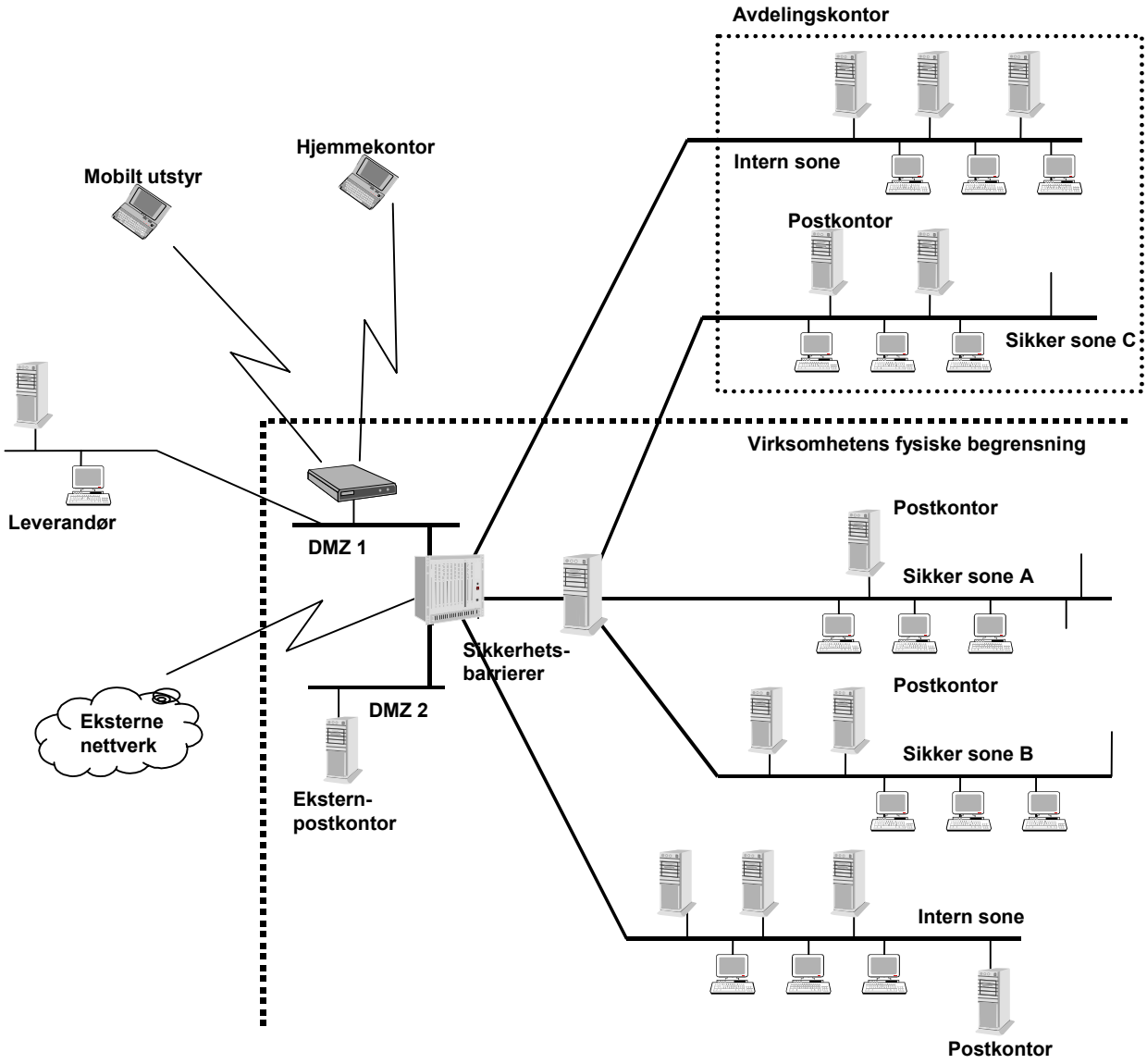
- Kryptert henvendelse som inneholder nødvendige autentiseringsdata og forespørsel om informasjon legges i virksomhetens postkontor på DMZ ("ekstern-postkontor").
- Henvendelsen hentes inn til sikret sone hvor den dekrypteres og verifiseres.
- Som respons på denne meldingen kan aktuell informasjon sendes tilbake kryptert.

18.4 Eksempler på tilgangs- og overføringssikkerhet

Her beskrives en løsning hvor sikkerhetsbarrierene består av to brannmurer. Det vil i den enkelte virksomhet være svært varierende behov for funksjonalitet og derfor ulike

sikkerhetsløsninger, uten at det er valgt å dokumentere disse i denne veiledningen. For eksempel kan brannmurer være unødvendige ved fysisk isolerte nettverk.

18.4.1 Soneinndeling ved bruk av brannmur



FIGUR 5: **Soneinndeling med bruk av 2 nivåer med brannmur**

Dette eksempelet er ikke ment å inkludere alt utstyr som er nødvendig i en løsning. Den gir en skisse av hvordan arkitekturen bør bygges opp for å gi den nødvendige sikkerhet. Det vil være varierende behov for f.eks. rutere, hub'er eller tilsvarende enheter ved implementering av løsning. Termineringer i DMZ'er kan alternativt gjøres ved hjelp av VPN-teknologi.

Figuren skisserer en virksomhet som har samlet behandling av sensitive personopplysninger innenfor et fysisk kontrollert område (betegnet som hovedkontor). Den stiplede linjen indikerer hva som er innenfor og utenfor hovedkontorets fysisk kontrollerte område. Hovedkontoret har ett internt nettverk med to sikrede soner hvor all behandling av sensitive personopplysninger legges. Det benyttes en brannmur mellom internt nettverk og de sikrede sonene. Krav til denne er beskrevet i kapittel 18.2.1.

I eksempelet er det forutsatt to nivåer av brannmurer, hvor den indre brannmuren kontrollerer

virksomhetens ulike soner, mens den ytre brannmuren kontrollerer alle øvrige eksterne forbindelser, inkludert mottak av ekstern E-post.

Tilgang mot eksterne forbindelser i figuren er kontrollert og begrenset via den ytre brannmuren. Denne brannmuren kontrollerer følgende soner og funksjoner:

- Tilgang til virksomhetens interne sone.
- Tilgang mot eksterne nettverk (f.eks. Internett).
- En demilitarisert sone (DMZ 1) for tilkopling og kontroll med kommunikasjonen mellom virksomhetens hovedkontor og eksterne forbindelser. Disse kan via DMZ 1 gis tilgang til internt nettverk. Siden DMZ 1 tillater ekstern tilgang fra kontrollerte eksterne forbindelser og inn i intern sone, må den ikke benyttes for tilgang mot Internett eller andre eksterne tjenester som ikke er underlagt virksomhetens sikkerhetsbestemmelser.
- En annen demilitarisert sone (DMZ 2) for mottak og formidling av ekstern E-post. Det frarådes å benytte denne for intern E-post. Dersom virksomheten selv ønsker å ha ansvar for Web-server som skal være åpen mot Internett, må den ligge i denne DMZ-sonen. Web-server kan selvsagt også legges utenfor virksomheten ved f.eks. å benytte såkalt Web-hotell. Det bør i så fall stilles samme krav til sikkerhet overfor leverandør av slik tjeneste som en ville gjort dersom Web-serveren lå under egen kontroll.

Hvor mange postkontorer som benyttes kan virksomheten i en viss grad velge selv. Der hvor sensitive personopplysninger skal mottas via E-post, må den aktuelle sikrede sone som skal motta E-posten ha et eget postkontor hvor denne posten blir dekryptert og sjekket for virus. I figuren er hver av de sikrede sonene gitt egne postkontor, mens det øvrige interne nettverk har felles postkontor.

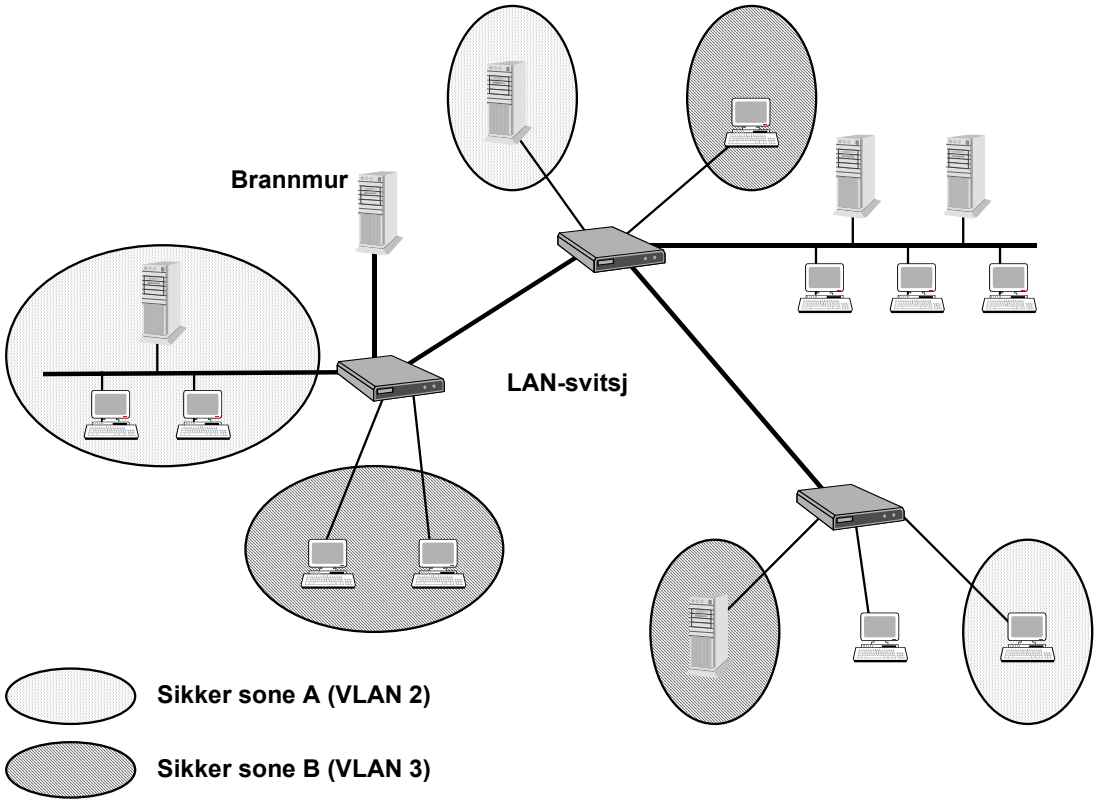
Lokalkontor
Virksomheten i eksempelet har et lokalkontor hvor den har tilsvarende fysisk kontroll som ved hovedkontoret. I denne løsningen er lokalkontorets sikrede sone kontrollert av samme brannmur som hovedkontorets sikrede sone, og det vil ikke være behov for å initiere noe fra intern sone inn mot den sikre sonen. Sikrede soner som tilknyttes den indre brannmuren, men som er lokalisert annet fysisk sted, må i tillegg ha kryptering ende til ende av forbindelsen.

Leverandører og hjemmekontor
Tilkobling hos virksomheten gjøres i eksempelet via DMZ 1. Tilkoblingen skal tilfredsstille følgende:

- Tilbakeringing og forhåndsdefinerte nummer, hvor det er virksomhetens maskin som bryter forbindelsen, eller
- bruk av VPN-løsning i kommunikasjonen, slik at forbindelsen kun tillates gjennom krypterte og sterkt autentiserte VPN-klienter.

18.4.2 Bruk av VLAN for nettverksinndeling

Det er også mulig å lage virtuelle LAN (VLAN) for å oppnå en deling av det interne nettet i sikrede soner. VLAN sammen med såkalte LAN-svitsjer og rutere, gir muligheten til å gruppere brukere i subnett uavhengig av nettverkets fysisk infrastruktur. Medlemmene i et VLAN vil kunne kommunisere som om de var tilkoblet samme LAN.



FIGUR 6: **Bruk av VLAN for å konfigurere sikkerhetssoner**

I et VLAN vil brukere og ressurser tilknyttet ulike LAN-svitsjer kunne tilhøre samme subnett, se Figur 6.

For å kunne kommunisere mellom VLAN, må rutingfunksjoner benyttes. Ruting kan både være implementert direkte i LAN-svitsjene eller håndtert med separate rutere. Figur 6 viser et eksempel der ruting er implementert i LAN-svitsjene.

Dette er ett alternativ for å dele en virksomhets informasjonssystem opp i flere VLAN, som ved å sikres kan danne sikre og interne soner. Ved å benytte brannmurer kan nettet deles opp i ulike sikkerhetssoner, der en gitt sikkerhetssone korresponderer til ett eller flere VLAN.

Ved bruk av denne teknologien for å oppnå sikkerhetssoner (se figur 6), må sikringen være like god som løsningen i Figur 5 med hensyn til:

- Hvordan ekstern kommunikasjon skal sikres og tillates. Prinsippene gitt i kapittel 18.1 og konfigurering av brannmur i kapittel 18.2.1 kan også benyttes ved bruk av VLAN.
- At uautoriserte ikke kan endre hvem som tilhører de ulike sikkerhetssoner. Dette innebærer å hindre følgende forsøk på uautorisert tilgang:

- Uautoriserte forsøk på å endre konfigurering av soner, dvs direkte angrep på tilgangskontroll-lister i rutere, brannmurer og annet som benyttes for å sikre soneinndelingen, dvs de ulike VLAN. Oppretting av et eget VLAN som en egen sikret sone for driftsfunksjoner og kun bruk av dedikert arbeidsplass for slike funksjoner kan benyttes for å oppnå nødvendig sikkerhet
- Uautoriserte forsøk på å gi seg ut for å tilhøre en annen sone enn den brukeren tilhører. For dette må det benyttes identifisering og autentisering på applikasjonsnivå for å verifisere hvem som utfører hver funksjon.

18.5 Ødeleggende program

Teknisk sikkerhetsbarrierer skal gjøre det mulig å hindre utførelse av program som automatisk overføres fra eksternt datanett, eksempelvis Active X og Java komponenter.

Det skal gjøres oppdateringer av de siste sikkerhetspatcher for brannmur og operativsystem og sikkerhetsbarrieren skal være motstandsdyktig mot "Denial of Service" angrep.

Virksomhetens sikkerhetstiltak omfatter også følgende sikring mot ødeleggende programmer:

- virussjekk av alle innkommende filer, inkludert pakkede filer
- gjennomføring av automatisk virussjekking ved bruk av flyttbare lagringsmedie
- ved mottak av krypterte filer inn i sikker sone, må disse filene virus sjekkes etter at de er pakket ut før de formidles til bruker.

18.6 Sletting

Sletting av sensitive personopplysninger er aktuelt både som følge av lovpålagte bestemmelser, ved gjenbruk av elektroniske lagringsmedier og i forbindelse med utrangering av utstyr. Ved utrangering / avhending av utstyr vil det være et særlig behov for å slette tidligere innhold, slik at ikke sensitive personopplysninger på denne måten kommer uvedkommende i hende.

Virksomheten må kunne ha tilfredsstillende rutiner for sletting/makulering av:

- disketter, tape, bånd, CD, DVD og annet flyttbart lagringsmedie
- harddisker/maskiner som sendes til reparasjon
- utrangerte/ødelagte harddisker
- utrangerte/ødelagte maskiner (PC, tjenermaskiner)
- papirbaserte dokumenter

Det skal innføres en rutine for merking av medier som inneholder sensitive personopplysninger, slik at virksomheten kan være trygg på at medier med slik informasjon ikke kommer uvedkommende i hende.

19 Dokumentsikkerhet

Begrepet dokumenter omfatter i denne sammenheng så vel papirutskrifter som datafiler på elektroniske lagringsmedia som disketter, CD-plater, harddisker etc. Dokumenter som inneholder sensitive personopplysninger eller informasjon om sikring av slike

opplysninger skal behandles slik at:

det ved intern og ekstern forsendelse av slike dokumenter:

- bare er personer som har tjenstlig behov for tilgang til opplysningene som mottar slike dokumenter
- er mulig å oppdage uautorisert utlevering eller forsøk på slik utlevering, eksempelvis ved emballering/forsegling av dokumentet. Dette gjelder også ved bruk av virksomhetens interne postsystem, hvor flere enn den autoriserte kan ha tilgang.

det ved oppbevaring av dokumenter med sensitive personopplysninger:

- tydelig fremgår av dokument at det inneholder sensitive opplysninger
- det er ivaretatt fysisk sikring når det ikke er under tilsyn av autorisert personell
- at utskrifter inneholdende sensitive personopplysninger ikke blir liggende på skriver eller lignende på utskriftssteder som kan være tilgjengelig for uautorisert personell.

Regler for sletting som beskrevet over omfatter også makulering av dokumenter som inneholder sensitive personopplysninger.

Del VI Dokumentasjon

20 Dokumentasjonskontroll

Dokumentasjon skal utarbeides og distribueres i henhold til rutine for dokumentasjonskontroll. Formålet med dokumentasjonskontrollen er å sikre at alle dokumenter er resultat av en ansvarlig beslutning, at de er korrekt utformet og kjent av virksomhetens ansatte i den grad dette er nødvendig for å utføre pålagte oppgaver.

Utarbeidelse av dokumentasjon av dokumenter skal gjennomføres slik at:

- det fastlegges hvem som er ansvarlig for utforming av dokumentet, herunder ansvar og myndighet for godkjenning av endrede og nye dokumenter
- formålet med dokumentet beskrives
- dokumentet gis en entydig identifikasjon (navn, versjon og dato)
- det eksisterer retningslinjer for dokumentutforming
- det gis beskrivelse av media (elektronisk, papir) og arkivering av dokumentet
- det fremgår hvem dokumentet skal distribueres til
- dette settes i verk for nye og endrede dokumenter.

21 Styrende dokumenter

Følgende styrende dokumenter skal utarbeides og distribueres i henhold til rutine for dokumentasjonskontroll:

- sikkerhetsmål
- sikkerhetsstrategi
- oversikt og klassifisering av personopplysinger
- informasjon om ansvars- og myndighetsforhold, organisasjonskart
- konfigurasjonskart med informasjon om teknisk sikkerhetsløsning
- informasjon om partnere og leverandører

Stillingsbeskrivelser skal utarbeides og distribueres i henhold til denne rutinen i den grad det er nødvendig for å få en tilfredsstillende informasjonssikkerhet. Strategiske planer bør også inngå som styrende dokumenter.

22 Prosedyrer

Prosedyrer av betydning for informasjonssikkerheten skal utarbeides og distribueres i henhold til rutine for dokumentasjonskontroll. Dette gjelder spesielt rutiner for:

- risikovurdering
- sikkerhetsrevisjon
- ledelsens gjennomgang
- konfigurasjonsendring
- beredskapsplaner
- avviksbehandling
- adgangskontroll
- tilgangskontroll
- datakommunikasjon
- dokumentsikkerhet.

23 Registreringer

Resultater fra arbeidet med informasjonssystemet skal registreres i den utstrekning det er nødvendig for å oppnå tilfredsstillende informasjonssikkerhet.

Følgende registreringer skal lagres i 5 år:

- resultater fra ledelsens gjennomgang, risikovurderinger, sikkerhetsrevisjoner og avviksbehandling
- oversikt over områder og utstyr med adgangskontroll
- oversikt over soner, data og program med tilgangskontroll
- autorisering av brukere
- tidligere utgaver av godkjente tekniske og administrative prosedyrer.

Hendelsesregistrering (aktivitetslogg) omfatter områdene adgang, tilgang og datakommunikasjon samt forsøk på uautorisert bruk. Disse skal lagres i 3 måneder. Hensikten med registreringene er sporbarhet på utført behandling. I sammenheng med informasjonssikkerhet vil slik registrering være et viktig hjelpemiddel for å avdekke og oppklare brudd på sikkerheten. Det skal etableres rutiner for gjennomgang av hendelsesregistre. Hendelser av betydning for informasjonssikkerheten skal behandles i henhold til prosedyre for avviksbehandling.

Bruk av logger begrenses til å benyttes i sikring og administrasjon av informasjonssystemet. Annen bruk av logger, eksempelvis oppfølging av de ansattes arbeidsinnsats, må ha et særskilt hjemmelsgrunnlag.

For internt informasjonssystem anbefales registrering av følgende i en aktivitetslogg:

- innlogging/utlogging
- aktivitet på brukerkonti utenfor arbeidstid
- store utskriftsjobber
- store filoverføringer
- filtilgang på andre enn egne kataloger
- endringer av brukerprivilegier og passord
- omstart
- forsøk på å endre registreringer eller det som skal registreres.

For tekniske sikkerhetsløsninger som f.eks. brannmur anbefales registrering av følgende:

- eksterne anrop til nettverksadresser i virksomhetens informasjonssystemer
- adresser i det eksterne datanettet som det kommuniseres med
- forsøk på å oppheve sperrer eller begrensninger som håndheves av brannmur
- endring av sikkerhetskonfigurering av brannmur
- omstart
- forsøk på å endre registreringer eller det som skal registreres

Når det gjelder elektroniske hendelser bør følgende parameter registreres i hendelsesregisteret:

- brukernavn
- tidspunkt
- terminal
- type hendelse
- resultat (vellykket, ikke vellykket).

Det skal utarbeides rutine for gjennomgang av hendelsesregistre som omfatter:

- hvem som skal ha ansvar for å gjennomgå registreringene
- hvor hyppig registreringene skal gjennomgås
- beskrivelse av "unormale" aktivitetsmønstre som bør undersøkes
- hvordan etterkontroll av "unormale" aktivitetsmønstre bør foretas
- hvordan eventuelle sikkerhetsbrudd eller mistanke om slikt skal følges opp
- hvem som har ansvar for sletting av registreringer ved lagringstidens utløp.