

ICS 35.040

Søkeord: informasjonsteknologi, informasjonssikkerhet, sikkerhet, sikkerhetsarbeid, programvare, informasjonssystem, sikkerhetsstandard, informasjonssikring, datasikkerhet

Descriptors: information technology, information security, security, security management, software, information system, security standard, information security, data security

Informasjonsteknologi Administrasjon av informasjonssikkerhet (ISO/IEC 17799:2000)

Information technology
Code of practice for information security management
(ISO/IEC 17799:2000)

Norsk versjon

Standarden er fastsatt av Norges Standardiseringsforbund (NSF). Den kan bestilles fra Pronorm AS, som også gir opplysninger om andre norske og utenlandske standarder.

Postboks 432 Skøyen, 0213 OSLO
Telefon: 22 04 92 30 Telefaks: 22 04 92 12

Norsk Teknologisenter (NTS) er faglig ansvarlig for standarden og kan gi opplysninger om saksinnholdet.

Postboks 7072 Majorstua, 0306 OSLO
Telefon: 22 59 01 00 Telefax: 22 59 01 33

Nasjonalt forord

Den norskspråklige versjonen av internasjonal standard ISO/IEC 17799:2000 ble fastsatt som Norsk Standard NS-ISO/IEC 17799:2001 i mai 2001.

Den internasjonale standarden ISO/IEC 17999 ble utarbeidet av den britiske standardiseringsorganisasjonen, BSI, som BS 7799:1999 del 1 og ble godkjent under den spesielle "Fast Track Procedure" av felles teknisk komite ISO/IEC JTC 1, Informasjonsteknologi, parallelt med at den ble godkjent av nasjonale standardiseringsorganisasjoner.

National foreword

The Norwegian translation of International Standard ISO/IEC 17799:2000 has been adopted as Norwegian Standard NS-ISO/IEC 17799:2001 in May 2000.

This International Standard ISO/IEC 17799 was prepared by the British Standards Institution, as BS 7799:1999 Part 1 and was adopted under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, Information technology, in parallel with its approval by national bodies of ISO and IEC.

Informasjonsteknologi – Administrasjon av informasjonssikkerhet (ISO/IEC 17799:2000)

Innhold

Orientering	6
1 Omfang.....	9
2 Termer og definisjoner	9
2.1 Informasjonssikkerhet	9
2.2 Risikovurdering	9
2.3 Risikostyring	9
3 Sikkerhetspolitikk	9
3.1 Retningslinjer for informasjonssikkerhet	9
3.1.1 Dokumentasjon av informasjonssikkerhetspolitikken	9
3.1.2 Revisjon og evaluering av retningslinjer basert på denne standarden	10
4 Sikkerhetsarbeid i organisasjonen.....	10
4.1 Rammeverk for informasjonssikkerhet	10
4.1.1 Ledelsens informasjonssikkerhetsforum.....	10
4.1.2 Koordinering av informasjonssikkerhet.....	11
4.1.3 Tildeling av ansvar for informasjonssikkerhet.....	11
4.1.4 Godkjenning av utstyr til informasjonsbehandling.....	12
4.1.5 Sikkerhetsanbefalinger fra spesialister	12
4.1.6 Samarbeid mellom organisasjoner.....	12
4.1.7 Uavhengig vurdering av informasjonssikkerheten	12
4.2 Sikkerhet i forhold til tredjepart	13
4.2.1 Identifisering av risikoer forbundet med tredjeparts tilgang og adgang	13
4.2.2 Sikkerhetsbetingelser for kontrakter med tredjeparter.....	14
4.3 Outsourcing	15
4.3.1 Krav til sikkerhet i outsourcingkontrakter.....	15
5 Klassifisering og sikring av aktiva	15
5.1 Ansvar for aktiva	15
5.1.1 Oversikt over aktiva.....	15

5.2	Klassifisering av informasjon	16
5.2.1	Retningslinjer for klassifisering	16
5.2.2	Merking og håndtering av informasjon	16
6	Personellsikkerhet	17
6.1	Sikkerhet i arbeidsbeskrivelse og personellutvelgelse	17
6.1.1	Sikkerhet i arbeidsbeskrivelse	17
6.1.2	Personellutvelgelse og -politikk	17
6.1.3	Taushetserklæring	18
6.1.4	Betingelser og ansettelsesvilkår	18
6.2	Brukeropplæring	18
6.2.1	Utdanning og opplæring i informasjonssikkerhet	18
6.3	Håndtering av sikkerhetshendelser og funksjonssvikt	18
6.3.1	Rapportering av sikkerhetshendelser	19
6.3.2	Rapportering av sikkerhetsmessige svakheter	19
6.3.3	Rapportering av funksjonsfeil i programvare	19
6.3.4	Lærdommer av sikkerhetshendelser	19
6.3.5	Disiplinære reaksjoner	19
7	Fysisk og miljømessig sikkerhet	20
7.1	Sikre områder	20
7.1.1	Fysisk sikkerhetssone	20
7.1.2	Fysisk adgangskontroll	20
7.1.3	Sikring av kontorer, rom og utstyr	21
7.1.4	Retningslinjer for arbeid i sikre områder	21
7.1.5	Isolert område for vareleveranser	22
7.2	Sikring av utstyr	22
7.2.1	Plassering og beskyttelse av informasjonssystem	22
7.2.2	Strømforsyning	23
7.2.3	Sikring av kabling	23
7.2.4	Vedlikehold av utstyr	23
7.2.5	Sikkerhet for eksternt plassert utstyr	24
7.2.6	Sikker avhending eller gjenbruk av utstyr	24
7.3	Generelle sikringstiltak	24
7.3.1	Retningslinjer for rydding av arbeidsplass	24
7.3.2	Fjerning av organisasjonens eiendeler	25
8	Kommunikasjons- og driftsadministrasjon	25
8.1	Driftsprosedyrer og ansvarsforhold	25
8.1.1	Dokumenterte driftsprosedyrer	25

8.1.2	Driftsmessig endringskontroll.....	26
8.1.3	Prosedyrer for håndtering av hendelser	26
8.1.4	Arbeidsdeling.....	27
8.1.5	Atskillelse av utviklings- og produksjonsutstyr.....	27
8.1.6	Administrasjon utført av eksterne.....	27
8.2	Systemplanlegging og akseptanse	28
8.2.1	Kapasitetsplanlegging	28
8.2.2	Systemakseptanse	28
8.3	Beskyttelse mot ødeleggende programvare.....	29
8.3.1	Viruskontroll.....	29
8.4	Administrative rutiner	30
8.4.1	Sikkerhetskopiering av data.....	30
8.4.2	Operatørlogger.....	30
8.4.3	Feillogging.....	30
8.5	Nettverksadministrasjon.....	31
8.5.1	Sikringstiltak i nettverk.....	31
8.6	Sikker håndtering av datamedia	31
8.6.1	Håndtering av flyttbare datamedia.....	31
8.6.2	Makulering av datamedia.....	31
8.6.3	Prosedyrer for håndtering av informasjon	32
8.6.4	Sikring av systemdokumentasjon	32
8.7	Utveksling av informasjon og programvare.....	33
8.7.1	Utvekslingsavtaler for data og programvare.....	33
8.7.2	Sikring av informasjon i transitt	33
8.7.3	Sikkerhet ved elektronisk handel.....	33
8.7.4	Sikkerhet ved bruk av elektronisk post.....	34
8.7.5	Sikring av elektroniske kontorsystemer.....	35
8.7.6	Offentlig tilgjengelige systemer.....	35
8.7.7	Andre former for utveksling av informasjon	36
9	Tilgangskontroll.....	36
9.1	Virksomhetskrav til tilgangskontroll.....	36
9.1.1	Retningslinjer for tilgangskontroll.....	37
9.2	Administrasjon av brukertilgang	37
9.2.1	Registrering av brukere.....	37
9.2.2	Administrasjon av rettigheter.....	38
9.2.3	Administrasjon av brukerpassord	38
9.2.4	Gjennomgang av brukers tilgangsrettigheter.....	39

9.3	Brukerens ansvar	39
9.3.1	Bruk av passord.....	39
9.3.2	Ubevoktet brukerstyr	40
9.4	Tilgangskontroll i nettverk	40
9.4.1	Retningslinjer for bruk av nettverkstjenester	40
9.4.2	Tvungen kommunikasjonsvei	40
9.4.3	Brukerautentisering av eksterne forbindelser.....	41
9.4.4	Nodeautentisering	41
9.4.5	Beskyttelse av porter for fjerndiagnose.....	42
9.4.6	Segmentering av nettverk.....	42
9.4.7	Kontroll av oppkobling i nettverk	42
9.4.8	Sikring av nettverksruting.....	42
9.4.9	Sikring av nettverkstjenester	43
9.5	Tilgangskontroll for informasjonssystemene.....	43
9.5.1	Automatisk identifisering av terminal.....	43
9.5.2	Påloggingsprosedyre	43
9.5.3	Brukeridentitet og autentisering	44
9.5.4	System for passordadministrasjon	44
9.5.5	Bruk av hjelpeprogrammer	45
9.5.6	Tvangsalarm for å sikre brukerne	45
9.5.7	Avstengning av terminal	45
9.5.8	Begrensninger på oppkoblingstidspunkt	45
9.6	Tilgangskontroll for program	45
9.6.1	Begrensning av tilgang til informasjon.....	46
9.6.2	Isolering av sensitive informasjonssystemer.....	46
9.7	Overvåkning av systemtilgang og bruk	46
9.7.1	Logging av hendelser	46
9.7.2	Overvåkning av systembruk.....	47
9.7.3	Synkronisering av klokker	48
9.8	Bruk av bærbart datautstyr og hjemmearbeid.....	48
9.8.1	Bruk av bærbart datautstyr.....	48
9.8.2	Hjemmearbeid.....	49
10	Systemutvikling og vedlikehold	49
10.1	Informasjonssystemenes sikkerhetskrav	49
10.1.1	Analyse og spesifikasjon av sikkerhetskrav.....	49
10.2	Sikkerhet i applikasjonssystemene.....	50
10.2.1	Godkjenning av inndata	50

10.2.2	Kontroll av intern behandling	50
10.2.3	Meldingsautentisering.....	51
10.2.4	Godkjenning av utdata	51
10.3	Kryptografisk kontroll	52
10.3.1	Retningslinjer for bruk av kryptografisk kontroll	52
10.3.2	Kryptering	52
10.3.3	Digitale signaturer.....	52
10.3.4	Ikke-benektelse	53
10.3.5	Administrasjon av kryptografiske nøkler.....	53
10.4	Sikring av systemfiler	54
10.4.1	Kontroll av produksjonsprogramvare	55
10.4.2	Beskyttelse av testdata	55
10.4.3	Tilgangskontroll til bibliotekene for kildekode	55
10.5	Sikkerhet i utviklings- og vedlikeholdsprosesser.....	56
10.5.1	Prosedyrer for endringskontroll	56
10.5.2	Teknisk gjennomgang av endringer i produksjonssystem	56
10.5.3	Begrensninger på endringer av programvarepakker	57
10.5.4	Bakdører og trojanske koder	57
10.5.5	Outsourcing av programvareutvikling	57
11	Kontinuitetsplanlegging	58
11.1	Aspekter ved kontinuitetsplanlegging.....	58
11.1.1	Kontinuitetsplanleggingsprosessen.....	58
11.1.2	Kontinuitets- og konsekvensanalyse.....	58
11.1.3	Utforming og implementering av kontinuitetsplanene	59
11.1.4	Rammeverk for kontinuitetsplanlegging.....	59
11.1.5	Prøving, vedlikehold og revisjon av kontinuitetsplanleggingen	60
12	Overensstemmelse.....	61
12.1	Overensstemmelse med juridiske krav	61
12.1.1	Identifisering av relevant lovgivning	61
12.1.2	Intellektuell eiendomsrett (IPR - Intellectual Property Rights)	61
12.1.3	Beskyttelse av organisasjonens lagrede informasjon.....	62
12.1.4	Sikring av data og beskyttelse av personopplysninger	62
12.1.5	Sikringstiltak mot misbruk av informasjonssystemene	62
12.1.6	Regulering av kryptografisk kontroll.....	63
12.1.7	Innsamling av bevis	63
12.2	Gjennomgang av sikkerhetspolitikk og samsvar med tekniske krav	64
12.2.1	Samsvar med sikkerhetspolicy.....	64

12.2.2	Samsvar med tekniske krav.....	64
12.3	Hensyn ved systemrevisjon.....	65
12.3.1	Revisjonskontroller.....	65
12.3.2	Beskyttelse av revisjonsverktøy.....	65

Orientering

Hva er informasjonssikkerhet?

Informasjon er et aktivum som, i likhet med andre viktige virksomhetsaktiva, har verdi for en organisasjon og derfor må vernes på forsvarlig måte. Informasjonssikkerhet beskytter informasjon mot en lang rekke trusler med det formål å sikre driftskontinuitet, redusere skader og maksimere utbyttet av investeringer og forretningsmuligheter.

Informasjon kan eksistere i mange former. Den kan trykkes eller skrives på papir, lagres elektronisk, overføres via post eller elektroniske media, vises på film eller formidles muntlig. Uansett hvilken form informasjonen har eller hvilket middel den formidles gjennom og lagres på, bør den alltid beskyttes på forsvarlig måte.

Informasjonssikkerhet omfatter her beskyttelse av:

- a) konfidensialitet: at informasjon bare er tilgjengelig for dem som har autorisert tilgang til den;
- b) integritet: nøyaktig og fullstendig informasjon og behandlingsprosesser;
- c) tilgjengelighet: at autoriserte brukere har tilgang til informasjon og tilhørende tjenester når de trenger dem.

Informasjonssikkerhet oppnås ved å iverksette passende kontrolltiltak, som kan være politikk, rutiner, prosedyrer, organisasjonsstrukturer og programvarefunksjoner. Disse tiltakene må etableres for å sikre at organisasjonens spesielle sikkerhetsmål oppfylles.

Hvorfor informasjonssikkerhet er nødvendig

Informasjon og støttefunksjoner, systemer og nettverk er viktige virksomhetsaktiva. Konfidensialitet, integritet og tilgjengelighet kan være avgjørende for å opprettholde konkurransefortrinn, pengestrøm, lønnsomhet, overholdelse av lovlighet og organisasjonens offentlige omdømme.

I stadig større grad står organisasjoner og deres informasjonssystemer overfor en rekke sikkerhetstrusler, for eksempel datasvindel, spionasje, sabotasje, hærverk, brann eller flom. Skadelige aktiviteter, slik som spredning av datavirus, datakriminalitet og tjenesteblokkering, er blitt mer omfattende, ambisiøse og stadig mer sofistikerte.

Avhengighet av informasjonssystemer og tjenester innebærer at organisasjoner blir mer sårbare for sikkerhetstrusler. Sammenkobling av offentlige og private nettverk og deling av informasjonsressurser gjør det stadig vanskeligere å sikre tilgangskontroll. Tendensen i retning av distribuert databehandling har redusert muligheten for sentralisert spesialistkontroll.

Mange informasjonssystemer er ikke utformet med sikkerhet for øyet. Sikkerheten som kan oppnås med tekniske virkemidler, er begrenset og bør suppleres med passende styring og prosedyrer. Det krever omhyggelig planlegging og blikk for detaljer å avgjøre hvilke sikringstiltak som skal etableres. Håndtering av informasjonssikkerhet krever deltakelse av alle ansatte i organisasjonen. Det kan også forutsette deltakelse fra leverandører, kunder eller andre interessenter. I noen tilfeller vil det være nødvendig å innhente råd fra utenforstående organisasjoner.

Sikringstiltak blir betydelig billigere og mer effektive dersom de innarbeides i forbindelse med kravspesifisering og i utformingsfasen.

Hvordan etablere krav til sikkerhet?

Det er helt avgjørende at en organisasjon definerer sine krav til sikkerhet. Det finnes tre hovedkilder:

Den første kilden er en vurdering av risikoen organisasjonen står overfor. Gjennom en slik risikovurdering identifiserer man mulige trusler mot organisasjonen, man vurderer sårbarhet og sannsynlighet for at noe skal inntreffe og anslår det potensielle skadeomfanget.

Den andre kilden er de juridiske, lovmessige og avtalefestede krav som en organisasjon, dens handelspartnere, kontraktører og tjenesteleverandører må tilfredsstille.

Den tredje kilden er de bestemte prinsippene, målene og kravene til informasjonsbehandling som organisasjonen har utviklet for å støtte sin forretningsdrift.

Vurdering av sikkerhetsrisiko

Krav til sikkerhet fastsettes gjennom en metodisk vurdering av sikkerhetsrisikoen. Ressursene man bruker på sikring, må veies mot de sannsynlige skadene ved sikkerhetssvikt. Teknikker for risikovurdering kan anvendes på hele eller deler av organisasjonen, så vel som på individuelle informasjonssystemer, spesifikke systemkomponenter eller tjenester der dette er mulig, realistisk og hensiktsmessig.

En risikovurdering er en systematisk gjennomgang av:

- a) sannsynlige skader for organisasjonen som følge av sikkerhetssvikt, når man tar hensyn til de potensielle følgene av tap av konfidensialitet, integritet eller tilgang på informasjon og andre aktiva;
- b) den realistiske sannsynligheten for at en slik svikt skal forekomme i lys av eksisterende trusler og svakheter, og kontrolltiltakene som allerede er etablert.

Resultatet av denne vurderingen vil bidra til å styre og avgjøre ledelsens tiltak og prioriteringer for å håndtere trusler mot informasjonssikkerheten, og for å gjennomføre sikringstiltakene som er valgt for å beskytte mot disse truslene. Prosessen med risikovurdering og valg av sikringstiltak må kanskje gjøres flere ganger for å dekke ulike deler av organisasjonen eller enkeltstående informasjonssystemer.

Periodisk gjennomgang av sikkerhetsrisikoer og iverksatte sikringstiltak er viktig for å:

- a) ta hensyn til endrede virksomhetskrav og prioriteringer;
- b) vurdere nye trusler og svakheter
- c) bekrefte at tiltakene fremdeles er effektive og hensiktsmessige.

Gjennomgangen bør foretas på ulike dybdenivå, avhengig av resultatene av foregående gjennomganger og de endrede risikonivåene som ledelsen er innstilt på å akseptere. Risikovurdering blir ofte gjennomført først på et høyt nivå for å prioritere ressurser i høyrisikoområder, og senere på et mer detaljert nivå, for å identifisere og analysere konkrete trusler.

Valg av sikringstiltak

Når kravene til sikkerhet er fastsatt, bør tiltakene velges og iverksettes for å sikre at risikoen reduseres til et akseptabelt nivå. Sikringstiltakene kan velges fra denne standarden eller fra andre sett med dokumenterte tiltak, eller det kan utformes nye hensiktsmessige tiltak ved behov. Det er mange ulike måter å håndtere risiko på, og denne standarden gir eksempler på vanlige metoder. Det er imidlertid viktig å være klar over at ikke alle sikringstiltak kan anvendes på alle informasjonssystemer eller –miljøer, og enkelte av tiltakene er kanskje ikke mulig å gjennomføre for alle organisasjoner. For eksempel beskriver 8.1.4 hvordan arbeidsdeling bør innføres for å motvirke svindel og feil. Det er kanskje ikke mulig for mindre organisasjoner å dele opp alle oppgaver, og det kan derfor være nødvendig å velge andre metoder for å oppfylle de samme kontrollmålene. Beskrivelsen i 9.7 og 12.1 hvor overvåking av systemer og innsamling av bevis beskrives kan være punkter hvor standarden kan være i konflikt med norsk lovgivning. De beskrevne tiltakene, eksempelvis logging av hendelser, kan komme i konflikt med relevante lover, som eksempelvis personopplysningsloven og arbeidsmiljøloven.

Valg av sikringstiltak bør baseres på totalkostnadene målt opp mot den oppnådde risikoreduksjonen og de potensielle tapene dersom en sikkerhetssvikt skulle inntreffe. Ikke-økonomiske faktorer, slik som tap av offentlig omdømme, bør også være med i regnestykket.

Noen av sikringstiltakene i dette dokumentet kan anses som ledende prinsipper for administrasjon av informasjonssikkerhet og bør anvendes i de fleste organisasjoner. De står forklart mer utførlig under overskriften ”Utgangspunkt for informasjonssikkerhet.”

Utgangspunkt for informasjonssikkerhet

Noen av sikringstiltakene er å regne for ledende prinsipper som danner et godt utgangspunkt for iverksettelse av informasjonssikkerhet. De er enten basert på viktige, lovfestede krav, eller generelt ansett å være de beste rutineene for informasjonssikkerhet.

Tiltak som anses for å være essensielle for en organisasjon fra et juridisk perspektiv omfatter:

- a) beskyttelse av data og personinformasjon (se 12.1.4);
- b) sikring av organisasjonens lagrede informasjon (se 12.1.3);
- c) intellektuell eiendomsrett (se 12.1.2).

Tiltak som er generelt ansett for å være de beste rutineene for informasjonssikkerhet, omfatter:

- a) informasjonssikkerhetspolitikk (se 3.1.1);
- b) tildeling av ansvar for informasjonssikkerhet (se 4.1.3);
- c) utdanning og opplæring innenfor informasjonssikkerhet (se 6.2.1);
- d) rapportering av sikkerhetshendelser (se 6.3.1);
- e) kontinuitetsplanlegging (se 11.1).

Disse sikringstiltakene gjelder for de fleste organisasjoner og miljøer. Legg imidlertid merke til at selv om alle tiltakene i denne standarden er viktige, bør relevansen av de ulike tiltakene vurderes i lys av de konkrete risikofaktorene en organisasjon står overfor. Selv om tilnærmingen ovenfor anses å være et godt utgangspunkt, kan den altså ikke erstatte valg av kontrollrutiner på grunnlag av egen risikovurdering.

Kritiske suksessfaktorer

Erfaring har vist at følgende faktorer ofte er vesentlige for en vellykket iverksettelse av informasjonssikkerhet i en organisasjon:

- a) sikkerhetspolitikk, -mål og -aktiviteter som gjenspeiler virksomhetsmålene;
- b) en tilnærming til iverksettelse av sikkerhet som er i samsvar med organisasjonskulturen;
- c) synlig støtte og forpliktelse fra toppledelsen;
- d) god forståelse av sikkerhetskrav, risikovurdering og risikohåndtering;
- e) effektiv markedsføring av sikkerhet overfor alle ledere og ansatte;
- f) distribusjon av retningslinjer for informasjonssikkerhetspolitikk og -standarder til alle medarbeidere og leverandører;
- g) hensiktsmessig utdanning og opplæring;
- h) et detaljert og balansert system av mål for å evaluere administrasjon av informasjonssikkerhet samt tilbakemeldinger med forslag til forbedringer.

Utvikling av egne retningslinjer

Denne standarden er å betrakte som et utgangspunkt for å utvikle informasjonsspesifikke retningslinjer. Kanskje er ikke alle anbefalingene og tiltakene i denne standarden relevante. Dessuten kan det være behov for ytterligere tiltak som ikke er behandlet i denne standarden. I slike tilfeller kan det være nyttig å beholde kryssreferanser som gjør det lettere for revisorer og samarbeidende virksomheter å undersøke om standarden blir fulgt.

1 Omfang

Denne standarden gir anbefalinger for administrasjon av informasjonssikkerhet til bruk for dem som er ansvarlige for å opprette, iverksette eller opprettholde sikkerhetsarbeidet i organisasjonen. Den har til hensikt å fremskaffe et felles grunnlag for å utvikle organisasjonens sikkerhetsstandard og effektiv sikkerhetspraksis innad i organisasjonen og for å skape tillit mellom samarbeidende organisasjoner. Anbefalinger fra denne standarden bør velges og benyttes slik at de er i overensstemmelse med gjeldende lover og forskrifter.

2 Termer og definisjoner

I denne standarden gjelder følgende definisjoner:

2.1 Informasjonssikkerhet

Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet.

- **Konfidensialitet**
Å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang.
- **Integritet**
Å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige.
- **Tilgjengelighet**
Å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov.

2.2 Risikovurdering

Vurdering av trusler opp mot, virkninger på og sårbarheten til informasjonen og informasjonssystemene, og sannsynligheten for at sikkerhetshendelser kan inntreffe.

2.3 Risikostyring

Prosessen med å identifisere, kontrollere og redusere eller eliminere sikkerhetsrisikoer som kan påvirke informasjonssystemer, innenfor en akseptabel kostnadsramme.

3 Sikkerhetspolitikk

3.1 Retningslinjer for informasjonssikkerhet

Mål: Ledelsen skal gi rettledning og støtte i forbindelse med informasjonssikkerhet.

Ledelsen bør utarbeide klare retningslinjer og vise sin støtte til og forpliktelse for informasjonssikkerhet gjennom utarbeidelse og vedlikehold av en informasjonssikkerhetspolitikk for hele organisasjonen.

3.1.1 Dokumentasjon av informasjonssikkerhetspolitikken

Dokumentasjon av informasjonssikkerhetspolitikken bør godkjennes av ledelsen og offentliggjøres og formidles på en hensiktsmessig måte til alle ansatte. Det bør uttrykke ledelsens støtte og skissere organisasjonens tilnærming til administrasjon av informasjonssikkerhet. Som et minimum bør den inneholde følgende retningslinjer:

- a) en definisjon av informasjonssikkerhet, dens generelle mål og omfang, og betydningen av sikkerhet for å muliggjøre deling av informasjon (se Orientering);
- b) en erklæring om ledelsens intensjoner som støtter opp om målene og prinsippene for informasjonssikkerhet;

- c) en kort redegjørelse for sikkerhetsreglene, prinsippene, standardene og forpliktelsene som er av særlig betydning for organisasjonen, for eksempel:
 - 1) tilpasning til juridiske og kontraktsmessige forpliktelser;
 - 2) krav til opplæring i informasjonssikkerhet;
 - 3) forebygging og oppdagelse av datavirus og annen skadelig programvare;
 - 4) kontinuitetsplanlegging;
 - 5) konsekvenser ved brudd på retningslinjene for informasjonssikkerhet;
- d) definisjon av generelt og spesifikt ansvar for administrasjon av informasjonssikkerhet, herunder rapportering av sikkerhetshendelser;
- e) referanser til dokumentasjon som kan understøtte organisasjonens sikkerhetspolitikk, for eksempel mer detaljerte retningslinjer og prosedyrer for bestemte informasjonssystemer eller utførlige sikkerhetsregler som brukerne bør rette seg etter.

Disse retningslinjene bør formidles til brukerne i hele organisasjonen i en form som er relevant, tilgjengelig og forståelig for mottakeren.

3.1.2 Revisjon og evaluering av retningslinjer basert på denne standarden

Retningslinjene bør tildeles en eier som står ansvarlig for å vedlikeholde og gjennomgå dem i samsvar med en definert revisjonsprosess. Denne prosessen bør sikre at det foretas ny gjennomgang dersom det oppstår endringer som påvirker grunnlaget for den opprinnelige risikovurderingen, for eksempel vesentlige sikkerhetshendelser, ny sårbarhet eller endringer i den organisatoriske eller tekniske infrastrukturen. Det bør også etableres regelmessig, obligatorisk gjennomgang av følgende:

- a) retningslinjenes effektivitet målt på grunnlag av typen, antallet og konsekvensene av registrerte sikkerhetshendelser;
- b) kostnadene og andre virkninger av sikringstiltak for virksomhetens resultat;
- c) effekter av endret teknologi.

4 Sikkerhetsarbeid i organisasjonen

4.1 Rammeverk for informasjonssikkerhet

Mål: Å styre informasjonssikkerheten i organisasjonen.

Ledelsen bør utarbeide et rammeverk for å iverksette og kontrollere implementeringen av informasjonssikkerhet innenfor organisasjonen.

Hensiktsmessige lederfora bør etableres for å godkjenne retningslinjene for informasjonssikkerhet, tildele sikkerhetsroller og koordinere iverksettelsen av sikkerhet i hele organisasjonen. Dersom det er nødvendig, bør det opprettes en kilde for spesialisert informasjonssikkerhetsrådgivning som gjøres tilgjengelig i organisasjonen. Kontakt med eksterne sikkerhetsspesialister bør etableres for å holde tritt med industritrender, overvåke standarder og vurderingsmetoder og sikre egnede kontaktpersoner for å kunne takle sikkerhetshendelser. Det bør oppmuntres til en multidisiplinær tilnærming til informasjonssikkerhet som for eksempel involverer samarbeid mellom og medvirkning fra ledelse, brukere, administratorer, applikasjonsdesignere, revisorer og sikkerhetsstab, så vel som spesialisert kompetanse innenfor felter som forsikring og risikohåndtering.

4.1.1 Ledelsens informasjonssikkerhetsforum

Informasjonssikkerhet er et virksomhetsansvar som deles av alle medlemmene i ledergruppen. Det bør derfor vurderes å opprette et forum for å sikre klar retning og synlig støtte fra ledelsens side til sikkerhetsinitiativer. Dette forumet bør fremme sikkerhet i organisasjonen gjennom nødvendig engasjement og tilstrekkelig ressursbruk. Forumet kan være del av et eksisterende ledelsesorgan. Et slikt forum vil typisk beskjefte seg med følgende oppgaver:

- a) gjennomgang og godkjenning av retningslinjer for informasjonssikkerhet og generelle ansvarsforhold;
- b) overvåkning av vesentlige endringer i truslene mot organisasjonens informasjonsaktiva;
- c) gjennomgang og overvåkning av informasjonssikkerhetshendelser;
- d) godkjenning av større initiativ for å styrke informasjonssikkerheten.

Én av lederne bør være ansvarlig for alle sikkerhetsrelaterte aktiviteter.

4.1.2 Koordinering av informasjonssikkerhet

I en stor organisasjon kan det være nødvendig å koordinere sikringstiltak gjennom et tverrfaglig forum bestående av representanter for ledelsen i de aktuelle delene av organisasjonen. Et slikt forum vil typisk:

- a) enes om bestemte roller og ansvar for informasjonssikkerhet utover i organisasjonen;
- b) enes om bestemte metoder og prosesser for å implementere informasjonssikkerhet, for eksempel risikovurdering og systemer for sikkerhetsklassifisering;
- c) avtale og støtte sikringstiltak som omfatter hele organisasjonen, for eksempel tiltak for å øke bevisstheten omkring informasjonssikkerhet;
- d) sørge for at sikkerhet er en naturlig del av IT-planleggingsprosessen;
- e) vurdere hensiktsmessigheten og koordinere iverksettelsen av spesifikke informasjonssikkerhetskontroller for nye systemer eller tjenester;
- f) gjennomgå informasjonssikkerhetshendelser;
- g) synliggjøre støtte til informasjonssikkerhet i hele organisasjonen.

4.1.3 Tildeling av ansvar for informasjonssikkerhet

Ansvar for beskyttelse av de enkelte aktiva og for å gjennomføre spesifikke sikkerhetsprosesser bør være klart definert.

Informasjonssikkerhetspolitikken (se kapittel 3) bør gi generell rettleiding om fordeling av sikkerhetsroller og ansvarsforhold i organisasjonen. Der det er behov for det, bør dette suppleres med mer detaljerte retningslinjer for bestemte områder, systemer eller tjenester. Lokalt ansvar for de enkelte aktiva (både fysiske gjenstander og informasjon) og sikkerhetsprosedyrer, for eksempel kontinuitetsplanlegging, bør være klart definert.

I mange organisasjoner blir det utnevnt en leder for informasjonssikkerhet som får det overordnede ansvaret for utvikling og iverksettelse av sikringstiltak, og bidra til å identifisere kontrollrutiner. Det er vanlig å utnevne eiere for de enkelte informasjonsaktiva, som så blir ansvarlige for den daglige sikkerheten.

Eierne av informasjonsaktiva kan delegere sikkerhetsansvaret til andre enkeltpersoner eller til tjenesteytere. Likevel er eieren i siste instans ansvarlig for informasjonens sikkerhet og bør kunne forvise seg om at eventuelt delegert ansvar blir forsvarlig ivaretatt.

Det er viktig at områdene som hver enkelt leder har ansvar for, er tydelig beskrevet. Særlig bør man passe på følgende:

- a) De ulike aktiva og sikkerhetsprosesser som er knyttet til hvert enkelt system, bør være identifisert og klart definert.
- b) Det bør avgjøres hvilken leder som har ansvar for hvert enkelt aktivum eller sikringstiltak, og detaljene omkring dette ansvaret bør dokumenteres.
- c) Autorisasjonsnivåer bør være klart definert og dokumentert.

4.1.4 Godkjenning av utstyr til informasjonsbehandling

Det bør etableres en godkjenningsprosess for nye informasjonssystemer. Følgende bør vurderes:

- a) Nye installasjoner bør ha den nødvendige godkjenningen fra brukerens leder, som autoriserer deres bruk og formål. Godkjenning bør også innhentes fra lederen som er ansvarlig for å opprettholde det lokale informasjonssikkerhetsmiljøet, for å sikre at alle relevante sikkerhetsforskrifter og krav blir overholdt.
- b) Der det er nødvendig, bør man kontrollere at maskinvare og programvare er kompatible med andre systemkomponenter.
MERKNAD: Typegodkjenning kan være nødvendig for bestemte forbindelser.
- c) Bruk av personlig IT-utstyr til å behandle virksomhetsinformasjon og eventuelle nødvendige kontroller bør autoriseres.
- d) Bruk av personlig IT-utstyr på arbeidsplassen kan øke sårbarheten og bør derfor vurderes og autoriseres.

Disse tiltakene er spesielt viktig i store nettverksmiljøer.

4.1.5 Sikkerhetsanbefalinger fra spesialister

Mange organisasjoner vil trenge råd fra sikkerhetsspesialister. Ideelt sett bør slike råd innhentes fra en erfaren sikkerhetsrådgiver internt. Men ikke alle organisasjoner ønsker å ansette en slik spesialist. I disse tilfellene anbefales det at en bestemt person blir utpekt til å koordinere intern kunnskap og erfaringer for å sikre ensartet behandling av sikkerhetsspørsmål og bistå med råd i utformingen av sikkerhetsbeslutninger. Vedkommende bør dessuten ha tilgang til egnede eksterne rådgivere som kan gi ekspertråd på områder der man selv ikke har erfaring.

Sikkerhetsrådgivere eller tilsvarende kontaktpersoner bør kunne gi anbefalinger om alle aspekter ved informasjonssikkerhet. Kvaliteten på deres vurderinger av sikkerhetstrusler og forslag til mottiltak vil være avgjørende for hvor effektiv organisasjonens informasjonssikkerhet er. For å oppnå størst mulig påvirkning og innflytelse bør rådgiverne ha direkte tilgang til all ledelse i hele organisasjonen.

Rådgiveren for informasjonssikkerhet eller tilsvarende kontaktperson bør rådspørres så tidlig som mulig ved mistanke om sikkerhetshendelser eller -brudd, for å bidra med råd eller ressurser til relevante undersøkelser. Selv om de fleste interne sikkerhetsundersøkelser normalt vil bli håndtert av ledelsen, kan sikkerhetsrådgiveren tilkalles for å gi anbefalinger, lede eller koordinere relevante undersøkelser.

4.1.6 Samarbeid mellom organisasjoner

Organisasjonen bør ha hensiktsmessig kontakt med myndigheter, reguleringsorganer, tjenesteleverandører og telekommunikasjonsorganisasjoner, for å sikre at hensiktsmessige tiltak kan iverksettes og råd innhentes i tilfelle sikkerhetshendelser. På samme måte bør medlemskap i sikkerhetsgrupper og industrifora vurderes.

Utveksling av sikkerhetsinformasjon bør begrenses slik at konfidensiell informasjon om organisasjonen ikke havner hos uautoriserte personer.

4.1.7 Uavhengig vurdering av informasjonssikkerheten

Organisasjonens informasjonssikkerhetspolitikk (se 3.1.1) beskriver overordnede krav og ansvaret for informasjonssikkerheten. Håndhevelsen av denne politikken bør gjennomgå av en uavhengig part for å sikre at organisasjonens praksis gjenspeiler retningslinjene, og at de er gjennomførbare og effektive (se 12.2).

En slik gjennomgang kan utføres av interne revisjonsorganer, en uavhengig seniorleder eller en ekstern organisasjon som spesialiserer seg på slike vurderinger i de tilfeller der slike kandidater har den nødvendige kompetanse og erfaring.

4.2 Sikkerhet i forhold til tredjepart

Mål: Å opprettholde sikkerheten i organisasjonens informasjonssystemer og informasjonssystemer i forbindelse med tilgang og adgang for tredjepart.

Tilgang til organisasjonens informasjonssystemer for tredjepart bør være underlagt kontroll.

Der det eksisterer et virksomhetsbehov for slik tredjepartstilgang, bør det foretas en risikovurdering for å kartlegge sikkerhetskonskvensene og kontrollkravene. Sikringstiltak bør avtales og defineres i kontrakten med tredjepart.

Tredjepartstilgang kan også involvere andre deltakere. Kontrakter som gir tredjepartstilgang, bør omfatte mulig engasjement for ytterligere ressurser og vilkårene for deres tilgang.

Denne standarden kan brukes som grunnlag for slike kontrakter og når man vurderer å sette bort hele eller deler av informasjonsbehandlingen.

4.2.1 Identifisering av risikoer forbundet med tredjeparts tilgang og adgang

4.2.1.1 Tilgang og adgang

Former for tilgang og adgang som man innvilger en tredjepart, er av særlig betydning. For eksempel er risikoen ved tilgang gjennom en nettverksforbindelse en annen enn risikoen ved fysisk adgang. Følgende bør vurderes:

- a) fysisk adgang, for eksempel til kontorer, datarom, arkivskap;
- b) logisk tilgang, for eksempel til en organisasjons databaser, informasjonssystemer.

4.2.1.2 Grunner til å gi tilgang og adgang

Det er en rekke grunner til at tredjepart kan innvilges tilgang eller adgang. For eksempel finnes det tredjeparter som leverer tjenester til en organisasjon, og som ikke befinner seg på stedet, men som kan bli innvilget tilgang eller adgang. Eksempler er:

- a) brukerstøtte for maskinvare og programvare som trenger tilgang på systemnivå eller applikasjonsfunksjonalitet på lavere nivå;
- b) handels- eller samarbeidspartnere som kan utveksle informasjon, knytte seg til informasjonssystemer eller dele databaser.

Informasjon kan utsettes for risiko ved tilgang fra tredjeparter med mangelfulle sikringstiltak. Der det finnes et forretningsmessig behov for tilknytning til tredjepart, bør man foreta en risikovurdering for å identifisere nødvendigheten av spesifikke kontrolltiltak. Denne vurderingen bør ta hensyn til hvilke former for tilgang som kreves, verdien av den aktuelle informasjonen, sikringstiltakene som benyttes av tredjepart og betydningen av denne tilgangen for organisasjonens informasjonssikkerhet.

4.2.1.3 Leverandører på stedet

Tredjeparter som oppholder seg på organisasjonens område i en periode som er definert i kontrakten deres, kan også skape svakheter i sikkerhetsopplegget. Eksempler på tredjeparter med fysisk adgang til organisasjonen omfatter:

- a) vedlikeholdspersonell og brukerstøtte for maskin- og programvare;
- b) rengjøring, catering, sikkerhetsvakter og andre støttefunksjoner som er satt bort;
- c) studenter på utplassering og andre korttidsansatte;
- d) konsulenter.

Det er viktig å forstå hvilke kontrollrutiner som bør innføres for å regulere tredjeparts tilgang til informasjonssystemene. Generelt bør alle krav til sikkerhet som følger av tredjepartstilgang eller interne kontroller, være gjenspeilet i kontrakten med tredjepart (se også 4.2.2). Hvis det for eksempel er særlig behov for konfidensialitet for informasjonen, kan man benytte taushetserklæring (se 6.1.3).

Tilgang for tredjepart til informasjon og informasjonssystemer bør ikke gis før de nødvendige tiltakene er innført og en kontrakt som definerer vilkårene for forbindelsen eller tilgangen, er signert.

4.2.2 Sikkerhetsbetingelser for kontrakter med tredjeparter

Ordninger der tredjepart får tilgang til organisasjonens informasjonssystemer, bør baseres på en formell kontrakt som inneholder, eller refererer til, alle nødvendige krav for å sikre overensstemmelse med organisasjonens sikkerhetspolitikk og standarder. Kontrakten bør sørge for at det ikke forekommer noen misforståelse mellom organisasjonen og tredjeparten. Organisasjonen bør forsikre seg om at leverandørens forsikringer er dekkende. Følgende betingelser bør vektlegges ved utarbeidelse av kontrakten:

- a) generelle retningslinjer for informasjonssikkerhet;
- b) beskyttelse av aktiva, herunder:
 - 1) prosedyrer for å beskytte organisasjonens aktiva, inklusive informasjon og programvare;
 - 2) prosedyrer for å avgjøre om aktiva er blitt kompromittert, for eksempel om tap eller endring av data har forekommet;
 - 3) kontrollrutiner for å sikre tilbakelevering eller ødeleggelse av informasjon og aktiva ved slutten av eller på et bestemt tidspunkt i løpet av kontraktens levetid;
 - 4) integritet og tilgjengelighet;
 - 5) restriksjoner på kopiering og offentliggjøring av informasjon;
- c) beskrivelse av de enkelte tjenestene som skal gjøres tilgjengelig;
- d) mål for tjenestenivå og definisjon av uakseptabelt tjenestenivå;
- e) ordninger for overføring av personale der dette er nødvendig;
- f) avtalepartenes respektive forpliktelser;
- g) ansvar av juridisk art, for eksempel lover og forskrifter for databeskyttelse, med særlig henblikk på ulike nasjonale rettssystemer dersom kontrakten involverer samarbeid mellom organisasjoner i ulike land (se også 12.1);
- h) rettigheter til intellektuell eiendom, fordeling av opphavsrettigheter (se 12.1.2) og beskyttelse av fellesprodukter (se også 6.1.3);
- i) avtale om tilgangskontroll som dekker:
 - 1) tillatte tilgangs- og adgangsmetoder samt kontroll og bruk av unik identifikasjon som for eksempel bruker-id og passord;
 - 2) autorisasjonsprosess for brukertilgang og privilegier;
 - 3) krav om ajourført liste over alle brukere som er autorisert for å bruke tjenestene som gjøres tilgjengelig, og en beskrivelse av hva disse brukerrettighetene og -privilegiene består i;
- j) definisjon av verifiserbare ytelseskriterier, samt overvåking og rapportering av ytelse;
- k) rett til å overvåke og sperre for brukeraktiviteter;
- l) rett til å revidere kontraktfestet ansvar eller la tredjepart gjennomføre slik revisjon;
- m) opprettelse av en opptrappingsprosess for problemløsning. Unntaksordninger bør også overveies der det er hensiktsmessig;
- n) ansvar for installasjon og vedlikehold av maskin- og programvare;
- o) klare rapporteringsrutiner og rapportformater;
- p) klar og spesifisert prosess for endringsledelse;
- q) nødvendige fysiske beskyttelsestiltak og mekanismer for å sikre at disse tiltakene blir gjennomført;
- r) opplæring av brukere og administratorer i metoder, prosedyrer og sikkerhet;
- s) sikringstiltak for å sikre beskyttelse mot skadelig programvare (se 8.3);
- t) ordninger for rapportering, varsling og granskning av sikkerhetshendelser og sikkerhetssvikt;
- u) tredjeparts forhold til underleverandører.

4.3 Outsourcing

Mål: Å opprettholde informasjonssikkerheten når ansvaret for informasjonsbehandling blir satt bort til en annen organisasjon.

Kontrakten mellom partene i en outsourcingavtale bør ta hensyn til sikkerhetsrisikoen, kontrolltiltakene og prosedyrene for informasjonssystemer, nettverk og/eller sluttbrukermiljøer.

4.3.1 Krav til sikkerhet i outsourcingkontrakter

Det bør utarbeides en kontrakt mellom partene som beskriver kravene til sikkerhet når en organisasjon setter bort hele eller deler av informasjonssystemet, nettverk og/eller sluttbrukermiljøet.

Kontrakten bør for eksempel beskrive:

- hvordan lover og forskrifter skal imøtekommes, for eksempel lover om beskyttelse av data;
- hvilke ordninger som skal iverksettes for å sikre at alle parter som er involvert i outsourcingavtalen, inklusive underleverandører, er oppmerksomme på sitt sikkerhetsansvar;
- hvordan integriteten og konfidensialiteten til organisasjonens virksomhetsaktiva skal opprettholdes og testes;
- hvilke fysiske og logiske sikringstiltak som skal benyttes for å begrense tilgangen til organisasjonens sensitive forretningsinformasjonen til autoriserte brukere;
- hvordan tjenestens tilgjengelighet skal opprettholdes i tilfelle katastrofe;
- hvilke fysiske sikkerhetsnivåer skal gjelde for informasjonssystemer som er satt bort;
- rett til å revidere.

Vilkårene som er listet opp i 4.2.2, er også å betrakte som en del av denne kontrakten. Kontrakten bør tillate at kravene til sikkerhet blir presisert i en plan for styring av sikkerheten som partene enes om.

Selv om outsourcingkontrakter kan by på enkelte sammensatte sikkerhetsspørsmål, kan sikringstiltakene som er angitt i disse retningslinjene, danne utgangspunkt for en avtale om struktur og innhold i planen for styring av sikkerhet.

5 Klassifisering og sikring av aktiva

5.1 Ansvar for aktiva

Mål: Å opprettholde nødvendig beskyttelse av organisasjonens aktiva.

Alle vesentlige informasjonsaktiva bør registreres og tildeles en eier.

Eieransvar for organisasjonens aktiva sikrer at den nødvendige beskyttelsen blir opprettholdt. Alle vesentlige aktiva bør ha identifiserte eiere, og ansvaret for opprettholdelse av nødvendige sikringstiltak bør tilskrives bestemte roller. Myndigheten til å gjennomføre tiltak kan delegeres. Ansvaret bør imidlertid ligge hos den oppnevnte eieren.

5.1.1 Oversikt over aktiva

En oversikt over organisasjonens aktiva bidrar til å sikre effektiv beskyttelse av aktiva, og kan også være påkrevd av andre virksomhetsgrunner, for eksempel helse og personsikkerhet, forsikring eller finansielle (formue- og verdiforvaltning) årsaker. Prosessen med å utarbeide en oversikt over aktiva er en viktig del av risikohåndteringen. En organisasjon bør kunne identifisere sine aktiva og den relative verdien og betydningen av disse aktiva. Basert på denne informasjonen kan organisasjonen så sørge for et beskyttelsesnivå som er i samsvar med deres verdi og betydning. En inventarliste over de viktigste aktiva i tilknytning til hvert enkelt informasjonssystem bør også utarbeides og holdes oppdatert. Hvert enkelt aktivum bør identifiseres. Eierskap og sikkerhetsklassifisering bør avklares og dokumenteres (dette er viktig når man gjenoppretter virksomheten etter tap eller skade). Eksempler på aktiva i tilknytning til informasjonssystemer er:

- a) informasjonsaktiva: databaser og datafiler, systemdokumentasjon, brukermanualer, opplæringsmaterieil, drifts- eller støtteprosedyrer, kontinuitetsplaner, reserveløsninger og arkivert informasjon;
- b) programvare: applikasjonsprogrammer, systemprogramvare, utviklingsverktøy og hjelpeprogrammer;
- c) fysiske aktiva: datamaskiner (prosessorer, skjermer, bærbare pc-er, modem), kommunikasjonsutstyr (rutere, hussentraler, telefaksmaskiner, telefonsvarere), magnetiske media (bånd og disketter), annet teknisk utstyr (strømforsyning, luftkjølingsenheter), møbler, lokaler;
- d) tjenester: data- og kommunikasjonstjenester, andre tekniske tjenester, for eksempel oppvarming, lys, strøm, luftkjøling.

5.2 Klassifisering av informasjon

Mål: Å sikre at informasjonsaktiva får riktig sikkerhetsnivå.

Informasjon bør klassifiseres for å indikere behovet for og graden av beskyttelse.

Informasjon har ulike grader av sensitivitet og viktighet. Enkelte typer informasjon krever ekstra beskyttelse eller spesiell håndtering. Et system for klassifisering av informasjon bør brukes for å definere de riktige beskyttelsesnivåene og formidle behovet for spesielle håndteringsprosedyrer.

5.2.1 Retningslinjer for klassifisering

Klassifisering av informasjon med tilhørende sikringstiltak bør ta hensyn til de forretningsmessige behovene for å dele eller holde tilbake informasjon, og de forretningsmessige problemene som er forbundet med disse behovene, for eksempel uautorisert tilgang eller skade på informasjon. Generelt er klassifiseringen av informasjon en kortfattet metode for å bestemme hvordan denne informasjonen skal håndteres og beskyttes. Informasjon og utdata fra systemer som håndterer klassifiserte data, bør merkes i henhold til deres verdi og sensitivitet for organisasjonen, for eksempel i forhold til informasjonens integritet og tilgjengelighet.

På den annen side opphører informasjon ofte å være sensitiv eller viktig etter en viss tid, for eksempel når informasjonen er offentliggjort. Dette bør man ta hensyn til, ettersom for høy klassifisering kan føre til unødige kostnader for bedriften. Retningslinjene for sikkerhetsklassifisering bør ta høyde for at klassifiseringen av en gitt informasjon ikke nødvendigvis er bestemt for all fremtid, men kan endres i henhold til retningslinjer som er avtalt på forhånd (se 9.1).

Man bør ta hensyn til antall klassifiseringsnivåer og fordelene man oppnår ved å bruke dem. Unødig kompliserte systemer kan bli brysomme og uøkonomiske i bruk, eller vise seg å være upraktiske. Det bør også utvises forsiktighet ved tolking av klassifiseringsmerker på dokumenter fra andre organisasjoner, som kan ha andre definisjoner på de samme, eller nesten likelydende, klassifiseringsmerkene.

Ansvar for å klassifisere en gitt informasjon, for eksempel et dokument, et dataregister, en datafil eller diskett, og for å gjennomgå klassifiseringen med jevne mellomrom, bør ligge på opphavspersonen eller den oppnevnte eier av informasjonen.

5.2.2 Merking og håndtering av informasjon

Det er viktig at man definerer riktige prosedyrer for merking og håndtering av informasjon i samsvar med klassifiseringssystemet som organisasjonen har valgt. Disse prosedyrene bør dekke informasjonsaktiva i fysisk og elektronisk form. For hvert klassifiseringsnivå bør det defineres håndteringsrutiner som dekker følgende former for informasjonsbehandling:

- a) kopiering;
- b) oppbevaring;
- c) forsendelse via post, telefaks og elektronisk post (e-post);

- d) muntlig overlevering, herunder mobiltelefon, talelagring (voice mail) og telefonsvarer;
- e) tilintetgjørelse.

Utdata fra systemer som inneholder informasjon som klassifiseres som sensitiv eller kritisk, bør ha et hensiktsmessig klassifikasjonsmerke (i utdataene). Merket bør gjenspeile klassifiseringen i henhold til reglene som er fastsatt i 5.2.1. Utskrevne rapporter, skjermbilder, lagringsmedia (bånd, disketter, CDer, kassetter), elektroniske beskjeder og filoverføringer bør tas i betraktning.

Fysiske merker er generelt den beste form for merking. Noen former for informasjon, for eksempel dokumenter i elektronisk form, kan imidlertid ikke merkes fysisk, og elektroniske former for merking må derfor benyttes.

6 Personellsikkerhet

6.1 Sikkerhet i arbeidsbeskrivelse og personellutvelgelse

Mål: Å redusere faren for menneskelig svikt, tyveri, svindel eller misbruk av informasjonssystemer.

Sikkerhet bør tas opp allerede i ansettelsesfasen, inkluderes i kontrakter og følges opp gjennom ansettelsesforholdet.

Potensielle kandidater bør sjekkes tilstrekkelig (se 6.1.2), spesielt for stillinger der sikkerhet spiller en viktig rolle. Alle ansatte og tredjepartsbrukere av informasjonssystemer bør undertegne en taushetserklæring.

6.1.1 Sikkerhet i arbeidsbeskrivelse

Sikkerhetsrollene og -ansvaret som er bestemt i organisasjonens retningslinjer for informasjonssikkerhet, bør dokumenteres. Det generelle ansvaret for å iverksette eller opprettholde av organisasjonens sikkerhetspolitikk, så vel som det spesifikke ansvaret for beskyttelse av bestemte aktiva, eller for gjennomføring av spesielle sikkerhetsprosesser eller -aktiviteter, bør detaljeres.

6.1.2 Personellutvelgelse og -politikk

En sjekk av søkere til stillinger bør gjennomføres når jobbsøknadene mottas. Den bør omfatte følgende:

- a) tilgjengelighet av tilfredsstillende referanser, for eksempel én yrkesmessig og én personlig;
- b) kontroll av søkerens CV (for å undersøke om den er uttømmende og korrekt);
- c) bekreftelse på påberopte akademiske og profesjonelle kvalifikasjoner;
- d) uavhengig identitetskontroll (pass eller tilsvarende dokumenter).

Organisasjonen bør gjennomføre kontroll av den ansattes kredittverdighet dersom en jobb, enten fra ansettelsestidspunktet eller etter forfremmelse, innebærer at personen får tilgang til informasjonssystemer, og særlig dersom disse systemene behandler sensitiv informasjon, for eksempel finansiell informasjon eller informasjon av svært fortrolig karakter. For ansatte i høyere stillinger bør slik kontroll gjennomføres jevnlig.

En lignende undersøkelsesprosess bør også gjennomføres for leverandører og midlertidig ansatte. Der disse ansatte blir leid inn gjennom et byrå, bør kontrakten med byrået tydelig spesifisere byråets ansvar for utvelgelse og varslingsprosedyrene som skal følges dersom utvelgelsesprosessen ikke er blitt gjennomført, eller hvis resultatene gir grunn til tvil eller bekymring.

Ledelsen bør vurdere nødvendigheten av oppfølging av nye og uerfarne ansatte som har autorisert tilgang til sensitive systemer. Alle ansatte bør gjennomgå periodisk vurdering og godkjenning av en overordnet medarbeider.

Ledere bør være oppmerksomme på at personlige forhold kan påvirke de ansattes arbeid. Personlige eller økonomiske problemer, endringer i oppførsel eller livsstil, gjentatt fravær og tegn på stress eller depresjon

kan føre til underslag, tyveri, feil, eller få andre sikkerhetsmessige konsekvenser. Slik informasjon må håndteres i samsvar med relevant lovgivning som foreligger på det aktuelle området.

6.1.3 Taushetserklæring

Taushetserklæringer brukes for å gjøre oppmerksom på at det forekommer konfidensiell eller hemmelig informasjon. De ansatte bør normalt undertegne en slik erklæring samtidig med ansettelseskontrakten.

Midlertidig ansatte og tredjepartsbrukere som ikke allerede er dekket av eksisterende kontrakt (som inneholder en taushetserklæring), bør undertegne en tilsvarende erklæring før de får tilgang til informasjonssystemer.

Taushetserklæringer bør gjennomgås på nytt når ansettelsesforholdet endres, særlig når ansatte skal forlate organisasjonen, eller kontrakter løper ut.

6.1.4 Betingelser og ansettelsesvilkår

Betingelsene og ansettelsesvilkårene bør opplyse om den ansattes ansvar for informasjonssikkerhet. Der det er relevant, bør dette ansvaret også gjelde i en nærmere spesifisert periode etter at ansettelsesforholdet er over. Kontrakten bør inkludere reaksjonsformer dersom den ansatte ser bort fra kravene til sikkerhet.

Den ansattes juridiske ansvar og rettigheter, for eksempel med hensyn til opphavsrettigheter eller lover om databeskyttelse, bør klargjøres og inkluderes i betingelsene og ansettelsesvilkårene. Ansvar for klassifisering og håndtering av arbeidsgivers data bør også inkluderes. I de tilfeller der det er nødvendig, bør betingelsene og ansettelsesvilkårene opplyse om at dette ansvaret også gjelder utenfor organisasjonens område og normal arbeidstid, for eksempel i forbindelse med fjernarbeid (se også 7.2.5 og 9.8.1).

6.2 Brukeropplæring

Mål: Å sørge for at brukerne er oppmerksomme på trusler mot informasjonssikkerheten, og at de er gitt mulighet til å etterleve organisasjonens sikkerhetspolitikk i sitt daglige arbeid.

Brukerne bør få opplæring i sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer.

6.2.1 Utdanning og opplæring i informasjonssikkerhet

Før ansatte i organisasjonen og eventuelle tredjepartsbrukere får tilgang til informasjon eller tjenester, bør de få hensiktsmessig opplæring. Dette omfatter krav til sikkerhet, juridisk ansvar og interne sikringstiltak, så vel som opplæring i riktig bruk av informasjonssystemer, for eksempel innloggingsprosedyrer og bruk av programvarepakker. I tillegg bør de få regelmessig oppdatering i organisasjonens politikk og prosedyrer.

6.3 Håndtering av sikkerhetshendelser og funksjonssvikt

Mål: Å begrense skadevirkningene av sikkerhetshendelse og funksjonssvikt samt overvåke og trekke lærdom av slike hendelser.

Hendelser som går ut over sikkerheten, bør rapporteres til ledelsen gjennom de riktige kanaler så fort som mulig.

Alle ansatte og leverandører bør gjøres oppmerksom på rapporteringsprosedyrer for ulike hendelser (sikkerhetsbrudd, trusler, svakheter eller feil) som kan ha betydning for sikringen av organisasjonens aktiva. De bør være pålagt å rapportere alle observerte eller mistenkelige hendelser til riktig instans så snart som mulig. Organisasjonen bør utarbeide en formell disiplinærprosess for å ta seg av ansatte som bryter sikkerhetsforskriftene. For å kunne håndtere hendelser på forsvarlig måte, kan det være nødvendig å samle inn bevis så snart som mulig etter at de har inntruffet (se 12.1.7).

6.3.1 Rapportering av sikkerhetshendelser

Sikkerhetshendelser bør rapporteres til ledelsen gjennom de riktige kanalene så raskt som mulig.

Formelle rapporteringsrutiner bør etableres sammen med prosedyrer som beskriver hvordan man skal forholde seg når man mottar rapport om en hendelse. Alle ansatte og leverandører bør gjøres oppmerksom på prosedyrene for å rapportere sikkerhetshendelser, og bør pålegges å rapportere slike hendelser omgående. Hensiktsmessige tilbakemeldingsprosesser bør utvikles for å sikre at de som rapporterer om hendelser, blir orientert om resultatet etter at hendelsen er behandlet og avsluttet. Erfaringer fra slike hendelser kan benyttes for å skape bevissthet blant brukerne (se 6.2), og som eksempler på hva som kan skje, hvordan man skal reagere, og hvordan man skal unngå slike hendelser i fremtiden (se også 12.1.7).

6.3.2 Rapportering av sikkerhetsmessige svakheter

Brukerne av informasjonstjenestene bør pålegges å rapportere observasjoner av sikkerhetsmessige svakheter i, eller trusler mot, systemer og tjenester, eller mistanke om slike. De bør omgående rapportere disse til sine overordnede eller direkte til sin tjenesteleverandør. Brukerne bør informeres om at de ikke under noen omstendigheter bør forsøke å bekrefte en mistanke om sikkerhetsmessige svakheter. Dette er for å beskytte dem selv, ettersom det å teste slike svakheter kan bli tolket som et forsøk på å misbruke systemet.

6.3.3 Rapportering av funksjonsfeil i programvare

Prosedyrer bør etableres for rapportering av funksjonsfeil i programvare. Følgende tiltak bør inkluderes:

- a) Notér symptomene og eventuelle meldinger som kommer til syne på skjermen.
- b) Slutt å bruke maskinen, og isoler den hvis mulig. Informer riktig instans umiddelbart. Dersom maskinen skal undersøkes, bør den frakobles alle organisasjonens nettverk før den startes på nytt. Diskettene bør ikke brukes i andre maskiner.
- c) Rapport saken omgående til informasjonssikkerhetsansvarlig.

Brukerne bør ikke forsøke å fjerne den mistenkelige programvaren med mindre de er autorisert til å gjøre det. Reparasjoner bør foretas av spesielt utdannede og erfarne medarbeidere.

6.3.4 Lærdommer av sikkerhetshendelser

Det bør foreligge mekanismer for å overvåke og måle typen, omfanget og kostnadene av sikkerhetshendelser og funksjonssvikt. Denne informasjonen bør brukes til å identifisere tilbakevendende eller alvorlige hendelser eller svikt. Dette kan indikere behov for forbedrede eller ytterligere sikringstiltak for å begrense hyppigheten, skaden og kostnadene ved fremtidige hendelser, eller vurderes i revisjonen av organisasjonens sikkerhetspolicy (se 3.1.2).

6.3.5 Disiplinære reaksjoner

Det bør foreligge en formell disiplinærprosess for ansatte som har forbrutt seg mot organisasjonens sikkerhetsforskrifter og prosedyrer (se 6.1.4 og, når det gjelder oppbevaring av bevismateriale, 12.1.7). En slik prosess kan avskrekke ansatte som ellers ville blitt fristet til å omgå sikkerhetsprosedyrer. I tillegg bør den sikre korrekt, rettfærdig behandling av ansatte som er mistenkt for alvorlige eller vedvarende sikkerhetsbrudd.

7 Fysisk og miljømessig sikkerhet

7.1 Sikre områder

Mål: Å forhindre uautorisert tilgang til, skade på og forstyrrelse av virksomhetsseiendom og informasjon.

Et system som behandler kritisk eller følsom virksomhetsinformasjon, bør plasseres i sikre områder beskyttet av en definert sikkerhetssone med hensiktsmessige sikkerhetsbarrierer og adgangskontroll. Systemet bør beskyttes fysisk mot uautorisert adgang, skader eller forstyrrelser.

De iverksatte sikringsstiltakene bør stå i samsvar med identifisert risiko. Retningslinjer for rydding av arbeidsplassen anbefales for å redusere faren for uautorisert adgang til eller skade på papir, media og IT-utstyr.

7.1.1 Fysisk sikkerhetssone

Fysiske sikringstiltak kan gjennomføres ved å skape ulike fysiske barrierer rundt forretningslokalene og IT-installasjonene. Hver barriere etablerer en sikkerhetssone, og for hver av disse sonene øker den totale sikkerheten. Organisasjoner bør bruke sikkerhetssoner for å beskytte områder som inneholder informasjonssystemer (se 7.1.3). En sikkerhetssone er noe som danner en barriere, for eksempel en vegg, en port med adgangskort eller en bemannet resepsjonsskranke. Plasseringen av og kravene til de enkelte barrierene vil avhenge av resultatene av en risikovurdering.

Følgende retningslinjer og tiltak bør vurderes og innføres der det er hensiktsmessig:

- Sikkerhetssonene bør være klart definert.
- Sonen rundt en bygning eller tomt som inneholder informasjonssystem, bør være fysisk sikker (det vil si at det ikke må være åpninger i sikkerhetssonen eller -området der et innbrudd lett vil kunne finne sted). Ytermurene på stedet bør være solid konstruert, og alle ytterdører bør være tilstrekkelig beskyttet mot uautorisert tilgang, for eksempel ved hjelp av kontrollmekanismer, sprinkler, alarmer, låser osv.
- Bemannet resepsjonsområde eller andre løsninger for å kontrollerer fysisk adgang til området eller bygningen bør opprettes. Tilgang til stedet og bygningen bør begrenses bare til autorisert personell.
- Fysiske stengsler bør, hvis nødvendig, være fra gulv til tak for å forhindre uautorisert adgang og miljømessig ødeleggelse, for eksempel ved brann eller oversvømmelse.
- Alle branddører i sikkerhetssonen bør være sikret med alarm og ha smekklås.

7.1.2 Fysisk adgangskontroll

Sikrede områder bør beskyttes med hensiktsmessige adgangskontroller for å sikre at bare autorisert personell får adgang. Følgende tiltak bør vurderes:

- Besøkende i sikrede områder bør holdes under overvåkning eller klareres, og dato og tid for inn- og utpassering bør registreres. Besøkende bør bare gis adgang for spesifikke, autoriserte formål, og de bør instrueres om sikkerhetskravene og nødprosedyrene i sonen.
- Tilgang til følsom informasjon og informasjonssystemer bør sikres og begrenses bare til autorisert personell. Adgangskontroll, for eksempel magnetkort med PIN-kode, bør benyttes for å autorisere og verifisere all adgang. Det bør opprettholdes forsvarlig revisjonsspor over all inn- og utpassering.
- Alt personell bør bære synlig identifikasjon og oppfordres til å kreve legitimasjon fra ukjente uten følge og alle som ikke bærer synlig identifikasjon.
- Adgangsrettigheter til sikrede områder bør gjennomgås og oppdateres regelmessig.

7.1.3 Sikring av kontorer, rom og utstyr

Et sikret område kan være et låst kontor eller flere rom innenfor en fysisk sikkerhetssone som kan låses av, og som kan inneholde låsbare arkiver eller pengeskap. Lokalisering og utforming av sikrede områder bør ta hensyn til risikoen for skade ved brann, oversvømmelse, eksplosjon, opprør og andre former for naturlige eller fremkalt katastrofer. Det bør også tas hensyn til relevante helse- og sikkerhetsforskrifter og standarder. Likeledes bør det tas høyde for de sikkerhetstrusler som naboområdene måtte utgjøre, for eksempel vannlekkasje fra tilliggende lokaler.

Følgende sikringstiltak bør overveies:

- a) Viktig utstyr bør plasseres slik at utenforstående ikke har adgang.
- b) Bygningene bør være nøytrale og fortelle minst mulig om sitt formål, uten åpenbare indikasjoner på innsiden eller utsiden om at de brukes til informasjonsaktivitet.
- c) Støttefunksjoner og -utstyr, for eksempel kopi- og telefaksmaskiner, bør plasseres på et egnet sted innenfor det sikrede området for å unngå behov for adgang som kan kompromittere informasjon.
- d) Dører og vinduer bør låses når de er ubevoktet, og utvendig beskyttelse av vinduer, særlig på bakkenivå, bør vurderes.
- e) Hensiktsmessige innbruddsdetektorer som oppfyller profesjonelle standarder og blir testet regelmessig, bør installeres på alle ytterdører og tilgjengelige vinduer. Ubenyttede områder bør beskyttes med alarm til alle tider. Det er også nødvendig å sørge for beskyttelse av andre områder, for eksempel datarom og kommunikasjonsentraler.
- f) Organisasjonens informasjonssystemer bør være fysisk atskilte fra utstyr som administreres av tredjepart.
- g) Interne adresse- og telefonlister som angir plasseringen av sensitivt informasjonssystem, bør ikke være offentlig tilgjengelig.
- h) Farlig eller lettantennelige materiale bør oppbevares forsvarlig og på trygg avstand fra sikrede områder. Rekvisita, for eksempel skrivepapir, bør ikke oppbevares i sikrede områder før det skal brukes.
- i) Reserveutstyr og sikkerhetskopier bør plasseres på et trygt sted for å unngå skade som følge av katastrofe ved hovedinstallasjonen.

7.1.4 Retningslinjer for arbeid i sikre områder

Det kan være behov for ytterligere kontrollrutiner og retningslinjer for å styrke sikkerheten i et sikret område. Dette omfatter kontroll av personell eller tredjepart som arbeider i det sikrede området, samt av tredjeparts aktiviteter som finner sted der. Følgende retningslinjer bør vurderes:

- a) Personell bør bare informeres om eksistensen av eller aktivitetene i et sikret område når det er helt nødvendig.
- b) Det bør unngås at personer arbeider uten oppsyn i sikrede områder både av hensyn til personsikkerhet og for å forhindre muligheten for ulovlige handlinger.
- c) Sikrede områder som står ledige, bør være fysisk avstengt og sjekkes regelmessig.
- d) Tredjeparts støttepersonell bør bare få begrenset adgang til sikre områder eller sensitivt informasjonssystem når det er helt nødvendig. Denne adgangen bør være autorisert og overvåket. Ytterligere barrierer og soner for å kontrollere fysisk adgang kan være påkrevet mellom områder med ulike sikkerhetskrav innenfor sikkerhetssonen.
- e) Fotografering, båndopptak eller bruk av videoutstyr bør ikke være tillatt med mindre det er autorisert.

7.1.5 Isolert område for vareleveranser

Områder for lasting og lossing bør kontrolleres, og hvis nødvendig, isoleres fra datarom for å unngå uautorisert adgang. Sikringskravene til disse områdene bør vurderes i forhold til trusselbildet. Følgende retningslinjer bør vurderes:

- a) Adgang til leveranseområdet fra utsiden av bygningen bør begrenses til identifisert og autorisert personell.
- b) Leveranseområdet bør utformes slik at forsyninger kan losses uten at det gis adgang til andre deler av bygningen.
- c) Ytterdørene til leveranseområdet bør være sperret når innerdøren er åpen.
- d) Innkommende varer bør kontrolleres for potensielle risikoer [se 7.2.1d)] før de flyttes fra leveranseområdet til bruksstedet.
- e) Innkommet materiell bør registreres, hvis mulig, når de ankommer stedet (se 5.1).

7.2 Sikring av utstyr

Mål: Å forhindre tap, skader eller misbruk av organisasjonens aktiva og forstyrrelser av organisasjonens aktiviteter.

Utstyret bør beskyttes fysisk mot sikkerhetsrisikoer og miljøtrusler.

Beskyttelse av utstyr (inklusive det som brukes utenfor organisasjonens område) er nødvendig for å redusere faren for uautorisert tilgang til data, og for å beskytte mot tap eller skade. Fysisk beskyttelse omfatter også plassering og disponering av informasjonssystem. Spesielle sikringstiltak kan være påkrevd for å beskytte mot skade eller uautorisert adgang, og for å beskytte støtteutstyr som strømforsyning og kablingsinfrastruktur.

7.2.1 Plassering og beskyttelse av informasjonssystem

Utstyr bør plasseres eller beskyttes slik at det reduserer risikoen for miljømessige trusler og farer, samt mulighetene for uautorisert adgang. Følgende retningslinjer bør vurderes:

- a) Utstyr bør plasseres slik at det blir minst mulig unødvendig adgang til arbeidsområdet.
- b) Informasjonssystem som håndterer sensitive data, bør plasseres slik at risikoen for tilfeldig innsyn ved bruk blir minst mulig.
- c) Komponenter som trenger særlig beskyttelse, bør isoleres for å unngå unødvendig beskyttelsesnivå for øvrig.
- d) Kontrolltiltak bør gjennomføres for å redusere faren for potensielle trusler som:
 - 1) tyveri;
 - 2) brann;
 - 3) eksplosjoner;
 - 4) røyk;
 - 5) oversvømmelse (eller vannmangel);
 - 6) støv;
 - 7) vibrasjon;
 - 8) kjemisk påvirkning;
 - 9) variasjoner i strømforsyning;
 - 10) elektromagnetisk stråling.
- e) Organisasjoner bør vurdere sine retningslinjer når det gjelder spising, drikking og røyking i nærheten av informasjonssystem.
- f) Organisasjonen bør overvåke miljømessige forhold som kan ha negativ innvirkning på driften av informasjonssystem.

- g) Innføring av spesielle beskyttelsestiltak, for eksempel tastaturbeskyttelse, bør også vurderes ved bruk av utstyr i industrimiljø.
- h) Konsekvensene av en eventuell katastrofe i nærheten, for eksempel brann i en nærliggende bygning, vannlekkasje fra taket eller i kjelleretasjer under bakkenivå, eller eksplosjon i gaten utenfor, bør vurderes.

7.2.2 Strømforsyning

Utstyr bør beskyttes mot strømbrudd og andre elektriske uregelmessigheter. Strømforsyningen bør være i overensstemmelse med utstyrsprodusentens spesifikasjoner. Tiltak for å sikre uavbrutt strømforsyning omfatter:

- a) bruk av flere kilder for å unngå strømstans ved svikt i ett enkelt punkt;
- b) avbruddsfri strømforsyning (UPS – Uninterruptable Power Supply);
- c) nødstrømforsyning.

Det anbefales å gå til anskaffelse av en UPS for å sikre kontrollert avstenging eller kontinuerlig drift av utstyr som understøtter kritiske driftoperasjoner. Kontinuitetsplaner bør beskrive hvilke aktiviteter som må utføres ved feil på UPS. UPS-er bør testes regelmessig i samsvar med produsentens spesifikasjoner.

Videre bør det plasseres nødstrømsbrytere i nærheten av nødutganger i utstyrsrommene for å muliggjøre rask avstenging av strømmen i krisetilfeller. Alle bygningene bør utrustes med lynavledere, og beskyttelsesfilter mot lynnedslag bør monteres på alle eksterne kommunikasjonslinjer.

7.2.3 Sikring av kabling

Kabler for strømforsyning og telekommunikasjonskabler som frakter data eller IT-støttetjenester, bør beskyttes mot avlytting og skade. Følgende sikringstiltak bør tas under overveielse:

- a) Strøm- og telekommunikasjonslinjer til IT-utstyret bør være gravd ned eller forsvarlig beskyttet på annen måte.
- b) Nettverkskabler bør beskyttes mot uautorisert avlytting eller skade, for eksempel ved hjelp av kabelgater, eller ved å unngå at de strekkes gjennom offentlig område.
- c) Strømkabler bør isoleres fra kommunikasjonskabler for å hindre forstyrrelser.
- d) Ved spesielt sensitive eller viktige systemer bør man vurdere ytterligere sikringstiltak som:
 - 1) installasjon av armerte kabelgater og låste rom eller bokser ved inspeksjons- og termineringspunkter;
 - 2) bruk av alternative rutings- eller overføringsmedia;
 - 3) bruk av fiberoptisk kabling;
 - 4) sveip etter uautoriserte utstyrsenheter som er tilkoblet kablene.

7.2.4 Vedlikehold av utstyr

Utstyr bør vedlikeholdes på riktig måte for å sikre fortsatt tilgjengelighet og integritet. De følgende retningslinjene bør vurderes:

- a) Informasjonssystem bør vedlikeholdes i henhold til leverandørens anbefalte serviceintervaller og spesifikasjoner.
- b) Bare autorisert vedlikeholdspersonell bør foreta reparasjoner og service på utstyret.
- c) Logg bør føres over alle feil og mistanker om feil, og over alt forebyggende og korrektivt vedlikehold.
- d) Hensiktsmessige sikringstiltak bør iverksettes når utstyr sendes bort fra organisasjonens område for vedlikehold (se også 7.2.6 med hensyn til slettede, utviskede og overskrevne data). Alle krav som stilles i forsikringspolicene, bør oppfylles.

7.2.5 Sikkerhet for eksternt plassert utstyr

All bruk av IT-utstyr bør autoriseres av ledelsen, ved behandling av virksomhetsdata utenfor virksomhetens lokaler, uavhengig av eierskap. Sikkerheten bør være den samme som for utstyr som brukes for de samme formålene internt i organisasjonen, og bør ta høyde for risikoen ved å arbeide utenfor organisasjonens område. IT-utstyr omfatter alle former for personlige datamaskiner, elektroniske tidsplanleggere, mobiltelefoner, papirer eller annet man bruker på hjemmekontor eller tar med bort fra det vanlige arbeidsstedet. Følgende retningslinjer bør etableres:

- a) Utstyr og media som medtas fra organisasjonens lokaler, bør ikke være ubevoktet på offentlige steder. Bærbare datamaskiner bør fraktes som håndbagasje og, hvis mulig, tildekkes under reise.
- b) Produsentens retningslinjer for beskyttelse av utstyret bør alltid overholdes, for eksempel beskyttelse mot sterke elektromagnetiske felt.
- c) Kontrollrutiner for hjemmearbeid bør etableres etter en risikovurdering, og hensiktsmessige sikringstiltak bør innføres der det er nødvendig, for eksempel låsbare arkivskap, retningslinjer for rydding av arbeidsplass og adgang til datamaskiner.
- d) Sørg for tilstrekkelig forsikring som dekker bruk av eksternt plassert utstyr.

Sikkerhetsrisikoer, for eksempel skade, tyveri og avlytting, vil variere sterkt fra sted til sted og bør tas med i beregningen når man vurderer egnede sikringstiltak. Mer informasjon om andre sider ved beskyttelse av mobilt utstyr finnes under 9.8.1.

7.2.6 Sikker avhending eller gjenbruk av utstyr

Informasjon kan komme på avveie ved uforsiktig avhending eller gjenbruk av utstyr (se også 8.6.4). Lagringsmedia som inneholder sensitiv informasjon, bør fysisk ødelegges eller overskrives, ikke bare slettes med standard slettefunksjon.

Alt utstyr som inneholder lagringsmedia, for eksempel stasjonære harddisker, bør alltid kontrolleres for å sikre at data og lisensiert programvare er blitt fjernet eller overskrevet før avhending. Det kan være nødvendig å gjennomføre en risikovurdering for å avgjøre om defekte lagringsmedia som inneholder sensitiv informasjon, bør ødelegges, repareres eller kasseres.

7.3 Generelle sikringstiltak

Mål: Å forhindre misbruk eller tyveri av informasjon og informasjonssystemer.

Informasjon og informasjonssystem bør beskyttes mot uautorisert innsyn, endringer eller tyveri, og sikringstiltak bør iverksettes for å redusere tap eller skader til et minimum. Håndterings- og lagringsprosedyrer er beskrevet i 8.6.3.

7.3.1 Retningslinjer for rydding av arbeidsplass

Organisasjonen anbefales å etablere retningslinjer som krever at arbeidsplassen alltid skal være ryddet for viktige papirer og lagringsmedia, og at dataskjermen skal være blank, for på den måten å redusere faren for uautorisert tilgang, tap av og skade på informasjon i og utenfor normal arbeidstid. Retningslinjene bør ta hensyn til informasjonens sikkerhetsklassifisering (se 5.2), risikofaktorer og kulturelle aspekter ved organisasjonen.

Informasjon som ligger fremme på skrivebordet, vil dessuten sannsynligvis bli skadd eller ødelagt i en eventuell katastrofe, for eksempel ved brann, oversvømmelse eller eksplosjon.

Følgende retningslinjene bør vurderes:

- a) Der det er mulig, bør dokumenter og lagringsmedia lagres i dertil egnede låsbare skap og/eller andre former for sikkerhetsmøbler når de ikke er i bruk, særlig utenfor arbeidstiden.
- b) Følsom eller særlig viktig virksomhetssinformasjon bør oppbevares innelåst (fortrinnsvis i et brannsikkert skap) når det ikke er behov for den, særlig når kontoret er ubemannet.

- c) Personlige datamaskiner, dataterminaler og skrivere bør ikke være pålogget når de står uten tilsyn, og bør beskyttes av nøkler, passord eller andre sikkerhetstiltak når de ikke er i bruk.
- d) Områder der innkommende og utgående post oppbevares, og der telefaksmaskiner står uten tilsyn, bør beskyttes.
- e) Kopimaskiner bør være låst (eller beskyttet mot uautorisert bruk på annen måte) utenfor vanlig arbeidstid.
- f) Sensitiv eller klassifisert informasjon bør fjernes fra skriveren straks den er skrevet ut.

7.3.2 Fjerning av organisasjonens eiendeler

Informasjonssystem, informasjon eller programvare bør ikke fjernes fra organisasjonens lokaler uten autorisasjon. Der det er nødvendig og hensiktsmessig, bør utstyr kvitteres for ved ut- og innlevering. Stikkprøver bør gjennomføres for å avdekke uautorisert fjerning av organisasjonens eiendeler. De ansatte bør orienteres om at stikkprøver vil finne sted.

8 Kommunikasjons- og driftsadministrasjon

8.1 Driftsprosedyrer og ansvarsforhold

Mål: Å sikre korrekt og sikker drift av informasjonssystemer.

Ansvar og prosedyrer for administrasjon og drift av IT-infrastruktur bør etableres. Dette omfatter utvikling av hensiktsmessige driftsinstruksjoner og prosedyrer for å håndtere ulike hendelser. Prinsippet om arbeidsdeling (se 8.1.4) bør gjennomføres der det er hensiktsmessig, for å redusere faren for utilsiktet eller overlagt misbruk av systemene.

8.1.1 Dokumenterte driftsprosedyrer

Driftsprosedyrene som er beskrevet i sikkerhetsretningslinjene, bør dokumenteres og vedlikeholdes. Driftsprosedyrene bør betraktes som formelle dokumenter, og endringer bør autoriseres av ledelsen. Prosedyrene bør inneholde instruksjoner for detaljert utførelse av hver enkelt oppgave, herunder:

- a) drift og håndtering av informasjon;
- b) krav til kjøreplan, herunder avhengighet av andre systemer, tidligste starttidspunkt og seneste avslutningstidspunkt for oppgaver;
- c) instruksjoner for behandling av feil eller andre spesielle forhold som kan oppstå under utførelse av oppgaver, herunder restriksjoner på bruk av hjelpeprogrammer (se 9.5.5);
- d) kontaktpersoner i tilfelle uventede driftsmessige eller tekniske problemer;
- e) spesielle instruksjoner for håndtering av utdata, for eksempel bruk av spesialblanketter eller håndtering av konfidensielle utskrifter, inklusive prosedyrer for sikker avhending av utdata fra feilkjøring;
- f) prosedyrer for omstart og gjenoppretting i tilfelle systemfeil.

Dokumenterte prosedyrer bør også utvikles for systemvedlikehold i forbindelse med IT-infrastrukturen, for eksempel prosedyrer for oppstart og stans av datamaskiner, sikkerhetskopiering, vedlikehold av utstyr, administrasjon av datarom, posthåndtering og sikkerhet.

8.1.2 Driftsmessig endringskontroll

Endringer i IT-infrastrukturen bør underlegges kontroll. Utilstrekkelig kontroll med endringer i IT-infrastrukturen er en vanlig kilde til system- eller sikkerhetssvikt. Formelt lederansvar og prosedyrer bør derfor foreligge for å sikre tilfredsstillende kontroll med endringer i utstyr, programvare eller prosedyrer. Driftsprogrammer bør underkastes streng endringskontroll. Når programmer endres, bør det føres revisjonslogg over all relevant informasjon. Endringer i driftsmiljøet kan påvirke applikasjoner. Hvis mulig bør kontrollprosedyrene for drifts- og applikasjonsendringer integreres (se også 10.5.1). Vær særlig oppmerksom på følgende faktorer:

- a) identifisering og registrering av vesentlige endringer;
- b) vurderinger av de sannsynlige konsekvensene av slike endringer;
- c) formelle prosedyrer for godkjenning av endringsforslag;
- d) formidling av detaljert informasjon om endringen til alle relevante instanser;
- e) prosedyrer som identifiserer ansvaret for å avbryte mislykkede endringer og gjenopprette tidligere versjoner.

8.1.3 Prosedyrer for håndtering av hendelser

Ansvarsforhold og prosedyrer for håndtering av hendelser bør foreligge for å sikre rask, effektiv og riktig reaksjon på sikkerhetshendelser (se også 6.1.3). Følgende retningslinjer bør tas under overveielse:

- a) Det bør etableres prosedyrer for alle typer system- og sikkerhetshendelser, inklusive:
 - 1) systemfeil og tap av tjenester;
 - 2) utilgjengelige informasjonssystemer;
 - 3) feil på grunn av ufullstendige eller ukorrekte data;
 - 4) brudd på regler om konfidensialitet.
- b) I tillegg til vanlige kriseplaner (utformet for å gjenopprette systemer eller tjenester så raskt som mulig) bør disse prosedyrene også dekke (se også 6.3.4):
 - 1) analyse og identifikasjon av årsaken til hendelsen;
 - 2) planlegging og iverksettelse av tiltak for å unngå gjentakelse hvis det er nødvendig;
 - 3) innsamling av revisjonsspor og lignende bevis;
 - 4) kommunikasjon med dem som ble rammet av hendelsen eller var involvert i gjenopprettingen;
 - 5) rapportering av hendelsen til rett instans.
- c) Revisjonsspor og lignende bevis bør samles inn (se 12.1.7) og sikres der dette er formålstjenlig:
 - 1) for intern problemanalyse;
 - 2) for bevisførsel i forbindelse med mulige kontrakts- eller lovbrudd, eller i tilfelle rettergang ved misbruk av IT-ressurser eller brudd på personvernlovgivning;
 - 3) i forhandling om kompensasjon fra programvare- eller tjenesteleverandøren.
- d) Tiltak for gjenoppretting etter sikkerhetsbrudd og korrigerende av systemfeil bør underlegges omhyggelig formell kontroll. Prosedyrene bør sikre at:
 - 1) bare uttrykkelig identifisert og autorisert personell får tilgang til produksjonssystemer og data (se også 4.2.2 når det gjelder tredjeparts tilgang);
 - 2) alle krisetiltak dokumenteres i detalj;
 - 3) krisetiltak rapporteres til ledelsen og gjennomgås på forsvarlig måte;
 - 4) integriteten til organisasjonens informasjonssystemer og kontrollrutiner gjenoprettes så raskt som mulig.

8.1.4 Arbeidsdeling

Arbeidsdeling er en metode som reduserer faren for utilsiktet eller overlatt misbruk av IT-infrastruktur. Man bør derfor overveie å skille mellom administrasjon og utførelse av bestemte ansvarsområder eller oppgaver for å redusere muligheten for uautoriserte endringer eller misbruk av informasjon eller tjenester.

Mindre organisasjoner kan ha vanskelig for å gjennomføre denne kontrollmetoden, men prinsippet bør gjennomføres så langt det er mulig og hensiktsmessig. Der det er vanskelig å dele opp oppgaver, bør man overveie andre kontrolltiltak, for eksempel overvåking av aktiviteter, revisjonslogg og tilsyn fra ledelsen. Det er viktig at sikkerhetsrevisjonen foretas av en uavhengig instans.

Det er også viktig å sørge for at ingen enkeltperson er i stand til å begå svindel på et område der vedkommende har eneansvar, uten å bli oppdaget. Iverksettelsen av et tiltak bør skilles fra autoriseringen av det. Følgende punkter bør vurderes:

- a) Det er viktig å atskille aktiviteter som krever samordning for å gjennomføre svindel, for eksempel plassering av kjøpsordre og bekreftelse på at varene er mottatt.
- b) Hvis det er fare for slik samordning, bør det utvikles kontrolltiltak som krever at to eller flere personer må involveres, og på den måte redusere muligheten for svindel.

8.1.5 Atskillelse av utviklings- og produksjonsutstyr

Det er viktig å skille mellom utviklings-, test- og produksjonsmiljøer for å sikre at man holder de involverte rollene fra hverandre. Reglene for overføring av programvare fra test til produksjon bør være definert og dokumentert.

Utviklings- og testaktivitet kan forårsake store problemer, for eksempel systemsvikt eller uønsket modifikasjon av filer og systemmiljøer. Graden av atskillelse mellom test-, drifts- og utviklingsmiljøer som er nødvendig for å forhindre driftsproblemer, bør derfor vurderes. Et lignende skille bør også etableres mellom utviklings- og testfunksjoner. I slike tilfeller er det behov for å opprettholde et kjent og stabilt miljø for å kunne foreta effektiv testing og forhindre at utviklere får utilbørlig tilgang.

I tilfeller der utviklings- og testpersonell har tilgang til produksjonssystemet og dets informasjon, kan de være i stand til å introdusere uautoriserte og utestet kodeverk eller endre driftsdata. I noen systemer kan denne muligheten misbrukes til å begå underslag eller introdusere utestet eller skadelig kodeverk. Utestet eller skadelig kode kan skape alvorlige driftsproblemer. Utviklere og testpersonell utgjør dessuten en trussel mot driftsdataenes konfidensialitet.

Utviklings- og testaktivitetene kan skape utilsiktede endringer i programvare og informasjon dersom de blir foretatt i det samme testmiljøet. Det er derfor ønskelig å skille utviklings-, test- og produksjonsmiljø for å redusere risikoen for utilsiktede endringer eller uautorisert tilgang til driftsprogramvare og forretningsopplysninger. Følgende sikringstiltak bør tas i betraktning:

- a) Programvare for utvikling og produksjon bør, der det er mulig, kjøres på forskjellige prosessorer eller i forskjellige domener eller filkataloger.
- b) Utvikling og testing bør adskilles der det er mulig.
- c) Programmeringsverktøy, kompilatorer, editorer og andre hjelpeprogrammer bør ikke være tilgjengelig fra produksjonssystemet hvis det ikke er nødvendig.
- d) Forskjellige påloggingsprosedyrer bør benyttes for produksjons- og testsystemene for å redusere faren for misforståelser. Brukerne bør oppfordres til å benytte ulike passord for disse systemene, og menyene bør vise egnede meldinger som angir hvilket system man befinner seg i.
- e) Utviklingspersonell bør ikke ha permanent administratortilgang til produksjonssystemer. Kontrollmekanismene bør sikre at passordene til administratorkontoer blir endret etter bruk.

8.1.6 Administrasjon utført av eksterne

Bruk av eksterne leverandører for å administrere informasjonssystem kan utgjøre en potensiell sikkerhetsrisiko, for eksempel kompromittering, ødeleggelse eller tap av data ved leverandørens installasjon. Disse risikoene bør utredes på forhånd, og passende sikringstiltak bør avtales med

leverandøren og innlemmes i kontrakten (se også 4.2.2 og 4.3 for veiledning angående outsourcingkontrakter og kontrakter med tredjepart som innebærer tilgang til organisasjonens IT-infrastruktur).

Spesielle punkter som det bør tas hensyn til, omfatter blant annet:

- a) behovet for å identifisere spesielt sensitive eller viktige applikasjoner som bør håndteres lokalt av sikkerhetsmessige årsaker;
- b) behovet for godkjenning fra applikasjonseierne;
- c) innvirkning på organisasjonens kontinuitetsplanlegging;
- d) hvilke sikkerhetsstandarder som skal spesifiseres, og hvordan overensstemmelse skal måles;
- e) fordeling av bestemte ansvarsoppgaver og prosedyrer for effektivt å overvåke all relevant sikkerhetsaktivitet;
- f) ansvar og prosedyrer for å rapportere og håndtere sikkerhetshendelser (se 8.1.3).

8.2 Systemplanlegging og akseptanse

Mål: Å redusere risikoen for systemfeil.

Forhåndsplanlegging og forberedelser er påkrevet for å sikre at tilstrekkelig kapasitet og ressurser er tilgjengelig.

Beregninger over fremtidige kapasitetsbehov bør utarbeides for å redusere faren for overbelastning av systemene. Driftskravene fra nye systemer bør kartlegges, dokumenteres og testes før de godkjennes og tas i bruk.

8.2.1 Kapasitetsplanlegging

Kapasitetsbehovene bør kontrolleres, og beregninger over fremtidige kapasitetsbehov bør foretas for å sikre at tilstrekkelig prosesseringskraft og lagringsplass er tilgjengelig. Disse beregningene bør ta høyde for nye forretnings- og systemkrav, så vel som organisasjonens nåværende og forventede fremtidige bruk av informasjonssystem.

Stormaskiner krever spesiell oppmerksomhet, fordi det er større kostnader og lengre leveringstid forbundet med anskaffelse av ny kapasitet. Ansvarlige for stormaskintjenester bør overvåke bruken av de viktigste systemressursene, herunder prosessorer, interne og eksterne datalagre, skrivere og annet periferutstyr og kommunikasjonssystemer. Man bør observere endringer i bruksmønster, spesielt i forbindelse med virksomhetens applikasjoner og verktøy for håndtering av informasjonssystemene.

Systemadministrator bør bruke denne informasjonen til å peke på og unngå potensielle flaskehalser som kan utgjøre en trussel mot systemsikkerhet eller brukertjenester, og planlegge hensiktsmessige tiltak.

8.2.2 Systemakseptanse

Akseptanskriterier for nye systemer, oppgraderinger og nye versjoner bør utarbeides, og relevante tester bør gjennomføres forut for akseptanse. Systemadministrator bør sørge for at krav og kriterier for akseptanse av nye systemer er klart definert, avtalt, dokumentert og testet. Følgende punkter bør vurderes:

- a) ytelses- og kapasitetskrav til systemet;
- b) prosedyrer for feilretting og omstart samt unntaksprosedyrer;
- c) forberedelse og testing av rutinemessige driftsprosedyrer i henhold til definerte standarder;
- d) etablert avtale om sikkerhetstiltak;
- e) effektive manuelle prosedyrer;
- f) ordninger for driftskontinuitet, som beskrevet i 11.1;
- g) garanti for at installasjon av et nytt system ikke vil påvirke eksisterende systemer, særlig i perioder med stor belastning, for eksempel i slutten av måneden;

- h) garanti for at man har vurdert virkningene av det nye systemet på den alminnelige sikkerheten i organisasjonen;
- i) opplæring i drift og bruk av nye systemer.

I forbindelse med større utviklingsprosjekt bør driftsfunksjonen og brukerne rådspørres på alle stadier i prosessen for å sikre at det planlagte systemet vil være effektivt i drift. Relevante tester bør utføres for å sikre at alle akseptansekrav er fullt ut tilfredsstillt.

8.3 Beskyttelse mot ødeleggende programvare

Mål: Å beskytte programvarens og informasjonens integritet.

Forholdsregler er nødvendig for å avdekke og beskytte mot ødeleggende programvare.

IT-infrastruktur er sårbar for ødeleggende programvare, for eksempel datavirus, nettverksormer, trojanske hester (se også 10.5.4) og logiske bomber. Brukerne bør gjøres oppmerksomme på farene ved uautorisert eller ødeleggende programvare, og der det er hensiktsmessig, bør IT-sjefen innføre spesielle tiltak for å avdekke og beskytte mot slik programvare. Det er særlig viktig at det tas forholdsregler for å avdekke og forhindre datavirus på personlige datamaskiner.

8.3.1 Viruskontroll

Det bør iverksettes tiltak for å avdekke og beskytte mot ødeleggende programvare og skape tilstrekkelig bevissthet hos sluttbrukerne. Virusforsvaret bør baseres på bevissthet om sikkerhet, hensiktsmessig systemtilgang og endringskontroll.

Følgende bør overveies:

- a) formelle retningslinjer som krever overholdelse av programvarelisenser og forbyr bruk av uautorisert programvare (se 12.1.2.2);
- b) formelle retningslinjer for å beskytte organisasjonen mot farene som er forbundet med å hente filer og programvare fra eller via eksterne nettverk eller på et hvilket som helst annet medium, og som spesifiserer hvilke beskyttelsestiltak som skal iverksettes (se også 10.5, særlig 10.5.4 og 10.5.5);
- c) installasjon og regelmessig oppdatering av antivirusprogrammer som gjennomgår maskin og datamedia, enten som et korrigerende tiltak eller på regelmessig basis;
- d) regelmessig gjennomgang av programvare og datainnhold i systemer som støtter kritiske produksjonsprosesser. Oppdages falske filer eller uautoriserte endringer, bør dette medføre formell undersøkelse;
- e) viruskontroll før bruk av alle filer på elektroniske media av ukjent eller uautorisert opprinnelse, og av filer som er mottatt over usikre nettverk;
- f) viruskontroll før bruk av alle vedlegg til e-post og alt nedlastet materiell. Denne kontrollen kan gjennomføres på ulike steder, for eksempel på e-postserveren, på sluttbrukers arbeidsstasjon, eller idet man går inn på organisasjonens nettverk;
- g) ledelsens ansvar og prosedyrer for å sikre virusbeskyttelse på systemene, opplæring i bruk av slik beskyttelse, rapportering og gjenoppretting etter virusangrep (se 6.3 og 8.1.3);
- h) hensiktsmessige kontinuitetsplaner for gjenoppretting etter virusangrep, herunder nødvendig sikkerhetskopiering av alle data og programvarepakker (se punkt 11);
- i) prosedyrer for å verifisere all informasjon angående ødeleggende programvare og sikre at varselmeldinger er pålitelige og etterrettelige. IT-sjefen bør forsikre seg om at kvalifiserte kilder, for eksempel vel ansatte tidsskrifter, pålitelige internettsteder eller produsenter av antivirusprogrammer, konsulteres for å skille mellom falske og ekte virus. Ansatte bør gjøres oppmerksom på problemet med falske virus og instrueres om hvordan de skal forholde seg når de mottar dem.

Disse kontrollrutinene er særlig viktige for nettverksservere som støtter et stort antall arbeidsstasjoner.

8.4 Administrative rutiner

Mål: Å opprettholde tilgjengelighet og integritet til IT-infrastruktur.

Det bør etableres rutiner som sikrer at avtalt strategi for sikkerhetskopiering følges opp (se 11.1). Disse rutineene bør omfatte sikkerhetskopiering av data, øvelser på gjenoppretting av data innenfor tidsfrister, loggføring av hendelser og feil og overvåking av datamiljøet dersom dette er hensiktsmessig.

8.4.1 Sikkerhetskopiering av data

Sikkerhetskopier av viktig programvare og data bør tas regelmessig. Tilfredsstillende utstyr bør være tilgjengelig for å sikre at all virksomhetskritisk informasjon og programvare kan gjenopprettes etter et eventuelt datasammenbrudd eller ved feil på datamedia. Reserveløsninger for individuelle systemer bør testes regelmessig for å sikre at de oppfyller kravene som stilles i organisasjonens kontinuitetsplan (se punkt 11). Følgende retningslinjer bør innføres:

- a) Et minstenivå av sikkerhetskopierte informasjon, sammen med nøyaktige og fullstendige opptegnelser over alle sikkerhetskopier og dokumenterte gjenopprettingsprosedyrer, bør lagres på et sted som ligger så langt unna at det ikke rammes av en eventuell katastrofe ved hovedinstallasjonen. Minst tre generasjoner eller sykluser av sikkerhetskopierte data for virksomhetskritiske applikasjoner bør oppbevares til enhver tid.
- b) Sikkerhetskopierte informasjon bør gis nødvendig fysisk og miljømessig beskyttelse (se kapittel 7) i samsvar med standardene som gjelder ved hovedinstallasjonen. Eksisterende kontroll av media ved hovedinstallasjonen bør utvides til også å gjelde lageret der sikkerhetskopiene oppbevares.
- c) Sikkerhetskopiene bør testes regelmessig for å sikre at de er til å stole på i en krisesituasjon.
- d) Gjenopprettingsprosedyrer bør gjennomgås og testes regelmessig for å sikre at de er effektive, og at de lar seg gjennomføre innenfor tidsfristene som er angitt i driftsprosedyrene for gjenoppretting.

Oppbevaringstiden for viktige virksomhetsdata, samt krav til arkivkopier for permanent oppbevaring (se 12.1.3) bør spesifiseres.

8.4.2 Operatørlogger

Driftsoperatører bør føre logg over arbeidet de utfører. I de tilfeller der det er formålstjenlig, bør operatørloggene inneholde:

- a) start- og stopptider for systemene;
- b) systemfeil og hvilke korrigerende tiltak som er iverksatt;
- c) bekreftelse på korrekt håndtering av datafiler og utdata fra systemene;
- d) navn på personen som har notert i loggen.

Operatørloggen bør gjennomgås regelmessig av uavhengige og sjekkes mot operatørrutinene.

8.4.3 Feillogging

Feil bør rapporteres og korrigerende tiltak iverksettes. Feil som blir rapportert av brukere i forbindelse med IT-infrastruktur, bør loggføres. Det bør foreligge klare regler for håndtering av rapporterte feil, herunder:

- a) gjennomgang av feillogger for å sikre at problemer er blitt løst på tilfredsstillende måte;
- b) gjennomgang av korrigerende tiltak for å sikre at kontrollrutinene ikke er brutt, og at tiltakene som ble iverksatt, er autorisert.

8.5 Nettverksadministrasjon

Mål: Å beskytte informasjon i nettverk og verne den underliggende infrastrukturen.

Sikkerhetsadministrasjon av nettverk som strekker seg over flere organisatoriske grenser, krever spesiell oppmerksomhet.

Ytterligere tiltak kan være påkrevd for å beskytte sensitive data som overføres via offentlige nettverk.

8.5.1 Sikringstiltak i nettverk

En rekke kontroller er nødvendige for å etablere og opprettholde sikkerheten i datanettverk. Nettverksadministrator bør iverksette tiltak for å sikre dataene i nettverkene og beskytte tilknyttede tjenester mot uautorisert tilgang. Spesielt bør følgende punkter vies oppmerksomhet:

- Der det er hensiktsmessig, bør driftsansvaret for nettverkene adskilles fra selve driften av datamaskinene (se 8.1.4).
- Ansvar og prosedyrer for administrasjon av fjerninstallert utstyr, herunder utstyr i brukerområder, bør etableres.
- Dersom det er nødvendig, bør spesielle sikringstiltak iverksettes for å beskytte konfidensialiteten og integriteten til data som overføres over offentlige nettverk, og for å beskytte tilknyttede systemer (se 9.4 og 10.3). Det kan også være nødvendig med spesielle tiltak for å sikre tilgjengelighet til nettverkstjenestene og de tilkoblede informasjonssystemene.
- Driftsadministrasjon bør koordineres nøye, både for å optimalisere tjenestene for organisasjonen, og for å påse at sikringstiltakene er konsistente i hele IT-infrastrukturen.

8.6 Sikker håndtering av datamedia

Mål: Å forhindre ødeleggelse av aktiva og avbrudd i organisasjonens aktiviteter.

Media bør kontrolleres og beskyttes fysisk.

Hensiktsmessige driftsprosedyrer bør innføres for å beskytte dokumenter, datamedia (bånd, disketter, kassetter), inn-/utdata og systemdokumentasjon mot ødeleggelse, tyveri og uautorisert tilgang.

8.6.1 Håndtering av flyttbare datamedia

Det bør foreligge prosedyrer for håndtering av flyttbare datamedia, for eksempel bånd, disketter, kassetter og utskrevne dokumenter. Følgende retningslinjer bør vurderes:

- Data som det ikke lenger er behov for, på media som skal fjernes fra organisasjonen, bør slettes.
- Autorisasjon bør kreves for alle datamedia som føres ut av organisasjonen, og fortegnelse bør føres over alle slike utførsler for å sikre revisjonsspor (se 8.7.2).
- Alle datamedia bør lagres i et sikkert og forsvarlig miljø i henhold til leverandørens spesifikasjoner.

Alle prosedyrer og autorisasjonsnivåer bør være entydig dokumentert.

8.6.2 Makulering av datamedia

Datamedia bør avhendes sikkert og forsvarlig når det ikke lenger er behov for dem. Følsom informasjon kan komme utenforstående i hende ved skjodesløs avhending av datamedia. Formelle prosedyrer for sikker avhending av datamedia bør utarbeides for å redusere denne risikoen. Følgende retningslinjer bør tas under overveielse:

- Media som inneholder sensitiv informasjon, bør lagres og avhendes på en sikker og forsvarlig måte, for eksempel brennes, strimles opp med makuleringsmaskin eller slettes for data, til bruk ved andre applikasjoner innenfor organisasjonen.

- b) Den følgende listen peker på materiale som krever sikker avhending:
 - 1) papirdokumenter;
 - 2) innspillinger av stemmer eller annet;
 - 3) blåpapir;
 - 4) utskrevne rapporter;
 - 5) engangsbånd til skrivere;
 - 6) magnetiske bånd;
 - 7) utskiftbare disker eller kassetter;
 - 8) optiske lagringsmedia (alle former, herunder alle distribusjonsmedia fra programvareprodusenter);
 - 9) programutskrifter;
 - 10) testdata;
 - 11) systemdokumentasjon.
- c) Det kan være enklere å samle inn alle datamedia som skal kastes, og destruere dem på forsvarlig måte, enn å forsøke å sortere ut det sensitive materialet.
- d) Mange organisasjoner tilbyr innsamling og avhending av papir, utstyr og media. Utvis varsomhet og velg en leverandør med tilfredsstillende kontroller og erfaring.
- e) Avhending av sensitivt materiale bør loggføres der det er mulig, for å bevare et revisjonsspor.

Når informasjon skal avhendes, bør man være klar over aggregeringseffekten, det vil si at en større mengde uklassifisert informasjon kan være mer sensitiv enn en liten mengde klassifisert informasjon.

8.6.3 Prosedyrer for håndtering av informasjon

Prosedyrer for håndtering og lagring av informasjon bør iverksettes for å hindre uautorisert innsyn eller misbruk. Prosedyrer bør utarbeides for å håndtere informasjon i samsvar med dens sikkerhetsklassifisering (se 5.2), både med hensyn til dokumenter, datasystemer, nettverk, bærbar datamaskiner, mobil kommunikasjon, post, talelagring (voice mail), muntlig kommunikasjon generelt, multimedia, posttjenester/utstyr, ved bruk av telefaksmaskiner og alt annet sensitive materiale, for eksempel blankosjekker og fakturaer. Følgende punkter bør behandles (se også 5.2 og 8.7.2):

- a) håndtering og merking av alle media [se også 8.7.2 a)];
- b) adgangsrestriksjoner for å identifisere uautorisert personell;
- c) vedlikehold av et formelt register over autoriserte mottakere av data;
- d) prosedyrer for å sikre at inndata er komplett, at behandlingen er fullført, og at godkjenning av utdata er innhentet;
- e) temporært lagrede data som venter på viderebehandling, bør beskyttes i samsvar med deres sensitivitet;
- f) lagring av media i et miljø som er i henhold til produsentens spesifikasjoner;
- g) distribusjon av data bør begrenses til et minimum;
- h) tydelig merking av alle kopier av data med navnet til den autoriserte mottakeren;
- i) regelmessig gjennomgang av distribusjonslister og lister over autoriserte mottakere.

8.6.4 Sikring av systemdokumentasjon

Systemdokumentasjon kan inneholde en mengde sensitiv informasjon, for eksempel beskrivelse av applikasjonsprosesser, prosedyrer, datastrukturer og autorisasjonsprosesser (se også 9.1). Følgende sikringstiltak bør innføres for å beskytte systemdokumentasjon mot uautorisert tilgang:

- a) Systemdokumentasjon bør lagres forsvarlig.
- b) Adgang til systemdokumentasjon bør begrenses og autoriseres av applikasjonseier.
- c) Systemdokumentasjon som lagres på offentlige nettverk, eller som overføres via offentlige nettverk, bør gis tilfredsstillende beskyttelse.

8.7 Utveksling av informasjon og programvare

Mål: Å forhindre tap, endring eller misbruk av informasjon som utveksles mellom organisasjoner.

Utteksling av informasjon og programvare mellom organisasjoner bør kontrolleres og være i samsvar med relevant lovgivning (se punkt 12).

Slik utveksling bør foretas på grunnlag av avtaler. Prosedyrer og standarder for å beskytte informasjon og media under forsendelsen bør utarbeides. Det bør også overveies hvilke sikkerhetsmessige forhold som er forbundet med utveksling av elektroniske data, elektronisk handel og elektronisk post, og hvilke krav som bør stilles til sikringstiltak.

8.7.1 Utvekslingsavtaler for data og programvare

Avtaler, som kan være av formell art, inklusive avtaler om deponering av programvare der dette er hensiktsmessig, bør utarbeides i forbindelse med utveksling av data og programvare (både elektronisk og manuell) mellom organisasjoner. Sikkerhetsinnholdet i en slik avtale bør gjenspeile den involverte forretningsinformasjonens følsomhet. Avtaler om sikkerhetsforhold bør spesifisere:

- a) ledelsens ansvar for å kontrollere og varsle sending, overføring og mottak;
- b) prosedyrer for å varsle sending, overføring og mottak;
- c) tekniske minimumsstandarder for pakking og overføring;
- d) standarder for identifisering av kuréer;
- e) forpliktelser og ansvar i tilfelle tap av data;
- f) bruk av avtalt merking for følsom eller kritisk informasjon, som sikrer at merkingen straks blir forstått, og at informasjonen får tilstrekkelig beskyttelse;
- g) eierskap til data og programvare samt ansvar for sikring av data, overensstemmelse med opphavsrettslover og lignende hensyn (se 12.1.2 og 12.1.4);
- h) tekniske standarder for skriving og lesing av data og programvare;
- i) spesialtiltak som er nødvendig for å beskytte sensitivt materiale, for eksempel krypteringsnøkler (se 10.3.5).

8.7.2 Sikring av informasjon i transitt

Informasjon kan være sårbar for uautorisert tilgang, misbruk eller ødeleggelse under fysisk transport, for eksempel når sendingen går via postverket eller budtjenester. Følgende tiltak bør derfor innføres for å sikre datamedia under transport mellom to steder:

- a) Pålitelig transport og kurértjeneste bør brukes. En liste over autoriserte kurértjenester bør avtales med ledelsen, og prosedyrer for å kontrollere kurérens identitet bør innføres.
- b) Pakkingen bør være tilstrekkelig til å beskytte innholdet mot alle former for fysisk skade som kan oppstå under transport, og bør være i henhold til produsentens spesifikasjoner.
- c) Der det er nødvendig, bør det innføres spesielle sikringstiltak for å beskytte følsom informasjon mot uautorisert innsyn eller endring. Det kan eksempelvis dreie seg om:
 - 1) bruk av låste containere;
 - 2) personlig leveranse;
 - 3) forseglet innpakking (som avslører eventuelle forsøk på å åpne forsendelsen);
 - 4) i unntakstilfeller: å dele enheten opp i mer enn én forsendelse og sende dem via forskjellige ruter;
 - 5) bruk av digitale signaturer og konfidensiell kryptering, se 10.3.

8.7.3 Sikkerhet ved elektronisk handel

Elektronisk handel kan innebære bruk av elektronisk datautveksling (EDI – electronic data interchange), elektronisk post og direkte tilkoblede transaksjoner via offentlige nettverk, for eksempel Internett. Elektronisk handel er utsatt for en rekke ulike trusler som kan føre til svindel, kontraktstvister og

avsløring eller endring av informasjon. Sikringstiltak bør innføres for å beskytte elektronisk handel mot disse truslene. En vurdering av sikkerheten ved elektronisk handel bør omfatte følgende:

- a) *Autentisering*: Hvilken garanti skal kjøper og selger kreve for hverandres påståtte identitet?
- b) *Autorisasjon*: Hvem er autorisert til å fastsette priser, utstede eller signere viktige handelsdokumenter? Hvordan vet handelspartneren dette?
- c) *Kontrakts- og anbudsprosesser*: Hvilke krav stilles til konfidensialitet, integritet og bevis for overføring og mottak av nøkkeldokumenter, og for ikke-benektelse av kontrakter?
- d) *Prisinformasjon*: Hvor stor tillit kan man ha til den annonserte prislstens integritet og sensitive rabattordningers konfidensialitet?
- e) *Ordretransaksjon*: Hvordan sikres konfidensialitet og integritet med hensyn til ordre, informasjon om betalings- og leveringsadresse og mottakskvittering?
- f) *Kredittkontroll*: Hvilke kontrolltiltak bør innføres for å undersøke betalingsinformasjonen som kunden oppgir?
- g) *Betaling*: Hva er den mest hensiktsmessige betalingsmåten for å forebygge svindel?
- h) *Bestilling*: Hvilke beskyttelsestiltak bør innføres for å opprettholde konfidensialitet og integritet med hensyn til ordreinformasjon, og for å unngå tap eller at ordrer registreres to ganger?
- i) *Erstatningsansvar*: Hvem skal bære risikoen for eventuelle urettmessige transaksjoner?

Mange av tiltakene ovenfor kan gjennomføres ved bruk av krypteringsteknikkene som er skissert i 10.3, og som er i overensstemmelse med lovfestede retningslinjer (se 12.1, særlig 12.1.6 om krypteringslovgivning).

Avtaler om elektronisk handel mellom handelspartnere bør støttes av en kontrakt som binder begge parter til de avtalte handelsbetingelsene, herunder også detaljene omkring autorisering [se b) over]. Det kan være behov for tilleggsavtaler med leverandører av informasjonstjenester og verdikjende nettverk.

Allment tilgjengelige handelssystemer bør offentliggjøre sine handelsbetingelser for kundene.

Serveren som benyttes til elektronisk handel, dens evne til å motstå dataangrep og de sikkerhetsmessige konsekvensene av nettverkstilkopling, bør vurderes. (se 9.4.7).

8.7.4 Sikkerhet ved bruk av elektronisk post

8.7.4.1 Sikkerhetsrisiko

Elektronisk post brukes til forretningskommunikasjon og erstatter tradisjonelle former for kommunikasjon som for eksempel brev. E-post skiller seg ut fra tradisjonelle former for forretningskommunikasjon med hensyn til blant annet hastighet, meldingsstruktur, grad av formalitet og sårbarhet overfor uautoriserte handlinger. Behovet for sikringstiltak for å motvirke truslene som følger ved bruk av e-post, bør vurderes. Mulige sikkerhetstrusler omfatter:

- a) faren for at meldinger skal fanges opp eller endres av utenforstående, eller at tjenesten gjøres utilgjengelig;
- b) faren for feil, for eksempel feiladressering eller feillevering, og tjenestens generelle pålitelighet og tilgjengelighet;
- c) konsekvensene av en endring i kommunikasjonsmedia på forretningsprosessen, for eksempel betydningen av økt overføringshastighet og følgene av at formelle henvendelser går fra person til person istedenfor fra firma til firma;
- d) juridiske betraktninger, for eksempel det potensielle behovet for bevis for opphav, forsendelse, levering og akseptanse;
- e) sikkerhetskonsekvensene av å offentliggjøre eksternt tilgjengelige adresselister;
- f) kontroll av fjernbrukeres tilgang til elektroniske postkontoer.

8.7.4.2 Retningslinjer for bruk av e-post

Organisasjonene bør utarbeide klare retningslinjer for bruk av e-post. Dette omfatter:

- a) angrep på e-post, for eksempel virus og oppfanging av meldinger;
- b) beskyttelse av e-postvedlegg;
- c) retningslinjer som forteller når man ikke skal bruke e-post;
- d) ansattes ansvar for å ikke kompromittere organisasjonen, for eksempel gjennom å sende e-post med krenkende eller sjikanøst innhold, eller bruk av e-post til uautoriserte innkjøp;
- e) bruk av krypteringsteknikker for å beskytte de elektroniske meldingenes konfidensialitet og integritet;
- f) lagring av meldinger som kan legges frem i tilfelle rettssak;
- g) ytterligere kontrollrutiner for å sjekke meldinger som ikke kan autentiseres.

8.7.5 Sikring av elektroniske kontorsystemer

Det bør utarbeides regler og retningslinjer for å begrense forretnings- og sikkerhetsrisikoen i forbindelse med elektroniske kontorsystemer. Slike systemer gir mulighet for raskere spredning og formidling av organisasjonens informasjon gjennom en kombinasjon av dokumenter, datamaskiner, bærbare datamaskiner, mobil kommunikasjon, post, talelagring (voice mail), muntlig kommunikasjon generelt, multimedia, posttjenester/utstyr og telefaksmaskiner.

Konsekvenser for sikkerhet og forretningsdrift ved sammenkobling av slikt utstyr omfatter:

- a) trusler mot informasjon i kontorsystemer, for eksempel innspilling av telefonsamtaler eller telefonmøter, konfidensialitet ved telefonsamtaler, oppbevaring av telefakser, åpning av post, fordeling av post;
- b) retningslinjer og hensiktsmessige kontrollrutiner for å administrere formidling av informasjon, for eksempel bruk av elektroniske oppslagstavler (se 9.1);
- c) behov for å utelukke visse kategorier av følsom virksomhetsinformasjon dersom informasjonssystemet ikke garanterer tilstrekkelig sikkerhetsnivå (se 5.2);
- d) behov for å begrense andres tilgang til utvalgte personers tidsplanleggere, for eksempel ansatte som jobber med sensitive prosjekter;
- e) systemets egnethet eller mangel på sådan, til å støtte applikasjoner, for eksempel overføring av bestillinger eller autorisasjoner;
- f) kategorier av ansatte, leverandører eller forretningspartnere som har tilgang til systemet, og hvilke steder systemet kan aksesseres fra (se 4.2);
- g) behovet for å begrense spesielle fasiliteter til utvalgte brukerkategorier;
- h) behovet for å identifisere brukernes status, for eksempel om de er ansatt i organisasjonen eller hos leverandøren, i organisasjonens adresselister slik at andre brukere har tilgang til denne informasjonen;
- i) retningslinjer for lagring og sikkerhetskopiering av informasjon som ligger i systemet (se 12.1.3 og 8.4.1);
- j) krav til reserveløsninger og kriseplaner (se 11.1).

8.7.6 Offentlig tilgjengelige systemer

Forholdsregler bør tas for å beskytte integriteten til elektronisk publisert informasjon og hindre uautoriserte endringer som kan skade omdømmet til organisasjonen som står bak. Informasjon på et offentlig tilgjengelig system, for eksempel på en nettsjerver som er tilgjengelig via Internett, er i enkelte tilfeller underlagt lover, regler og forskrifter i rettsområdet der den er plassert, eller der handel finner sted. Det bør derfor etableres en formell autorisasjonsprosess før informasjon gjøres offentlig tilgjengelig.

Programvare, data og annen informasjon som krever høy grad av integritet, og som gjøres tilgjengelig på et offentlig tilgjengelig system, bør beskyttes av hensiktsmessige mekanismer, for eksempel digitale

signaturer (se 10.3.3). Elektroniske publikasjonssystemer, særlig de som tillater tilbakemelding og direkte innskrevet informasjon, bør overvåkes nøye slik at:

- a) informasjonen er innhentet i samsvar med lovgivning om databeskyttelse (se 12.1.4);
- b) inndata som føres inn i og behandles av publikasjonssystemet blir behandlet fullstendig, nøyaktig og til rett tid;
- c) sensitiv informasjon blir beskyttet under innsamlingsfasen og når den lagres;
- d) tilgang til publikasjonssystemet ikke gir utilsiktet tilgang til nettverk som det er koblet opp mot.

8.7.7 Andre former for utveksling av informasjon

Prosedyrer og kontrollrutiner bør etableres for å beskytte utveksling av informasjon, som for eksempel tale, telefaks- og videokommunikasjon. Informasjon kan bli kompromittert ved uaktsomhet eller manglende retningslinjer og prosedyrer ved bruk av slike kommunikasjonsmetoder, for eksempel ved at man blir overhørt mens man snakker i mobiltelefon på et offentlig sted, at beskjeder på telefonsvarer blir overhørt, at noen får uautorisert tilgang til oppringbare talelagringssystemer eller at man ved et uhell sender telefaks til feil person ved bruk av telefaksmaskin.

Driften av virksomheten kan bli avbrutt og informasjon kompromittert dersom kommunikasjonsutstyr svikter, blir overbelastet eller forstyrret (se 7.2 og punkt 11). Informasjon kan også bli kompromittert dersom den blir aksessert av uautoriserte brukere (se punkt 9).

Det bør foreligge tydelige retningslinjer for hvilke prosedyrer de ansatte skal følge ved bruk av talelagring (voice mail), telefaks og videokommunikasjon. Disse bør:

- a) minne de ansatte på at de må ta passende forholdsregler, for eksempel mot å avsløre følsom informasjon, ved å unngå at telefonsamtaler blir avlyttet eller overhørt:
 - 1) av mennesker i deres umiddelbare nærhet, særlig ved bruk av mobiltelefon;
 - 2) ved telefonavlytting og andre former for tjuvlytting gjennom fysisk adgang til telefonapparatet eller telefonlinjen, eller ved hjelp av frekvensskannere avlytte analoge mobiltelefoner;
 - 3) mennesker i mottakers nærhet;
- b) minne de ansatte på at de må unngå konfidensielle samtaler på offentlige steder eller åpne kontorer og møterom med tynne vegger;
- c) minne de ansatte på at de ikke må etterlate seg beskjeder på telefonsvarere, ettersom beskjeder kan bli avspilt av uautoriserte personer, lagret på et fellessystem eller lagret feil som følge av at man har slått feil nummer;
- d) gjøre de ansatte oppmerksomme på problemene ved bruk av telefaksmaskin:
 - 1) uautorisert tilgang til innebygd minne for å finne igjen meldinger;
 - 2) bevisst eller tilfeldig programmering av maskinen til å sende meldinger til bestemte nummer;
 - 3) faren for å sende dokumenter og meldinger til feil nummer, enten ved feiltasting eller ved bruk av feil lagret nummer.

9 Tilgangskontroll

9.1 Virksomhetskrav til tilgangskontroll

Mål: Å kontrollere tilgang til informasjon.

Tilgang til informasjon og forretningsprosesser bør kontrolleres på grunnlag av virksomhets- og sikkerhetsbehov.

Tilgangskontrollen bør avspeile organisasjonens retningslinjer for autorisasjon til og distribusjon av informasjon.

9.1.1 Retningslinjer for tilgangskontroll

9.1.1.1 Politikk og virksomhetskrav

Virksomhetskrav til tilgangskontroll bør defineres og dokumenteres. Regler for tilgangskontroll og rettigheter for hver enkelt bruker eller brukergruppe bør være tydelig beskrevet i retningslinjene for tilgangskontroll. Brukere og tjenesteleverandører bør få en klar forståelse av organisasjonens krav til tilgangskontroll.

Retningslinjene bør ta hensyn til følgende:

- sikringskravene til de enkelte applikasjonene;
- identifisering av all informasjon i tilknytning til virksomhetsapplikasjoner;
- retningslinjer for spredning og autorisasjon av informasjon, for eksempel "need to know"-prinsippet, og bruk av sikkerhetsnivåer og klassifisering av informasjon;
- samsvar mellom tilgangskontroll og retningslinjer for klassifisering av informasjon i ulike systemer og nettverk;
- relevante lovfestede og kontraktmessige krav om å beskytte tilgang til data eller tjenester (se punkt 12);
- standardiserte og felles tilgangsprofiler for vanlige jobbkategorier;
- administrasjon av tilgangsrettigheter i et distribuert nettverksmiljø som anerkjenner alle typer tilgjengelige forbindelser.

9.1.1.2 Regler for tilgangskontroll

Ved spesifisering av regler for tilgangskontroll bør det tas hensyn til følgende:

- differensiering mellom regler som alltid bør håndheves, og regler som er valgfrie eller betinget;
- utarbeidelse av regler basert på prinsippet om at det «generelt er forbudt med mindre det er uttrykkelig tillatt» heller enn den svakere regelen at det «generelt er tillatt med mindre det er uttrykkelig forbudt»;
- endringer i merking av informasjon (se 5.2) som iverksettes automatisk av informasjonssystemet, og endringer som iverksettes av brukeren etter skjønn;
- endringer i brukertilgang som iverksettes automatisk av informasjonssystemet, og endringer som iverksettes av en administrator;
- regler som krever godkjenning av administrator eller andre før de iverksettes, og regler som ikke gjør det.

9.2 Administrasjon av brukertilgang

Mål: Å hindre uautorisert tilgang til informasjonssystemer.

Formelle prosedyrer bør foreligge for å kontrollere tildeling av tilgangsrettigheter til informasjonssystemer og tjenester.

Prosedyrene bør dekke alle stadier i brukertilgangens livssyklus, fra registrering av nye brukere til sletting av brukere som ikke lenger bør ha tilgang til informasjonssystemene og –tjenestene. I de tilfeller det er aktuelt, bør det vies spesiell oppmerksomhet til behovet for å begrense utdelingen av privilegerte tilgangsrettigheter som gir brukere rett til å overstyre systemkontroller.

9.2.1 Registrering av brukere

Det bør foreligge formelle prosedyrer for registrering og sletting av tilgang til alle flerbrukersystemer og -tjenester.

Tilgang til flerbrukertjenester bør kontrolleres gjennom en formell prosess for brukerregistrering som sikrer følgende:

- a) at det benyttes unike brukeridentiteter, slik at brukere kan knyttes til og gjøres ansvarlige for det de foretar seg. Bruk av gruppe-id bør bare tillates der arbeidets art tilsier det;
- b) at det kontrolleres at brukeren har autorisasjon fra systemeier til å bruke informasjonssystemet eller -tjenesten. Separat godkjenning av tilgangsrettigheter fra ledelsen kan også være nødvendig;
- c) at det kontrolleres at tilgangsnivået som gis, er i overensstemmelse med tjenstlige behov (se 9.1), og i samsvar med organisasjonens sikkerhetspolitikk, dvs. ikke kompromitterer prinsippet om arbeidsdeling (se 8.1.4);
- d) at brukerne mottar skriftlig bekreftelse på sine tilgangsrettigheter;
- e) at det kreves en signert erklæring fra brukerne som bekreftelse på at de forstår betingelsene for tilgang;
- f) at tjenesteleverandørene ikke gir tilgang før autorisasjonsprosedyrene er gjennomført;
- g) at det opprettes et formelt register over alle personer som har tilgang til tjenesten;
- h) at tilgangsrettighetene til brukere som har byttet jobb eller forlatt organisasjonen, endres umiddelbart;
- i) at det foretas regelmessig gjennomgang og sletting av overflødige brukeridentiteter og kontoer;
- j) at overflødige brukeridentiteter ikke overføres til andre brukere.

Det bør også vurderes å inkludere avsnitt i ansettelses- og tjenestekontrakter som spesifiserer sanksjoner dersom egne eller tjenesteyters ansatte forsøker å få tilgang uten autorisasjon (se også 6.1.4 og 6.3.5).

9.2.2 Administrasjon av rettigheter

Tildeling og bruk av spesielle privilegier (alle funksjoner eller fasiliteter i et flerbrukersystem som setter brukere i stand til å overstyre system- eller applikasjonskontroller) bør begrenses og kontrolleres. Uhensiktsmessig bruk av systemprivilegier viser seg ofte å være en vesentlig faktor til den sviktende sikkerheten i informasjonssystemer som har hatt innbrudd.

Flerbrukersystemer som krever beskyttelse mot uautorisert tilgang, bør kontrollere tildelingen av privilegier gjennom en formell autorisasjonsprosess. Følgende tiltak bør vurderes:

- a) Kartlegging av privilegiene som er knyttet til hvert enkelt systemprodukt, for eksempel operativsystem, systemer for databaseadministrasjon og de enkelte applikasjonene, samt hvilke kategorier av ansatte som bør tildeles disse privilegiene.
- b) Tildeling av privilegier til enkeltindivider på grunnlag av behov og på «gang-for-gang»-basis, dvs. tildeling av det minimum av privilegier som kreves for deres funksjonelle rolle, og bare ved behov;
- c) Vedlikeholde en autorisasjonsprosess og et register over alle tildelte privilegier. Privilegier bør ikke tildeles uten at autorisasjonsprosessen er fullstendig.
- d) Fremme utvikling og bruk av systemrutiner for å unngå å tildele privilegier til brukere.
- e) Privilegiene bør tildeles andre brukeridentiteter enn dem brukerne benytter til sine vanlige arbeidsoppgaver.

9.2.3 Administrasjon av brukerpassord

Passord er en vanlig metode for å verifisere en brukers autorisasjon til å bruke et informasjonssystem eller en -tjeneste. Tildelingen av passord bør styres av en formell administrasjonsprosess som omfatter følgende:

- a) Krav om at brukere undertegner en erklæring om å holde personlige passord hemmelig og gruppepassord utelukkende innenfor arbeidsgruppen (dette kan inkluderes i betingelser og vilkår for ansettelse, se 6.1.4).
- b) Prosedyre for å sikre at brukere i de tilfeller der de har ansvar for å vedlikeholde sine egne passord, blir utstyrt med et sikkert, midlertidig passord som de er nødt til å endre ved første gangs

bruk. Midlertidige passord som utleveres når brukere har glemt passordet sitt, bør bare gis etter en sikker identifikasjon av brukeren.

- c) Prosedyre for å sikre at midlertidige passord utleveres brukeren på en sikker måte. Overlevering via en tredjepart eller via ubeskyttet (klartekst) e-post bør unngås. Brukerne bør bekrefte mottagelse av passordet.

Passord bør aldri lagres på datasystemet i ubeskyttet form (se 9.5.4).

Andre teknologier for brukeridentifikasjon og autentisering, som biometri, for eksempel fingeravtrykk eller verifisert signatur, og bruk av fysiske enheter, for eksempel smartkort, er tilgjengelig og bør vurderes dersom det er hensiktsmessig.

9.2.4 Gjennomgang av brukers tilgangsrettigheter

For å opprettholde effektiv kontroll over tilgang til data og informasjonstjenester bør det etableres en formell prosedyre for å gjennomgå brukernes tilgangsrettigheter, slik at:

- a) brukernes tilgangsrettigheter gjennomgås med jevne mellomrom (6 måneders intervaller anbefales) og etter endringer (se 9.2.1);
- b) autorisasjoner for spesielt privilegerte tilgangsrettigheter (se 9.2.2) gjennomgås med kortere mellomrom. Kvartalsvis gjennomgang anbefales;
- c) tildeling av privilegier kontrolleres med regelmessige mellomrom for å påse at ingen har tilegnet seg uautoriserte privilegier.

9.3 Brukerens ansvar

Mål: Å forhindre uautorisert brukertilgang.

Samarbeid fra brukernes side er avgjørende for effektiv informasjonssikkerhet.

Brukerne bør gjøres oppmerksomme på sitt ansvar for å vedlikeholde effektiv tilgangskontroll, særlig med hensyn til bruk av passord og sikring av informasjonssystemet.

9.3.1 Bruk av passord

Brukere bør følge god sikkerhetspraksis ved valg og bruk av passord.

Passord er en metode for å bekrefte brukerens identitet og dermed fastslå tilgangsrettigheter til informasjonssystemer eller -tjenester. Alle brukere bør rådes til å:

- a) holde passord hemmelige;
- b) unngå å skrive ned passord på papir med mindre det kan oppbevares trygt;
- c) endre passord når det er indikasjoner på at systemet eller passordet er blitt misbrukt;
- d) velg gode passord med en minimumslengde på 6 tegn som:
 - 1) er lette å huske;
 - 2) ikke er basert på noe andre lett kan gjette seg til, eller personrelatert informasjon, slik som navn, telefonnummer og fødselsdag, osv;
 - 3) unngår flere etterfølgende like tegn, og passord med bare numeriske eller alfabetiske tegn;
- e) bytt passord med jevne mellomrom eller basert på antall pålogginger (passord for privilegerte kontoer bør endres oftere enn vanlige passord), og unngå gjenbruk eller resirkulering av gamle passord;
- f) bytt midlertidig passord ved første pålogging;
- g) unngå å inkludere passord i automatiske påloggingsprosedyrer, for eksempel lagret i en makro eller knyttet til en funksjonstast;
- h) aldri låne bort passordet til andre.

Hvis brukere trenger tilgang til flere tjenester eller plattformer hvor det er behov for å ha flere passord, bør de rådes til å bruke ett enkelt, kvalitetsmessig godt passord [se 9.3.1 d)] for alle tjenestene, som gir tilfredsstillende beskyttelse av lagrede passord.

9.3.2 Ubevoktet brukerutstyr

Brukerne bør forsikre seg om at ubevoktet utstyr er beskyttet på en tilfredsstillende måte. Utstyr som er installert i brukerområder, for eksempel arbeidsstasjoner og filtjenere, kan kreve spesiell beskyttelse mot uautorisert tilgang når de står ubevoktet over lengre tid. Alle brukere og leverandører bør gjøres oppmerksomme på sikkerhetskravene og prosedyrene for å beskytte ubevoktet utstyr, og på ansvaret for å iverksette slik beskyttelse. Brukerne bør rådes til å:

- avslutte aktive sesjoner når de er ferdig, med mindre de kan beskyttes ved hjelp av tilfredsstillende låsmekanismer, for eksempel passordbeskyttet skjermsparer;
- logge av hovedmaskinen når sesjonen er over (dvs. ikke bare skru av pc-en eller terminalen);
- sikre pc-er eller terminaler mot uautorisert bruk ved hjelp av lås eller lignende kontroller, for eksempel passord, når de ikke er i bruk.

9.4 Tilgangskontroll i nettverk

Mål: Å beskytte av nettverkstjenester.

Tilgang til både interne og eksterne nettverkstjenester bør kontrolleres.

Dette er nødvendig for å sikre at brukere som har tilgang til nettverk og nettverkstjenester, ikke kompromitterer disse nettverkstjenestenes sikkerhet. Kontrollen bør omfatte:

- hensiktsmessig grensesnitt mellom organisasjonens nettverk og nettverk eid av andre bedrifter eller offentlige nettverk;
- tilfredsstillende autentiseringsmekanismer for brukere og utstyr;
- kontroll av brukertilgang til informasjonstjenestene.

9.4.1 Retningslinjer for bruk av nettverkstjenester

Usikrede forbindelser til nettverkstjenester kan få konsekvenser for hele organisasjonen. Brukerne bør bare gis direkte tilgang til de tjenestene de er uttrykkelig autorisert til å bruke. Denne kontrollen er spesielt viktig for nettverksforbindelser til sensitive eller virksomhetskritiske applikasjoner, og for brukere i høyrisikoområder, for eksempel offentlige og eksterne områder som er utenfor organisasjonens sikkerhetsadministrasjon og kontroll.

Retningslinjer bør utarbeides i forbindelse med bruk av nettverk og nettverkstjenester. Regelverket bør ta hensyn til:

- hvilke nettverk og nettverkstjenester som det er tillatt å benytte;
- autorisasjonsprosedyrene for å avgjøre hvem som har tilgang til hvilke nettverk og nettverkstjenester;
- kontrollmekanismer og prosedyrer for å beskytte tilgangen til nettverksforbindelser og nettverkstjenester.

Disse retningslinjene bør være i overensstemmelse med organisasjonens retningslinjer for tilgangskontroll (se 9.1).

9.4.2 Tvungen kommunikasjonsvei

Forbindelsen mellom brukerterminalen og informasjonstjenesten bør kontrolleres. Nettverkene er utformet for å skape størst mulig rom for deling av ressurser og fleksibilitet i ruting. Disse egenskapene åpner imidlertid for uautorisert tilgang til virksomhetsapplikasjoner og uautorisert bruk av IT-utstyr. Denne risikoen kan reduseres ved å etablere kontroller som begrenser kommunikasjonsveiene mellom en

brukerterminal og informasjonstjenestene som brukeren har tilgang til, for eksempel ved å skape en tvungen kommunikasjonsvei.

Hensikten med en slik tvungen kommunikasjonsvei er å hindre brukere i å velge kommunikasjonsveier utenom den ruten mellom brukerterminalen og tjenestene som brukeren har autorisert tilgang til.

Dette krever vanligvis etablering av en rekke sikringstiltak på ulike punkter langs kommunikasjonsveien. Prinsippet er å begrense veivalgene ved hvert punkt i nettverket gjennom forhåndsdefinerte valg. Eksempler på dette er:

- a) bruk av faste linjer eller telefonnummer;
- b) automatisk kopling mellom porter og bestemte applikasjonssystemer eller sikre nettverksporter;
- c) begrensning av meny- og undermenyvalg for individuelle brukere;
- d) sperring mot ubegrenset nettverksstrefing;
- e) innføring av spesielle applikasjonssystemer og/eller sikkerhetsporter for eksterne nettverksbrukere;
- f) aktiv kontroll av tillatt avsender- og mottakerkommunikasjon via sikre porter, for eksempel brannmurer;
- g) begrensning av nettverkstilgang ved å etablere separate logiske domener, for eksempel virtuelle private nettverk for brukergrupper innenfor organisasjonen (se 9.4.6).

Kravene til tvungen kommunikasjonsvei bør være basert på organisasjonens retningslinjer for tilgangskontroll (se 9.1).

9.4.3 Brukerautentisering av eksterne forbindelser

Eksterne forbindelser medfører en fare for uautorisert tilgang til virksomhetsinformasjon, for eksempel tilgang ved hjelp av oppringt samband. Tilgang for eksterne brukere bør derfor autentiseres. Det finnes ulike typer av autentiseringsmetoder, noen av dem gir større beskyttelse enn andre. For eksempel kan metoder som baserer seg på bruk av kryptografiske teknikker, gi sterk autentisering. Det er viktig å avgjøre hvilket beskyttelsesnivå som kreves ut fra en risikovurdering. Dette er avgjørende for å velge en hensiktsmessig autentiseringsmetode.

Autentisering av fjernbrukere kan gjøres for eksempel ved hjelp av kryptografisk baserte teknikker, fysiske enheter eller et spørsmål-/svarsystem. Bruk av dedikerte, private linjer eller kontroll av brukers nettverksadresse kan gi ytterligere forsikring om kilden til forbindelsen.

Tilbakeringingsprosedyrer og kontroller, for eksempel ved bruk av tilbakeringingsmodem, kan gi beskyttelse mot uautorisert og uønsket oppkobling mot virksomhetens IT-infrastruktur. Denne typen tiltak autentiserer brukere som forsøker å opprette forbindelse til organisasjonens nettverk fra et sted utenfor organisasjonens lokaliteter. Dersom organisasjonen bruker dette tiltaket, bør den ikke benytte nettverkstjenester som omfatter viderekobling av samtaler, eller i så fall bør den koble fra disse funksjonene for å unngå sårbarheter som er forbundet med viderekobling av samtaler. Det er også viktig at prosessen for tilbakeringing inkluderer en faktisk nedkopling av teleforbindelsen fra organisasjonens side. Ellers kan fjernbrukeren holde linjen åpen og late som om verifikasjon av tilbakeringing har funnet sted. Prosedyrer for tilbakeringing med tilhørende tiltak bør testes grundig for å unngå denne muligheten.

9.4.4 Nodeautentisering

Et system for automatisk tilkobling til eksterne datamaskiner kan gi muligheter for uautorisert tilgang til forretningsapplikasjoner. Forbindelser med eksterne informasjonssystemer bør derfor autentiseres. Dette er særlig viktig hvis forbindelsen bruker et nettverk som er utenfor kontrollen til organisasjonens sikkerhetsledelse. Noen eksempler på autentisering og hvordan det kan gjøres, er gitt i punkt 9.4.3 ovenfor.

Nodeautentisering kan være en alternativ metode for å autentisere grupper av fjernbrukere når de er tilkoblet et sikkert, delt informasjonssystem (se 9.4.3).

9.4.5 Beskyttelse av porter for fjerndiagnose

Tilgang til diagnoseporter bør gis tilfredsstillende beskyttelse. Mange datamaskiner og kommunikasjonssystemer er installert med en oppringbar diagnosefunksjon til bruk for vedlikeholdspersonell. Dersom disse portene er ubeskyttet, kan de åpne for uautorisert tilgang. De bør derfor beskyttes av tilfredsstillende sikringsmekanismer, eksempelvis nøkkellås og en prosedyre for å sikre at de bare er tilgjengelig etter avtale mellom IT-ansvarlig og personell hos maskinvare-/programvareleverandøren som har behov for slik tilgang.

9.4.6 Segmentering av nettverk

Datanettverk blir i stadig større grad utvidet på tvers av tradisjonelle organisasjonsgrenser når virksomhetene inngår samarbeidsavtaler som krever sammenkobling eller deling av IT-ressurser og nettverksutstyr. Slike utvidelser kan øke risikoen for uautorisert tilgang til allerede eksisterende informasjonssystemer som benytter nettverket. Noen av disse systemene vil kanskje også trenge beskyttelse mot andre nettverksbrukere, fordi de er sensitive eller virksomhetskritiske. I slike tilfeller vil det være tilrådelig å innføre kontroller i nettverket for å skille mellom grupper av informasjonstjenester, brukere og informasjonssystemer.

En metode for å kontrollere sikkerheten i store nettverk er å dele dem opp i separate logiske nettverksdomener, for eksempel organisasjonens interne og eksterne nettverksdomener, som hver er beskyttet av definerte forsvarsverker. Slike forsvarsverker kan opprettes ved å installere en sikker port mellom de to domenene. Denne porten bør utformes slik at den filtrerer trafikken mellom de ulike domenene (se 9.4.7 og 9.4.8) og sperrer for uautorisert tilgang i samsvar med organisasjonens retningslinjer for tilgangskontroll (se 9.1). Ett eksempel på nettverksporter av denne typen er det man gjerne kaller en brannmur.

Kriteriene for å dele opp nettverk i domener bør være basert på organisasjonens tilgangsbehov og retningslinjer for tilgangskontroll (se 9.1), og de bør også ta hensyn til kostnader og konsekvenser for ytelse ved innføring av egnet nettverksruting eller portteknologi (se 9.4.7 og 9.4.8).

9.4.7 Kontroll av oppkobling i nettverk

Organisasjonens retningslinjer for delte nettverk, særlig de som strekker seg over organisasjonsgrenser, kan kreve at det innføres spesielle sikringstiltak for å begrense brukernes oppkoblingsmuligheter. Slike kontroller kan iverksettes ved hjelp av nettverksporter som filtrerer trafikken i henhold til predefinerte tabeller eller regler. Begrensningene som iverksettes, bør være basert på organisasjonens retningslinjer for tilgangskontroll og kravene til virksomhetsapplikasjonene (se 9.1), og de bør vedlikeholdes og oppdateres deretter.

Eksempler på applikasjoner der begrensninger bør gjelde er:

- a) elektronisk post
- b) énveis filoverføring
- c) toveis filoverføring
- d) interaktiv tilgang:
- e) nettverkstilgang knyttet til dato og klokkeslett.

9.4.8 Sikring av nettverksruting

Delte nettverk, særlig de som strekker seg ut over organisasjonens grenser, kan kreve at det etableres nettverksruting for å sikre at dataforbindelser og informasjonsstrømmer ikke bryter med retningslinjene for tilgang til virksomhetsapplikasjonene (se 9.1). Denne kontrollen er ofte avgjørende for nettverk som deles med tredjeparts (ikke organisasjonens) brukere.

Rutingkontroller bør være basert på sikre kontrollmekanismer for avsender- og mottakeradresser. Oversetting av nettverksadresser (NAT - Network Address Translation) er også en nyttig mekanisme for å isolere nettverk og hindre ruter i å spre seg fra den ene organisasjonens nettverk til en annen

organisasjons nettverk. Disse kontrollene kan innføres i programvare eller maskinvare. De som iverksetter slike tiltak, bør vite i hvor stor grad de ulike mekanismene er dekkende.

9.4.9 Sikring av nettverkstjenester

Et stort antall offentlige og private nettverkstjenester er tilgjengelige, og noen av dem tilbyr verdiknede tjenester. Nettverkstjenester kan ha unike eller komplekse sikkerhetsløsninger. Organisasjoner som bruker nettverkstjenester, bør forsikre seg om at tjenesteleverandøren gir en klar beskrivelse av sikkerhetsløsningene for alle tjenestene som brukes.

9.5 Tilgangskontroll for informasjonssystemene

Mål: Å forhindre uautorisert tilgang til informasjonssystemene.

Sikringstiltak på operativsystemnivå bør benyttes for å begrense tilgangen til IT-ressurser. Disse sikringstiltakene bør kunne:

- a) identifisere og verifisere identiteten og, hvis nødvendig, terminalen eller plasseringen til hver enkelt autorisert bruker;
- b) loggføre vellykkede og mislykkede systemtilganger;
- c) sørge for hensiktsmessige autorisasjonsmetoder. Dersom et system for passordadministrasjon benyttes, bør kvaliteten på passordene sikres (se 9.3.1);
- d) begrense oppkoblingstiden for brukere, der det er nødvendig.

Andre metoder for tilgangskontroll, for eksempel spørsmål/svar, er også tilgjengelig dersom det kan forsvares i forhold til virksomhetsrisikoen.

9.5.1 Automatisk identifisering av terminal

Automatisk identifisering av terminal bør vurderes for å autentisere forbindelser til bestemte steder og til bærbar utstyr. Automatisk terminalidentifikasjon er en teknikk som kan brukes dersom det er viktig at sesjonen bare kan startes opp fra ett bestemt sted eller én bestemt dataterminal. En identifikator i eller koblet til terminalen brukes for å indikere hvorvidt denne bestemte terminalen har tillatelse til å initiere eller motta bestemte transaksjoner. Det kan være nødvendig å installere fysisk beskyttelse av terminalen for å oppnå tilfredsstillende sikkerhet for terminalidentifikatoren. En rekke andre teknikker kan også benyttes for å autentisere brukere (se 9.4.3).

9.5.2 Påloggingsprosedyre

Tilgang til informasjonstjenester bør skje gjennom en sikker påloggingsprosess. Prosedyren for å logge seg på et datasystem bør utformes slik at den reduserer muligheten for uautorisert tilgang. Påloggingsprosedyren bør derfor avsløre så lite informasjon om systemet som mulig for å forhindre at uautoriserte brukere får unødig assistanse. En god påloggingsprosedyre bør:

- a) ikke vise informasjon om systemet eller applikasjonene før påloggingsprosedyren er komplett og vellykket;
- b) vise en advarsel om at bare autoriserte brukere har tilgang til datamaskinen;
- c) ikke gi hjelpetekster som kan hjelpe uautoriserte brukere;
- d) godkjenne påloggingen først etter at alle inndata er registrert. Dersom en feilsituasjon oppstår, bør systemet ikke avsløre hvilken del av informasjonen som er korrekt eller uriktig;
- e) begrense antall mislykkede påloggingsforsøk som er tillatt (tre forsøk anbefales) og vurdere:
 - 1) loggføring av mislykkede forsøk
 - 2) innføring av en tidsforsinkelse før ytterligere påloggingsforsøk kan foretas, eller avvise ytterligere forsøk med mindre spesiell autorisasjon innhentes;
 - 3) koble fra forbindelsen;

- f) begrense maksimums- og minimumstidene som er tillatt for en påloggingsprosedyre. Hvis denne grensen overskrides, bør systemet avbryte påloggingen;
- g) Vise følgende informasjon etter en vellykket pålogging:
 - 1) dato og klokkeslett for forrige vellykkede pålogging
 - 2) informasjon om eventuelle mislykkede påloggingsforsøk siden forrige vellykkede pålogging.

9.5.3 Brukeridentitet og autentisering

Alle brukere (også teknisk støttepersonell som for eksempel operatører, nettverksadministratorer, systemprogrammerere og databaseadministratorer) bør ha et unikt identifikasjonsnavn (brukeridentitet) til personlig bruk for å sikre at aktiviteter i ettertid kan spores tilbake til én bestemt person. Brukeridentiteten bør ikke gi noen indikasjon om hvilke privilegier bruker har (se 9.2.2), for eksempel leder, systemadministrator eller lignende.

I unntakstilfeller der det er en klar virksomhetsmessig fordel, kan man benytte delt brukeridentitet for en gruppe av brukere eller en bestemt jobb. I slike tilfeller bør det foreligge dokumentert godkjenning fra ledelsen. Ytterligere kontrolltiltak kan være nødvendig for å sikre sporbarhet.

Det finnes en rekke ulike autentiseringsprosedyrer som kan benyttes for å bekrefte en brukers påståtte identitet. Passord (se også 9.3.1 og under) er en utbredt metode for å sikre identifikasjon og autentisering (I og A), basert på fortrolig informasjon som bare brukeren kjenner til. Det samme kan oppnås ved bruk av kryptografiske metoder og autentiseringsprotokoller.

Gjenstander som minnebrikker eller smartkort som er i brukerens besittelse, kan også brukes til I og A. Biometriske autentiseringsteknologier som baserer seg på unike kjennetegn eller egenskaper ved den enkelte person, kan også benyttes for å autentisere personens identitet. En kombinasjon av teknikker og mekanismer som er knyttet sammen på en sikker måte, vil gi sterkere autentisering.

9.5.4 System for passordadministrasjon

Passord er en av de viktigste metodene for å bekrefte en brukers identitet og derigjennom styre tilgangsrrettigheter til en informasjonstjeneste. Systemer for passordadministrasjon bør gi en effektiv, interaktiv mulighet som sikrer kvaliteten på passordene (se 9.3.1 for veiledning om bruk av passord).

Noen applikasjoner krever at brukernes passord blir tildelt av en uavhengig instans. I de fleste tilfeller blir passordene valgt og vedlikeholdt av brukerne selv.

Et godt system for passordadministrasjon bør:

- a) stille krav om bruk av individuelle passord for å sikre sporbarhet;
- b) hvis mulig, la brukerne velge og bytte sine egne passord og inkludere en egen bekreftelsesprosedyre for å forhindre skrivefeil;
- c) stille krav om valg av gode passord som beskrevet i 9.3.1;
- d) når brukerne vedlikeholder sine egne passord: stille krav om bytte av passord, som beskrevet i 9.3.1;
- e) tvinge brukere til å endre midlertidig passord ved første pålogging i de tilfeller der brukerne selv velger passord (se 9.2.3);
- f) føre logg over tidligere brukerpassord, for eksempel de siste 12 månedene, og hindre gjenbruk;
- g) ikke vise passord på skjermen når det blir skrevet inn;
- h) lagre passordfiler adskilt fra andre applikasjoner i datasystemet;
- i) lagre passord i kryptert form ved bruk av en énveis krypteringsalgoritme;
- j) endre standard leverandørpassord etter installasjon av programvare.

9.5.5 Bruk av hjelpeprogrammer

De fleste datainstallasjoner har ett eller flere hjelpeprogrammer som kan være i stand til å overstyre system- og applikasjonskontroller. Det er helt avgjørende at bruken av slike programmer er begrenset og strengt kontrollert. Følgende sikringstiltak bør overveies:

- a) bruk av autentiseringsprosedyrer for hjelpeprogrammer;
- b) å skille systemfunksjoner fra applikasjonsprogramvare;
- c) å begrense bruk av hjelpeprogrammer til et absolutt minimum av betroede, autoriserte brukere;
- d) autorisasjon for ad hoc-bruk av hjelpeprogrammer;
- e) å begrense tilgjengeligheten av hjelpeprogrammer, for eksempel under utføring av en autorisert endring;
- f) logg over all bruk av hjelpeprogrammer;
- g) å definere og dokumentere autorisasjonsnivå for hjelpeprogrammer;
- h) å fjerne alle unødvendige programvarebaserte hjelpeprogrammer og systemprogramvare.

9.5.6 Tvangsalarm for å sikre brukerne

Anskaffelse av tvangsalarm (alarm som varsler om en bruker handler under tvang) bør vurderes for brukere som kan bli utsatt for tvang. Beslutningen om å anskaffe slik alarm bør bygge på en risikovurdering. Ansvar og prosedyrer for å reagere på tvangsalarmen bør være definert.

9.5.7 Avstengning av terminal

Inaktive terminaler i høyrisikoområder, for eksempel offentlige områder eller områder utenfor kontroll av organisasjonens sikkerhetsledelse eller terminaler som betjener høyrisikosystemer, bør stenge seg av automatisk etter en nærmere definert periode uten aktivitet for å forhindre tilgang fra uautoriserte personer. Denne avstengningsfunksjonen bør blanke terminalens skjerm og stenge både applikasjoner og nettverksoppkoblinger etter en angitt periode med inaktivitet. Tidsforsinkelsen før avstengning bør gjenspeile sikkerhetsrisikoen i området og hvem som benytter terminalen.

En begrenset form for avstengningsfunksjon tilbys på enkelte pc-er, som blunker skjermen og hindrer uautorisert tilgang, men som ikke stenger aktive applikasjoner eller nettverksoppkoblinger.

9.5.8 Begrensninger på oppkoblingstidspunkt

Begrensninger på tidspunkt for oppkobling kan gi ytterligere sikkerhet ved høyrisikoapplikasjoner. Ved å begrense tidsrommet der terminaloppkobling til informasjonstjenester er tillatt, reduseres mulighetene for uautorisert tilgang. Slik kontroll bør vurderes for sensitive applikasjoner, spesielt når terminalene er installert i høyrisikoområder, for eksempel offentlige eller eksterne områder som er utenfor kontroll av organisasjonens sikkerhetsledelse. Eksempler på slike begrensninger omfatter:

- a) bruk av forhåndsdefinerte tidsintervaller, for eksempel for satsvise overføringer (batch) eller regelmessige interaktive sesjoner av kort varighet;
- b) tidsrommet for oppkobling begrenses til normal arbeidstid dersom det ikke er nødvendig med overtid eller utvidet bruk.

9.6 Tilgangskontroll for program

Mål: Å unngå uautorisert tilgang til informasjon i informasjonssystemene.

Sikringsmekanismer bør iverksettes for å styre tilgangsrettighetene innenfor applikasjonssystemene.

Logisk tilgang til programvare og informasjon bør begrenses til autoriserte brukere.

Applikasjonssystemene bør:

- a) kontrollere brukertilgang til informasjon og programfunksjoner i henhold til organisasjonens definerte strategi for tilgangskontroll;

- b) gi beskyttelse mot uautorisert tilgang til hjelpeprogrammer og programvare for operativsystem som kan overstyre system- eller programkontroller;
- c) ikke kompromittere sikkerheten i andre systemer som IT-ressursene deles med;
- d) være i stand til å gi tilgang til informasjon utelukkende til eieren, andre nominerte, autoriserte personer eller definerte grupper av brukere.

9.6.1 Begrensning av tilgang til informasjon

Brukere av applikasjoner, inkludert støttepersonell, bør ha tilgang til informasjon og programfunksjoner i henhold til definerte retningslinjer for tilgangskontroll, basert på individuelle tjenstlige behov, og i samsvar med organisasjonens definerte strategi for tilgangskontroll (se 9.1). Følgende sikringstiltak bør vurderes for å oppfylle kravene om tilgangsbegrensning:

- a) bruk av menyer for å kontrollere tilgang til applikasjonenes systemfunksjoner;
- b) begrense brukeres kjennskap til informasjon eller programsystemfunksjoner som de ikke er autorisert til å bruke, med hensiktsmessig tilrettelegging av brukerdokumentasjon;
- c) kontroll av brukernes tilgangsrettigheter, for eksempel lese, skrive, slette, utføre;
- d) sikre at utdata fra applikasjonssystemer som håndterer følsom informasjon, bare inneholder informasjon som er relevant for bruken av utdataene, og at de bare sendes til autoriserte terminaler og steder. Slike utdata bør gjennomgå med jevne mellomrom for å sikre at overflødig informasjon blir fjernet.

9.6.2 Isolering av sensitive informasjonssystemer

Informasjonssystemer som inneholder sensitive data, kan kreve et dedikert (isolert) driftsmiljø. Noen applikasjonssystemer er så følsomme overfor mulige tap at de krever spesiell behandling. Graden av sensitivitet avgjør om applikasjonssystemet bør kjøres på en dedikert maskin, om det kan dele ressurser med pålitelige applikasjonssystemer, eller om begrensninger er nødvendig. Følgende vurderinger bør være gjeldende:

- a) Applikasjonssystemenes sensitivitet bør være uttrykkelig identifisert og dokumentert av applikasjonseier (se 4.1.3).
- b) Når en sensitiv applikasjon skal kjøres i et delt brukermiljø, bør andre programmer som den skal dele ressurser med, identifiseres og godkjennes av eieren av den følsomme applikasjonen.

9.7 Overvåking av systemtilgang og bruk

Mål: Å avsløre uautoriserte aktiviteter.

Systemer bør overvåkes for å avdekke avvik fra retningslinjene for tilgangskontroll og registrere sporbar aktivitet for å sikre bevis i tilfelle sikkerhetshendelser.

Systemovervåking er nødvendig for å bestemme de vedtatte kontrolltiltakenes effektivitet og stadfeste overensstemmelse med organisasjonens strategi for tilgangskontroll (9.1).

9.7.1 Logging av hendelser

Logger over alle avvik og sikkerhetsrelevante hendelser bør produseres og oppbevares i en nærmere avtalt periode for å bidra til eventuell fremtidig etterforskning og for å overvåke tilgangskontrollen.

Loggene bør også inneholde:

- a) brukernavn;
- b) dato og tidspunkt for pålogging og avlogging;
- c) terminalidentitet eller lokalisering hvis mulig;
- d) oversikt over vellykkede og avviste forsøk på systemtilgang;
- e) oversikt over vellykkede og avviste forsøk på tilgang til data og andre ressurser.

Enkelte revisjonslogger bør oppbevares som et ledd i organisasjonens retningslinjer for arkivering, eller på grunn av behov for å samle bevis (se også punkt 12).

9.7.2 Overvåkning av systembruk

9.7.2.1 Prosedyrer og risikoområder

Prosedyrer for å overvåke bruk av IT-utstyr bør innføres. Slike prosedyrer er nødvendige for å sikre at brukerne bare utfører oppgaver som de er uttrykkelig autorisert til. Kravene til overvåkning av det enkelte system bør fastsettes etter egen risikovurdering. Områder som bør vurderes, omfatter:

- a) autorisert tilgang, inkludert detaljer som:
 - 1) brukeridentitet;
 - 2) dato og klokkeslett for viktig aktivitet;
 - 3) typer av aktivitet;
 - 4) filene som er aksessert;
 - 5) programmene/hjelpesprogrammene som er brukt;
- b) alle privilegerte operasjoner, for eksempel:
 - 1) bruk av systemansvarliges konto;
 - 2) systemoppstart og -stans;
 - 3) tilkobling/frakobling av inn/ut-enheter
- c) uautoriserte forsøk på tilgang, for eksempel:
 - 1) mislykkede påloggingsforsøk;
 - 2) brudd på tilgangsrettigheter og varsling i forbindelse med nettverksportene og brannmurer;
 - 3) alarmer fra proprietære innbruddsvarslingssystemer;
- d) systemalarmer eller -svikt som for eksempel:
 - 1) konsollalarmer eller meldinger;
 - 2) avvik i systemlogger;
 - 3) alarmer i forbindelse med nettverksadministrasjon.

9.7.2.2 Risikofaktorer

Resultatet av overvåkningsaktivitetene bør gjennomgås regelmessig. Hyppigheten av slik gjennomgang bør avhenge av risikoen som er involvert. Risikofaktorer som bør vurderes, omfatter:

- a) applikasjonsprosessenes viktighet;
- b) verdien, følsomheten og viktigheten av informasjonen det dreier seg om;
- c) tidligere erfaring med systeminfiltrasjon og misbruk;
- d) omfanget av systemtilkobling (særlig til offentlige nettverk).

9.7.2.3 Logging og gjennomgang av hendelser

En loggjennomgang innebærer å etablere en forståelse av truslene systemet står overfor, og hvordan disse truslene kan oppstå. Eksempler på forhold som kan kreve ytterligere granskning i tilfelle sikkerhetshendelser, er gitt i 9.7.1.

Systemlogger inneholder ofte store mengder informasjon, og mye av denne vedkommer ikke sikkerhetsovervåkingen. For lettere å kunne identifisere aktiviteter som er viktige for overvåkingen, bør det vurderes å innføre automatisk kopiering av bestemte meldingstyper til en annen logg og/eller bruk av egnede hjelpeprogrammer eller revisjonsverktøy for å utføre søking i loggfilene.

Når ansvaret for loggrevisjon tildeles, bør man overveie en rolledeling mellom personen(e) som skal foreta gjennomgangen, og de som blir overvåket.

Særlig oppmerksomhet bør vies til beskyttelse av loggingsutstyret. Dersom dette utstyret blir modifisert, kan det gi falsk trygghetsfølelse. Kontrolltiltak bør ta sikte på å beskytte utstyret mot uautoriserte endringer og driftsproblemer, herunder:

- a) deaktivering av loggingsutstyret;
- b) endringer med hensyn til hvilke meldingstyper som blir registrert;
- c) at loggfilen blir redigert eller slettet;
- d) at media der loggfilene lagres, blir slitt ut og enten ikke registrerer hendelser, eller skriver over seg selv.

9.7.3 Synkronisering av klokker

Riktig innstilling av systemklokke er viktig for å sikre revisjonsloggernes nøyaktighet, noe som kan vise seg nødvendig ved etterforskning eller som bevis i straffe- eller disiplinærsaker. Unøyaktige revisjonslogger kan forhindre etterforskning og svekke bevisenes troverdighet.

Dersom en datamaskin eller kommunikasjonsenhet har muligheten til å benytte en sanntidsklokke, bør denne stilles etter en avtalt standard, for eksempel Greenwich Mean Time (GMT). I og med at mange klokker blir unøyaktige over tid, bør det foreligge prosedyrer som sjekker og korrigerer signifikante variasjoner.

9.8 Bruk av bærbart datautstyr og hjemmearbeid

Mål: Å sikre informasjonssikkerhet ved bruk av mobilt IT-utstyr og utstyr for hjemmearbeid.

Beskyttelseskravene bør stå i forhold til risikoen disse ulike arbeidsformene innebærer. Ved bruk av bærbart datautstyr bør man ta hensyn til risikoen som er forbundet med å arbeide i et ubeskyttet miljø, og ta hensiktsmessige forholdsregler. Ved hjemmearbeid bør organisasjonen sikre arbeidsstedet og sørge for at egnede ordninger er etablert for denne arbeidsformen.

9.8.1 Bruk av bærbart datautstyr

Ved bruk av bærbart datautstyr, for eksempel elektroniske dagbøker, tidsplanleggere, bærbare datamaskiner og mobiltelefoner, bør det utvises særlig forsiktighet, slik at forretningsinformasjon ikke blir kompromittert. Det bør innføres formelle retningslinjer som tar hensyn til risikoen ved å arbeide med bærbart datautstyr, særlig i ubeskyttede miljøer. Slike retningslinjer bør for eksempel omfatte kravene som stilles til fysisk beskyttelse, tilgangskontroll, kryptografiske teknikker, sikkerhetskopier og virusbeskyttelse. Retningslinjene bør også inneholde regler og råd om oppkobling av bærbart utstyr til nettverk og rettledning om bruk av slikt utstyr på offentlige steder.

Stor forsiktighet bør utvises ved bruk av bærbart IT-utstyr på offentlig område, i møterom og andre ubeskyttede steder utenfor organisasjonens lokaler. Sikringstiltak bør iverksettes for å hindre uautorisert tilgang til eller avdekking av informasjonen som er lagret og behandlet på dette utstyret, for eksempel bruk av kryptografiske teknikker (se 10.3). Når slikt utstyr benyttes på offentlige steder, er det viktig å unngå å bli iakttatt av uautoriserte personer. Prosedyrer mot skadelig programvare bør etableres og holdes oppdatert (se 8.3). Det bør også finnes tilgjengelig utstyr som muliggjør rask og enkel sikkerhetskopiering av informasjon. Disse sikkerhetskopiene bør gis tilfredsstillende beskyttelse mot for eksempel tyveri eller tap av informasjon.

Egnet beskyttelse bør også gis til bruk av bærbart utstyr som er koblet til nettverk. Fjerntilgang til virksomhetsinformasjon over offentlige nettverk ved bruk av bærbart datautstyr bør bare finne sted etter vellykket identifikasjon og autentisering, og der det foreligger egnede mekanismer for tilgangskontroll (se 9.4).

Bærbart datautstyr bør dessuten beskyttes fysisk mot tyveri, særlig når det blir etterlatt i biler eller andre transportmidler, hotellrom, konferansesenter og møtesteder. Utstyr som inneholder viktig, følsom og/eller kritisk forretningsinformasjon, bør ikke forlates ubevoktet, og bør hvis mulig låses inn eller beskyttes av spesiallåser. Mer informasjon om fysisk beskyttelse av bærbart utstyr finnes under 7.2.5.

Det bør gis opplæring til ansatte som bruker bærbart datautstyr, for å øke deres bevissthet omkring risikoen som er knyttet til denne arbeidsformen, og kontrolltiltakene som bør iverksettes.

9.8.2 Hjemmearbeid

Hjemmearbeid benytter seg av kommunikasjonsteknologi for å gi de ansatte mulighet til å arbeide fra et fast sted utenfor organisasjonens område. Egnede beskyttelse av arbeidsplassen bør etableres mot for eksempel tyveri av utstyr og informasjon, uautorisert innsyn, uautorisert fjerntilgang til organisasjonens interne systemer eller misbruk av fasiliteter. Det er viktig at hjemmearbeid er både autorisert og kontrollert av ledelsen, og at passende ordninger er etablert for denne arbeidsformen.

Organisasjonen bør vurdere å utvikle retningslinjer, prosedyrer og standarder for kontroll av hjemmearbeid. Organisasjonen bør bare autorisere hjemmearbeid dersom den har forvisset seg om at tilstrekkelige sikkerhetsordninger og kontrolltiltak er på plass, og at disse er i samsvar med organisasjonens sikkerhetspolitikk. Følgende punkter bør drøftes:

- a) eksisterende fysisk sikkerhet på arbeidsplassen, herunder den fysiske sikkerheten til bygningen og nærmiljøet;
- b) miljøet der hjemmearbeidet skal foregå;
- c) kravene til informasjonssikkerhet, inkludert behovet for fjerntilgang til organisasjonens interne systemer, følsomheten av informasjonen som skal aksesseres og sendes over kommunikasjonsforbindelsen, og de interne systemenes følsomhet;
- d) trusselen om uautorisert tilgang til informasjon eller ressurser fra andre personer som bruker utstyret, for eksempel familie og venner.

Kontrolltiltak og ordninger som bør vurderes inkluderer:

- a) anskaffelse av tilfredsstillende utstyr og lagringsmøbler for hjemmearbeid;
- b) en definisjon av tillatte arbeidsoppgaver, arbeidstider og klassifiseringsnivå på informasjon som kan oppbevares, og de interne systemene og tjenestene som hjemmearbeideren har autorisert tilgang til;
- c) anskaffelse av egnet kommunikasjonsutstyr, inkludert metoder for å sikre fjerntilgang;
- d) fysisk sikring;
- e) regler og retningslinjer for familie og besøkendes tilgang til IT-utstyr og informasjon;
- f) anskaffelse av maskin- og programvarestøtte og vedlikehold;
- g) prosedyrer for sikkerhetskopiering og driftskontinuitet;
- h) revisjon og sikkerhetsovervåkning;
- i) inndragelse av autorisasjon, tilgangsrettigheter og utstyr når hjemmearbeidet opphører.

10 Systemutvikling og vedlikehold

10.1 Informasjonssystemenes sikkerhetskrav

Mål: Å påse at sikkerhet innebygges i informasjonssystemene.

Dette omfatter infrastruktur, forretningsapplikasjoner og egenutviklede applikasjoner. Utforming og gjennomføring av driftsprosedyrer som støtter applikasjonen eller tjenesten, kan være avgjørende for sikkerheten. Sikkerhetskravene bør identifiseres og avtales før utvikling av informasjonssystemet starter.

Alle sikringskrav, inkludert behovet for reserveløsninger, bør identifiseres i forbindelse med kravspesifiseringen til et prosjekt og bør begrunnes, godkjennes og dokumenteres som en del av den overordnede driftsmessige begrunnelsen for et informasjonssystem.

10.1.1 Analyse og spesifisering av sikkerhetskrav

Utredninger av virksomhetsbaserte krav til nye systemer eller til forbedringer av eksisterende systemer bør spesifisere hvilke kontrollkrav som stilles. Slike spesifikasjoner bør ta stilling til hvilke automatiske

kontroller som skal integreres i systemet, og behovet for ytterligere manuell kontroll. Lignende overveielser bør gjøres ved vurdering av programvarepakker for forretningsapplikasjoner. Dersom ledelsen finner det hensiktsmessig, kan den velge å benytte produkter som er vurdert og sertifisert av uavhengige instanser.

Omfanget av sikringskrav og kontrolltiltak bør gjenspeile forretningsverdien av informasjonen som er involvert, og de potensielle skadene for organisasjonen ved sviktende eller mangelfull sikkerhet. Risikoanalysen og -håndteringen danner rammeverket for å analysere sikkerhetskravene og identifisere kontrolltiltakene som bør innføres for å oppfylle dem.

Kontrolltiltak som introduseres i utformingsfasen, er betydelig billigere å gjennomføre og vedlikeholde enn de som føyes til under eller etter innføringen av systemet.

10.2 Sikkerhet i applikasjonssystemene

Mål: Å forhindre tap, endring eller misbruk av brukerdata i applikasjonssystemene.

Hensiktsmessige kontrolltiltak og revisjonsspor eller aktivitetslogger bør integreres i applikasjonssystemene, også i egenutviklede applikasjoner. Disse kontrolltiltakene bør omfatte godkjenning av inndata, intern behandling og utdata.

Ytterligere kontrolltiltak kan være påkrevd for systemer som behandler eller har innvirkning på informasjon som er sensitiv eller kritisk for organisasjonen. Slike tiltak bør iverksettes på grunnlag av sikkerhetskrav og risikovurdering.

10.2.1 Godkjenning av inndata

Inndata til applikasjonssystemene bør godkjennes for å sikre at de er korrekte og gyldige. Kontroller bør utføres på inndata om forretningstransaksjoner, løpende data (navn og adresser, kredittgrenser, kunders referansenummer) og parametertabeller (salgspriser, valutakurser, skattesatser). Følgende tiltak bør vurderes:

- a) dobbelt kontroll av inndata eller andre kontrolltiltak for å avdekke følgende feil:
 - 1) verdier utenfor vedtatte grenseverdier;
 - 2) ugyldige tegn i datafelt;
 - 3) manglende eller ufullstendige data;
 - 4) overskridelse av øvre eller nedre grenseverdi for datavolum;
 - 5) uautoriserte eller uoverensstemmende kontrolldata;
- b) periodisk gjennomgang av innholdet i nøkkelfelter eller datafiler for å bekrefte deres gyldighet og datakvalitet;
- c) kontroll av originaldokumenter mot uautoriserte endringer i inndata (alle endringer i inndatadokumenter bør være autorisert);
- d) prosedyrer for å korrigere feil som avdekkes i gyldighetskontroller;
- e) prosedyrer for å teste at inndata er sannsynlige;
- f) definert ansvar for alle medarbeidere som er involvert i prosessen med registrering av data.

10.2.2 Kontroll av intern behandling

10.2.2.1 Risikoområder

Data som er korrekt registrert, kan endres eller ødelegges på grunn av systemfeil eller overlagte handlinger. Gyldighetskontroller bør integreres i systemene for å avdekke slike forhold. Utformingen av applikasjonene bør sikre at det gjennomføres begrensninger for å redusere risikoen for systemfeil som kan føre til tap av integritet. Spesielle områder som bør vurderes er:

- a) bruk og plassering av funksjoner for å legge til, fjerne eller endre data i programmer;

- b) prosedyrer for å forhindre at programmer kjøres i feil rekkefølge, eller kjøres etter at foregående behandling har mislykkes (se også 8.1.1);
- c) bruk av riktige programmer for å gjenopprette data etter svikt i rutinene for å sikre korrekt databehandling.

10.2.2.2 Kontroll og etterprøving

Hvilke kontroller som er nødvendig, vil avhenge av applikasjonens art og de forretningsmessige konsekvensene av skader på data. Eksempler på kontroller som kan legges inn, omfatter blant annet:

- a) sesjons- eller buntkontroller for å avstemme saldo i registre etter transaksjonsoppdatering;
- b) saldokontroller for å kontrollere inngående saldo mot tidligere registrert utgående saldo:
 - 1) kontroll mot utgående saldo fra forrige kjøring;
 - 2) kontroll av totalsummer ved oppdatering av register/fil;
 - 3) program-til-programkontroller;
- c) bekreftelse av systemgenererte data (se 10.2.1);
- d) kontroll av data og programvare som hentes ned fra eller lastes opp til sentrale og eksterne maskiner (se 10.3.3);
- e) kontrollsummer for felter og filer;
- f) prosedyrer for å sikre at applikasjonsprogrammer kjøres på riktig tidspunkt;
- g) tiltak for å sikre at programmer kjøres i riktig rekkefølge og avsluttes i tilfelle feil, og at videre behandling stanses inntil problemet er løst.

10.2.3 Meldingsautentisering

Meldingsautentisering er en teknikk som brukes for å avdekke uautoriserte endringer eller ødeleggelse av innholdet i en elektronisk overført melding. Teknikken kan innføres ved hjelp av maskinvare eller programvare som støtter en fysisk meldingsautentiseringsenhet eller en programvarebasert algoritme.

Meldingsautentisering bør vurderes for applikasjoner der det er avgjørende å beskytte meldingsinnholdets integritet, for eksempel ved elektroniske pengeoverføringer eller annen lignende elektronisk datautveksling. En sikkerhetsvurdering bør gjennomføres for å avgjøre om meldingsautentisering er nødvendig, og for å identifisere den mest egnede metoden for implementering.

Meldingsautentisering er ikke utviklet for å beskytte innholdet i en melding fra uautorisert innsikt. Kryptografiske teknikker (se 10.3.2 og 10.3.3) kan være en egnet metode for å iverksette meldingsautentisering.

10.2.4 Godkjenning av utdata

Utdata fra et applikasjonssystem bør godkjennes for å sikre at behandlingen av lagret informasjon er korrekt og hensiktsmessig under omstendighetene. Systemer er ofte konstruert ut fra en antakelse om at etter tilfredsstillende godkjenning, verifisering og testing, vil utdata alltid være korrekt. Dette er imidlertid ikke alltid tilfellet. Godkjenning av utdata kan omfatte:

- a) sannsynlighetskontroll for å sjekke om utdata virker sannsynlige;
- b) kontrolltelling for å sikre at alle data er behandlet;
- c) sikring av tilstrekkelig informasjon til at leseren eller et senere behandlingssystem kan vurdere informasjonens nøyaktighet, fullstendighet, presisjon og klassifisering;
- d) prosedyrer for å aksjonere på gyldighetstester for utdata;
- e) definert ansvar for alle medarbeidere som er involvert i utdataprosessen.

10.3 Kryptografisk kontroll

Mål: Å beskytte informasjonens konfidensialitet, autentisitet og integritet.

Kryptografiske systemer og teknikker bør anvendes for å beskytte sårbar informasjon som ikke beskyttes tilstrekkelig av andre kontrolltiltak.

10.3.1 Retningslinjer for bruk av kryptografisk kontroll

Beslutningen om hvorvidt en kryptografisk løsning er hensiktsmessig, bør inngå som en del av en større prosess som omfatter risikovurdering og valg av kontrolltiltak. Risikovurderingen bør gjennomføres for å avgjøre hvilket beskyttelsesnivå informasjonen skal tildeles. Denne risikovurderingen bør så brukes for å avgjøre hvorvidt kryptografisk kontroll er hensiktsmessig, hvilken type kontroll som eventuelt skal benyttes, og for hvilke formål og forretningsprosesser.

Organisasjonen bør utvikle retningslinjer for bruk av kryptografiske kontroller for å beskytte sin informasjon. Slike retningslinjer er nødvendige for å maksimere fordelene og redusere risikoen ved bruk av kryptografiske teknikker, og for å unngå uhensiktsmessig eller uriktig bruk. I utviklingen av disse retningslinjene bør man ta hensyn til følgende:

- a) ledelsens holdning til bruk av kryptografiske kontroller i organisasjonen som helhet og de generelle prinsippene for beskyttelse av forretningsinformasjon;
- b) regler for administrasjon av kryptografiske nøkler, herunder metoder for å håndtere gjenoppretting av kryptert informasjon i tilfelle tap av, skade på eller ødeleggelse av kryptografiske nøkler;
- c) roller og ansvar, for eksempel hvem som er ansvarlig for:
- d) implementering av retningslinjene;
- e) administrasjon av de kryptografiske nøklene;
- f) hvordan riktig nivå av kryptografisk beskyttelse skal fastsettes;
- g) standardene som velges for effektiv iverksettelse i organisasjonen som helhet (hvilke løsninger skal velges for hvilke forretningsprosesser).

10.3.2 Kryptering

Kryptering er en kryptografisk teknikk som kan brukes til å beskytte informasjonens konfidensialitet. Denne teknikken bør vurderes for beskyttelse av sensitiv eller kritisk informasjon.

Det nødvendige beskyttelsesnivået bør fastsettes på grunnlag av en risikovurdering. Beskyttelsesnivået bør ta hensyn til typen av og kvaliteten på krypteringsalgoritmen som benyttes, og lengden på de kryptografiske nøklene som skal benyttes.

Når organisasjonens kryptografiske retningslinjer settes ut i livet, bør det tas hensyn til de nasjonale forskriftene og restriksjonene som gjelder ved bruk av kryptografiske teknikker i ulike deler av verden, og til problemene som er forbundet med flyt av kryptert informasjon over landegrensene. Organisasjonen bør dessuten være oppmerksom på reguleringene som gjelder for eksport og import av krypteringsteknologi (se også 12.1.6).

Det anbefales å søke eksperthjelp for å plukke ut riktige produkter som gir nødvendig beskyttelse, og et sikkert system for administrasjon av kryptografiske nøkler (se også 10.3.5). I tillegg kan det være nødvendig å søke juridisk bistand med hensyn til lover og regler som angår organisasjonens planlagte bruk av kryptering.

10.3.3 Digitale signaturer

Digitale signaturer er en metode som benyttes til å sikre autentisiteten og integriteten til elektroniske dokumenter. De kan for eksempel anvendes ved elektronisk handel der det er behov for å verifisere hvem

som har signert et elektronisk dokument, eller å undersøke om innholdet i det signerte dokumentet er blitt endret.

Digitale signaturer kan benyttes på alle dokumenter som behandles elektronisk. De kan for eksempel brukes til å signere elektronisk betaling, pengeoverføringer, kontrakter og avtaler. Digitale signaturer kan implementeres ved hjelp av en kryptografisk teknikk som er basert på et unikt nøkkelpar der den ene nøkkelen brukes til å lage en signatur (den private nøkkelen) og den andre til å kontrollere signaturen (den offentlige nøkkelen).

Det er viktig å beskytte den private nøkkelen sin konfidensialitet. Denne nøkkelen bør holdes hemmelig, for enhver som har tilgang til nøkkelen, kan signere dokumenter, for eksempel betalinger og kontrakter, og på den måten forfalske signaturen til nøkkelen sin eier. I tillegg er det viktig å beskytte den offentlige nøkkelen sin integritet. Denne beskyttelsen oppnås ved hjelp av sertifisering av offentlige nøkler (se 10.3.5).

Det er dessuten viktig å være oppmerksom på typen av og kvaliteten på signaturalgoritmen som brukes, og lengden på nøkkelen som skal benyttes. Kryptografiske nøkler som brukes til digitale signaturer, bør være forskjellige fra dem som benyttes til kryptering (se 10.3.2).

Ved bruk av digitale signaturer er det viktig å være oppmerksom på relevant lovgivning som beskriver under hvilke forhold digitale signaturer er juridisk bindende. For eksempel ved elektronisk handel er det avgjørende å kjenne den juridiske statusen til digitale signaturer. Det kan være nødvendig å lage bindende kontrakter eller andre avtaler som støtter bruken av digitale signaturer i tilfeller der det juridiske rammeverket er utilstrekkelig. Juridisk veiledning bør innhentes med hensyn til lover og bestemmelser som gjelder for organisasjonens planlagte bruk av digitale signaturer.

10.3.4 Ikke-benektelse

Ikke-benektelse bør benyttes der det er behov for å løse tvister om hvorvidt en hendelse eller handling har funnet sted eller ei, for eksempel uenighet om bruk av en digital signatur på en elektronisk kontrakt eller betaling. Slike tjenester kan bidra til å sikre bevis for at en bestemt hendelse eller handling har funnet sted, for eksempel dersom noen nekter for å ha sendt en digitalt signert instruks via e-post. Disse tjenestene baserer seg på bruk av teknikker for bruk av kryptering og digital signatur (se også 10.3.2 og 10.3.3).

10.3.5 Administrasjon av kryptografiske nøkler

10.3.5.1 Beskyttelse av kryptografiske nøkler

Administrasjonen av kryptografiske nøkler er avgjørende for effektiv bruk av kryptografiske teknikker. Kompromittering og tap av kryptografiske nøkler kan føre til at informasjonens konfidensialitet, autenticitet og/eller integritet skades. Et administrasjonssystem bør etableres for å støtte organisasjonens bruk av de to typene av kryptografiske teknikker, som baserer seg på:

- a) hemmelig nøkkel, der to eller flere parter har samme nøkkel og denne nøkkelen brukes både for å kryptere og dekryptere informasjon. Denne nøkkelen bør holdes hemmelig, fordi enhver som har adgang til den, er i stand til å dekryptere all informasjon som blir kryptert med denne nøkkelen, eller til å introdusere uautorisert informasjon;
- b) offentlige nøkler, der hver enkelt bruker har ett nøkkelpar bestående av en offentlig nøkkel, som kan avsløres for hvem som helst, og en privat nøkkel, som bør holdes hemmelig. Teknikken kan brukes til kryptering (se 10.3.2) og for å produsere digitale signaturer (10.3.3).

Alle nøkler bør beskyttes mot endringer og ødeleggelse. Hemmelige og private nøkler krever beskyttelse mot uautorisert innsyn. Kryptografiske teknikker kan også benyttes til dette formålet. Fysisk beskyttelse bør brukes for å beskytte utstyret som brukes for å generere, lagre og arkivere nøkler.

10.3.5.2 Standarder, prosedyrer og metoder

Administrasjonssystemet for nøkler bør være basert på et avtalt sett med standarder, prosedyrer og sikre metoder for å:

- a) generere nøkler for ulike kryptografiske systemer og forskjellige applikasjoner;
- b) generere og skaffe sertifikater for offentlige nøkler;
- c) distribuere nøkler til de planlagte brukerne og opplyse om hvordan nøklene skal aktiviseres når brukerne mottar dem;
- d) oppbevare nøkler, blant annet for å forklare hvordan autoriserte brukere får tilgang til nøkler;
- e) endre eller oppdatere nøkler, herunder regler for når nøkler skal byttes og hvordan dette gjøres;
- f) håndtere kompromitterte nøkler;
- g) tilbakekalle nøkler, herunder instruksjoner om hvordan nøkler skal trekkes tilbake eller deaktiveres, for eksempel når nøkler er blitt kompromittert eller når en bruker forlater organisasjonen. I sistnevnte tilfelle bør nøkkelen dessuten arkiveres;
- h) gjenopprette nøkler som er tapt eller kompromittert, som en naturlig del av kontinuitetsplanleggingen, for eksempel for gjenopprettelse av kryptert informasjon;
- i) arkivere nøkler, for eksempel til arkivert eller sikkerhetskopiert informasjon;
- j) ødelegge nøkler;
- k) gjennomføre logging og revisjon av aktiviteter som er knyttet til administrasjon av nøkler.

For å redusere sannsynligheten for kompromittering bør nøklene ha definerte aktiviserings- og deaktiviseringsdatoer slik at de bare kan brukes innenfor et begrenset tidsrom. Lengden av dette tidsrommet avhenger av omstendighetene omkring den kryptografiske kontrollen og den vurderte risikoen.

Det kan være nødvendig å vurdere prosedyrer for å håndtere forespørsler fra rettsapparatet om tilgang til kryptografiske nøkler. For eksempel bør kryptert informasjon i noen tilfeller legges frem i ukryptert form som bevis i rettsaker.

I tillegg til sikker administrasjon av hemmelige og private nøkler bør det vurderes å innføre beskyttelse av offentlige nøkler. Det er fare for at noen forfalsker en digital signatur ved å erstatte en brukers offentlige nøkkel med sin egen. Dette problemet håndteres ved hjelp av et sertifikat for offentlige nøkler. Disse sertifikatene bør produseres på en måte som knytter informasjon relatert til eieren av det offentlige/private nøkkelparet til den offentlige nøkkelen på en unik måte. Det er derfor viktig at administrasjonsprosessene som generer disse sertifikatene, er pålitelige. Denne prosessen utføres vanligvis av en ekstern sertifiseringsinstans, som bør være en kjent organisasjon med tilstrekkelige kontrolltiltak og etablerte prosedyrer til å sikre nødvendig grad av tillit.

Innholdet i avtaler eller kontrakter med eksterne leverandører av kryptografiske tjenester, for eksempel sertifiseringsmyndigheter, bør dekke spørsmålene om ansvar, tjenestenes pålitelighet og svartid for levering av tjenester (se 4.2.2).

10.4 Sikring av systemfiler

Mål: Å sikre at IT-prosjekter og støtteaktiviteter gjennomføres på en sikker måte.

Tilgang til systemfiler bør kontrolleres.

Ansvar for å vedlikeholdet systemets integritet bør tillegges den bruker- eller utviklingsgruppen som applikasjonssystemet eller programvaren tilhører.

10.4.1 Kontroll av produksjonsprogramvare

Det er nødvendig å føre kontroll med innføring av programvare i produksjonssystemer. For å redusere risikoen for ødeleggelse av produksjonssystemer bør følgende tiltak vurderes:

- a) Oppdatering av produksjonsprogramvarens bibliotek bør bare utføres av den som er ansvarlig for vedkommende bibliotek, og bare etter autorisasjon fra ledelsen (se 10.4.3).
- b) Om mulig bør bare kjørbar kode legges inn i produksjonssystemet.
- c) Kjørbar kode bør ikke legges inn i produksjonssystemet før vellykket testing og brukerkseptans er oppnådd og de tilhørende kildebibliotekene er blitt oppdatert.
- d) Revisjonslogg bør føres over alle oppdateringer av produksjonsprogramvarens bibliotek.
- e) Tidligere versjoner av programvare bør oppbevares som en sikkerhetsforanstaltning.

Programvare som er levert fra forhandler, og som brukes i produksjonssystemet, bør vedlikeholdes på et nivå som støttes av leverandøren. Beslutninger om å oppgradere til nye versjoner bør ta hensyn til disse versjonenes sikkerhet, dvs. innføringen av ny sikkerhetsfunksjonalitet eller antall og omfang av sikkerhetsproblemer som har oppstått i forbindelse med disse versjonene. Programvareoppdateringer bør installeres når det kan bidra til å fjerne eller redusere sikkerhetssvakheter.

Leverandører bør bare gis fysisk adgang og logisk tilgang ved behov, og bare med godkjenning fra IT-ansvarlig. Leverandørens aktiviteter bør overvåkes.

10.4.2 Beskyttelse av testdata

Testdata bør beskyttes og kontrolleres. System- og akseptansetester krever vanligvis betydelige mengder testdata som ligger så nært opp til virkelige produksjonsdata som mulig. Bruk av produksjonsdatabaser som inneholder persondata bør unngås. Hvis slik informasjon benyttes, bør den først anonymiseres. Følgende sikringstiltak bør innføres for å beskytte produksjonsdata som benyttes i testsammenheng:

- a) Prosedyrene som gjelder for produksjonssystemene, bør også gjelde for testsystemene.
- b) Det bør kreves separat autorisering hver gang produksjonsinformasjon kopieres til et testsystem.
- c) Produksjonsdata bør slettes fra testsystemet umiddelbart etter at testingen er avsluttet.
- d) Kopiering og bruk av produksjonsinformasjon bør logges for å sikre revisjonsspor.

10.4.3 Tilgangskontroll til bibliotekene for kildekode

For å redusere faren for ødeleggelse av dataprogrammer bør det føres streng kontroll med tilgang til bibliotekene for kildekode. Følgende tiltak anbefales (se også 8.3):

- a) Der det er mulig, bør bibliotek for kildekode ikke ligge i produksjonssystemene.
- b) En programbibliotekar bør oppnevnes for hver applikasjon.
- c) IT-støttepersonell bør ikke ha ubegrenset tilgang til biblioteker for kildekode.
- d) Programmer som er under utvikling eller vedlikehold, bør ikke legges inn i produksjonsprogrammernes bibliotek.
- e) Oppdatering av biblioteker for kildekode og utlevering av kildekode til programmerere bør bare utføres av den oppnevnte bibliotekaren og etter autorisasjon fra vedlikeholdsansvarlig for applikasjonen.
- f) Programlister bør oppbevares sikkert (se 8.6.4).
- g) Det bør føres revisjonslogg over all tilgang til bibliotekene for kildekode.
- h) Gamle versjoner av kildekode bør arkiveres med tydelig merking av nøyaktig dato og klokkeslett da de var operative, sammen med alle støtteprogrammer, jobbkontroll, datadefinisjoner og prosedyrer.
- i) Vedlikehold og kopiering av programbibliotek bør underlegges streng endringskontroll (se 10.4.1).

10.5 Sikkerhet i utviklings- og vedlikeholdsprosesser

Mål: Å opprettholde sikkerheten rundt programvare for applikasjonssystemer og data.

Utviklings- og vedlikeholdsmiljøer bør underlegges streng kontroll.

Ledere som er ansvarlige for applikasjonssystemer bør også være ansvarlige, for sikkerheten rundt utviklings- og vedlikeholdsmiljøet. De bør forsikre seg om at alle planlagte systemendringer er kontrollert, slik at de ikke svekker sikkerheten til det aktuelle systemet eller driftsmiljøet.

10.5.1 Prosedyrer for endringskontroll

For å begrense forringelse av informasjonssystemene bør det føres streng kontroll med gjennomføringen av endringer. Formelle prosedyrer for endringskontroll bør innføres. Disse prosedyrene skal sørge for at sikkerhet og kontrollprosedyrer ikke blir kompromittert, at programmerere bare får tilgang til de delene av systemet som er nødvendig for arbeidet deres, og at en formell avtale om og godkjenning av alle endringer er oppnådd. Endringer i applikasjonsprogramvaren kan påvirke produksjonsmiljøet. Om mulig bør kontrollprosedyrene for applikasjonene og produksjonsmiljøet derfor integreres (se også 8.1.2). Denne kontrollprosessen skal blant annet:

- a) etablere en oversikt over godkjente autorisasjonsnivåer;
- b) sikre at endringsforslag stammer fra autoriserte brukere;
- c) gjennomgå kontrolltiltak og kvalitetsprosedyrer for å påse at de ikke blir kompromittert av endringene;
- d) identifisere all programvare, informasjon, databaseobjekter og maskinvare som bør oppdateres;
- e) innhente formell godkjenning av detaljerte arbeidsplaner før arbeidet begynner;
- f) sikre at den autoriserte brukeren aksepterer endringene før de iverksettes;
- g) sikre at implementeringen gjennomføres på en slik måte at den i minst mulig grad forstyrrer den daglige driften;
- h) sikre at systemdokumentasjonen er oppdatert ved avslutning av hver endring, og at gammel dokumentasjon blir arkivert eller kastet;
- i) gjennomføre versjonskontroll ved alle oppdateringer av programvare;
- j) opprettholde revisjonsspor over alle endringsanmodninger;
- k) sørge for de nødvendige endringene i driftsdokumentasjonen (se 8.1.1) og brukerprosedyrene slik at de er oppdatert;
- l) sikre at innføringen av endringer finner sted på rett tidspunkt og ikke forstyrrer de involverte forretningsprosessene.

Mange organisasjoner gir brukerne anledning til å teste ny programvare i et eget miljø som er atskilt fra utviklings- og produksjonsmiljøene. Dette gir mulighet til å få kontroll over ny programvare og gir ytterligere beskyttelse av produksjonsinformasjon som brukes til testformål.

10.5.2 Teknisk gjennomgang av endringer i produksjonssystem

Med jevne mellomrom vil det være nødvendig å gjøre endringer i produksjonssystemet, for eksempel for oppgradering til nye programvareversjoner eller -rettelser. Når slike endringer finner sted, bør applikasjonssystemet gjennomgås og testes for å sikre at det ikke får negative konsekvenser for drift eller sikkerhet. Denne prosessen bør sørge for å:

- a) gjennomgå applikasjonskontroller og kvalitetsprosedyrer for å sikre at de ikke er blitt kompromittert av endringene i operativsystemet;
- b) sikre at årlige vedlikeholdsplaner og -budsjetter dekker gjennomgang og test av følgene av endringer i operativsystemet;
- c) melde fra om endringer i operativsystemet i god tid før iverksettelse, slik at nødvendige gjennomganger kan utføres;

- d) sikre at hensiktsmessige endringer blir gjort i kontinuitetsplanene (se punkt 11).

10.5.3 Begrensninger på endringer av programvarepakker

Endringer i programvarepakker bør forhindres. Så langt det er praktisk mulig, bør standard programvarepakker brukes uten modifikasjoner. I de tilfeller der man anser det som tvingende nødvendig å foreta endringer, bør det tas hensyn til følgende:

- a) risikoen for at innebygde kontroller og kvalitetsprosedyrer kan bli kompromittert;
- b) behovet for å innhente tillatelse fra leverandøren;
- c) muligheten for å gjennomføre de ønskede endringene ved hjelp av standard oppdateringer fra leverandøren;
- d) konsekvensene dersom organisasjonen blir ansvarlig for fremtidig vedlikehold av programvaren som følge av endringer.

Dersom endringene vurderes som nødvendige, bør den opprinnelige programvaren oppbevares og endringene gjennomføres på en omhyggelig merket kopi. Alle endringer bør testes og dokumenteres grundig, slik at de kan legges inn på nytt ved senere oppdateringer av programvaren.

10.5.4 Bakdører og trojanske koder

Bakdører kan blottlegge informasjon på indirekte og skjulte måter. Den kan bli aktivisert ved endringer i et parameter som er tilgjengelig for både sikre og usikre elementer i et datasystem, eller ved å pakke inn informasjon i en datastrøm. Trojanske koder er utviklet for å påvirke et system på en måte som ikke er autorisert og ikke umiddelbart blir oppdaget, og som ikke mottakeren eller brukeren av programmet har bedt om. Bakdører og trojanske koder oppstår sjelden ved en tilfeldighet. I de tilfeller der skjulte kanaler og trojanske koder er en trussel, bør følgende overveies:

- a) å bare kjøpe programmer fra anerkjente kilder;
- b) å kjøpe programmer i kildekode slik at koden kan verifiseres;
- c) å bruke evaluerte produkter;
- d) å gjennomgå all kildekode før programmet tas i bruk;
- e) å kontrollere tilgang til og endringer av kode etter at den er installert;
- f) å bruke betrodde medarbeidere til arbeid på nøkkelsystemer.

10.5.5 Outsourcing av programvareutvikling

I de tilfeller der programvareutvikling er satt ut til tredjepart, bør følgende punkter vurderes:

- a) lisensavtaler, eiendomsrett til koder og intellektuell eiendomsrett (se 12.1.2);
- b) sertifisering av det utførte arbeidets kvalitet og nøyaktighet;
- c) deponeringsavtaler i tilfelle svikt fra tredjeparts side;
- d) tilgangsrettigheter for revisjon av det utførte arbeidets kvalitet og nøyaktighet;
- e) kontraktsfestede krav til kodekvalitet;
- f) testing før installasjon for å avdekke trojansk koder.

11 Kontinuitetsplanlegging

11.1 Aspekter ved kontinuitetsplanlegging

Mål: Å motvirke avbrudd i forretningsaktivitetene og beskytte kritiske driftsprosesser fra konsekvensene av større feil eller katastrofer.

En prosess for kontinuitetsplanlegging bør igangsettes for å redusere avbrudd som følge av katastrofer og sikkerhetssvikt (som kan være resultat av for eksempel naturkatastrofer, uhell, feil på utstyr og overlagte handlinger) til et akseptabelt nivå gjennom en kombinasjon av forebyggende tiltak og planer for gjenopprettelse av systemet.

Konsekvensene av katastrofer, sikkerhetssvikt og tap av tjenester bør analyseres. Kriseplaner bør utarbeides og iverksettes for å sikre at driftsprosessene kan gjenopprettes innenfor de fastsatte tidsrammene. Disse planer bør vedlikeholdes og innøves slik at de blir en integrert del av de øvrige administrasjonsprosessene.

Kontinuitetsplanlegging bør omfatte kontrolltiltak for å identifisere og redusere risikoer, begrense konsekvensene av ødeleggende hendelser og sikre rask gjenopprettelse av viktige driftsprosesser.

11.1.1 Kontinuitetsplanleggingsprosessen

Det bør etableres en styrt prosess for å utvikle og vedlikeholde driftskontinuitet i organisasjonen som helhet. Den bør sammenføre følgende nøkkelementer i kontinuitetsplanleggingen:

- a) vurdere truslene som organisasjonen står overfor, målt mot sannsynligheten for og konsekvensene av de inntreffer. Dette omfatter også identifisering og prioritering av kritiske virksomhetsprosesser;
- b) vurdere konsekvensene av eventuelle avbrudd for organisasjonen (det er viktig at det finnes løsninger som kan håndtere både mindre hendelser og alvorlige problemer som kan true organisasjonens overlevelse), og etablere virksomhetsmålene med IT-utstyret;
- c) vurdere innkjøp av hensiktsmessig forsikring som en del av kontinuitetsplanleggingen;
- d) formulere og dokumentere en strategi for kontinuitetsplanlegging som er i samsvar med de avtalte virksomhetsmålene og prioriteringene;
- e) formulere og dokumentere kontinuitetsplaner i samsvar med den avtalte strategien;
- f) teste og oppdatere de foreliggende planene og prosessene med regelmessige mellomrom;
- g) sikre at kontinuitetsplanleggingen er integrert i organisasjonens prosesser og strukturer. Ansvaret for å koordinere kontinuitetsplanleggingen bør plasseres på et hensiktsmessig nivå innenfor organisasjonen, for eksempel i et informasjonssikkerhetsforum (se 4.1.1).

11.1.2 Kontinuitets- og konsekvensanalyse

Kontinuitetsplanleggingen bør begynne med å identifisere hendelser som kan forstyrre virksomhetsprosessene, for eksempel utstyrsfeil, oversvømmelse og brann. Dette bør følges opp med en risikovurdering der man anslår konsekvensene av slike avbrudd (både med hensyn til skadeomfang og tidsramme for gjenopprettelse). Begge disse aktivitetene bør utføres i fullt samarbeid med eierne av virksomhetsressursene og -prosessene. Denne analysen tar hensyn til alle virksomhetsprosesser og er ikke begrenset til informasjonssystemene.

På grunnlag av resultatene av risikovurderingen bør det utarbeides en plan for å fastlegge de generelle retningslinjene for driftskontinuitet. Når denne planen er utarbeidet, bør den godkjennes av ledelsen.

11.1.3 Utforming og implementering av kontinuitetsplanene

Det bør utarbeides planer for å opprettholde eller gjenopprette forretningsdriften innenfor fastsatt tid etter avbrudd eller svikt i kritiske driftsprosesser. Kontinuitetsplanleggingen bør ta hensyn til følgende:

- a) identifikasjon av og enighet om alle ansvarsforhold og nødprosedyrer;
- b) iverksettelse av nødprosedyrer for å sikre gjenoppretting innenfor avtalte tidsrammer. Særlig oppmerksomhet bør vies til vurderingen av eksterne bindinger og eksisterende kontrakter;
- c) dokumentasjon av avtalte prosedyrer og prosesser;
- d) tilstrekkelig opplæring av de ansatte i de avtalte nødprosedyrene og -prosessene, inkludert krisehåndtering;
- e) testing og oppdatering av planene.

Planleggingsprosessen bør fokusere på de viktigste virksomhetsmålene, for eksempel gjenoppretting av spesielle tjenester til kunder innenfor akseptable tidsrammer. Tjenestene og ressursene som gjør dette mulig, bør kartlegges. Dette omfatter også kravene til bemanning, manuelle ressurser og reserveløsninger for IT-utstyr.

11.1.4 Rammeverk for kontinuitetsplanlegging

Ett enkelt rammeverk med felles kontinuitetsplaner bør utarbeides for å sikre at alle planene er i overensstemmelse med hverandre, og for å bestemme prioritering med hensyn til testing og vedlikehold. Enhver kontinuitetsplan bør definere nøyaktig i hvilke tilfeller den skal iverksettes, og hvem som er ansvarlige for å sette de ulike delene av planen ut i livet. Når nye krav blir innført, bør de foreliggende nødprosedyrene, for eksempel evakueringsplaner eller eksisterende reserveløsninger, revideres tilsvarende.

Et rammeverk for kontinuitetsplanlegging bør dekke følgende:

- a) betingelsene som bør være til stede for at planen skal settes ut i livet, herunder en beskrivelse av prosedyrene som skal følges (hvordan situasjonen skal vurderes, hvem som skal involveres osv.) før hver enkelt plan aktiveres;
- b) nødprosedyrer som beskriver hva man skal gjøre i tilfelle hendelser som setter forretningsdriften og/eller menneskeliv i fare. Disse prosedyrene bør omfatte rutiner for håndtering av informasjon til omverdenen og for effektiv kontakt med relevante offentlige myndigheter, for eksempel politiet, brannvesenet og lokale myndigheter;
- c) nødprosedyrer som beskriver hva som bør gjøres for å flytte viktige forretningsaktiviteter eller støttetjenester til andre, midlertidige lokaler, og for å få forretningsaktivitetene tilbake i drift innenfor de avtalte tidsrammene;
- d) gjenopprettingsprosedyrer som beskriver hva som bør gjøres for å vende tilbake til normal driftssituasjon;
- e) vedlikeholdsplaner som spesifiserer hvordan og når kontinuitetsplanen skal testes ut, og prosedyrene for å holde planen vedlike;
- f) bevissthetsskapende aktiviteter og opplæring som er utformet for å skape forståelse for kontinuitetsprosessene og sikre at prosessene til enhver tid er virksomme;
- g) individuelle ansvarsforhold, med en beskrivelse av hvem som er ansvarlig for å gjennomføre hvilke deler av planen. Reserver bør utnevnes der det er behov for det.

Hver plan bør ha en bestemt eier. Ansvaret for nødprosedyrer, manuelle reserveløsninger og gjenopprettingsplaner bør påhvile eieren av de involverte driftsressursene eller -prosessene. Reserveløsninger for alternative tekniske tjenester, for eksempel IT- og kommunikasjonsutstyr, er vanligvis tjenesteleverandørens ansvar.

11.1.5 Prøving, vedlikehold og revisjon av kontinuitetsplanleggingen

11.1.5.1 Testing av planen

Mange kontinuitetsplaner svikter når de blir testet, ofte fordi de bygger på uriktig forutsetninger, fordi man overser ting, eller som følge av endringer i utstyr og personell. De bør derfor testes regelmessig for å sikre at de er oppdaterte og virksomme. Slike tester bør også sikre at medlemmene av kriseteamet og andre relevante medarbeidere er oppmerksomme på planene.

Tidsplanen for testing av kontinuitetsplanen bør indikere hvordan og når hvert enkelt element i planen skal testes. Det anbefales at man tester de ulike elementene i planen(e) hyppig. En rekke ulike teknikker kan benyttes for å sikre at planen(e) skal fungere i krisetilfeller. Disse omfatter:

- a) skrivebordstesting av ulike scenarier (diskusjon om rutinene for gjenoppretting av vanlig drift, der man tar for seg ulike eksempler på avbrudd);
- b) simulering (særlig for å informerer de ansatte om deres oppgaver i etterkant av hendelser/katastrofer);
- c) tekniske gjenopprettingstester (for å sikre at informasjonssystemene kan gjenopprettes effektivt);
- d) øvelse i gjenoppretting på et alternativt sted (dvs. at man kjører vanlige driftsprosesser parallelt med at man iverksetter gjenopprettingsprosedyrer på et annet sted enn hovedinstallasjonen);
- e) teste leverandørens utstyr og tjenester (for å sikre at eksternt leverte tjenester og produkter oppfyller avtalte forpliktelser);
- f) komplette øvelser (for å teste at organisasjonen, medarbeiderne, utstyret, fasilitetene og prosessene kan håndtere avbrudd).

Teknikkene kan benyttes av alle organisasjoner og bør gjenspeile deres konkrete planer for gjenoppretting.

11.1.5.2 Vedlikehold og revisjon av planen

Kontinuitetsplaner bør vedlikeholdes gjennom regelmessige revisjoner og oppdateringer for å sikre at de til enhver tid er effektive. Prosedyrene bør innlemmes i organisasjonens program for endringsstyring for å sikre at hensynet til driftskontinuitet får tilstrekkelig oppmerksomhet.

Ansvar for regelmessig revisjon av de enkelte kontinuitetsplanene bør fordeles. Identifisering av nye driftsordninger som ennå ikke er gjenspeilt i kontinuitetsplanen, bør følges opp gjennom tilfredsstillende oppdatering av planen. Denne formelle prosessen for endringskontroll skal sikre at de oppdaterte planene distribueres og styrkes gjennom regelmessig revisjon av den fullstendige planen.

Eksempler på situasjoner som kan gjøre det nødvendig å oppdatere planene, inkluderer anskaffelse av nytt utstyr eller oppgradering av operativsystem og endringer i:

- a) personell;
- b) adresser eller telefonnummer;
- c) forretningsstrategi;
- d) plassering, utstyr og ressurser;
- e) lovgivning;
- f) leverandører og viktige kunder;
- g) prosesser, eller nye/avsluttede prosedyrer;
- h) risiko (driftsmessig og finansiell).

12 Overensstemmelse

12.1 Overensstemmelse med juridiske krav

Mål: Å unngå brudd på straffelov og sivilrett, forskrifter eller kontraktmessige forpliktelser, og eventuelle krav til sikkerhet.

Design, drift, bruk og administrasjon av informasjonssystemer kan i noen tilfeller være underlagt lovbestemte, forskriftsmessige og kontraktsfestede krav til sikkerhet.

Råd om konkrete lovbestemte krav bør innhentes fra organisasjonens juridiske rådgivere eller tilstrekkelig kvalifiserte praktiserende jurister. Lovbestemte krav varierer fra land til land og for informasjon som produseres i ett land og overføres til et annet land (dvs. datastrøm over landegrensene).

12.1.1 Identifisering av relevant lovgivning

Alle relevante lover, vedtekter og kontraktmessige krav bør være tydelig definert og dokumentert for hvert enkelt informasjonssystem. Spesifikke kontroller og individenes ansvar for å etterleve disse kravene bør defineres og dokumenteres på samme måte.

12.1.2 Intellektuell eiendomsrett (IPR - Intellectual Property Rights)

12.1.2.1 Opphavsrett

Hensiktsmessige prosedyrer bør etableres for å sikre overholdelse av juridiske begrensninger på bruk av materiell som kan være berørt av intellektuelle eiendomsrettigheter, slik som opphavsrett, designrettigheter eller varemerker. Brudd på opphavsrett kan få juridiske konsekvenser som kan medføre rettsforfølgelse.

Lovbestemte vedtekter og kontraktmessige forpliktelser kan legge begrensninger på kopiering av proprietært materiell. Mer spesifikt kan de kreve at bare programvare som er utviklet av organisasjonen selv, eller som er lisensiert eller stilt til rådighet for organisasjonen av utvikler, kan benyttes.

12.1.2.2 Opphavsrett til programvare

Proprietære programvareprodukter leveres vanligvis med en lisensavtale som begrenser bruken av produktene til bestemte maskiner, og kan innskrenke kopiering til bare å gjelde sikkerhetskopier. Følgende sikringstiltak bør overveies:

- a) kunngjøring av retningslinjer for overholdelse av opphavsrett til programvare. Disse retningslinjene bør samtidig definere lovlig bruk av programvare og IT-produkter;
- b) å utarbeide standardprosedyrer for anskaffelse av programvareprodukter;
- c) å opprettholde bevissthet omkring rettigheter til programvare og prosedyrer for anskaffelse, og informere om at det vil bli iverksatt disiplinærtiltak mot ansatte som bryter dem;
- d) vedlikehold av egnede register over aktiva;
- e) oppbevaring av bevis og tegn på eierskap til lisenser, originaldisker, manualer osv.;
- f) innføring av kontrolltiltak for å sikre at maksimumsgrensen for antall tillatte brukere ikke overskrides;
- g) å kontrollere at bare autorisert programvare og lisensierte produkter er installert;
- h) utarbeidelse av retningslinjer for å opprettholde hensiktsmessig lisensbetingelser;
- i) utarbeidelse av retningslinjer for å avhende eller overføre programvare til andre;
- j) bruk av hensiktsmessige revisjonsredskaper;
- k) å overholde betingelsene og vilkårene for programvare og informasjon som anskaffes via offentlige nettverk (se også 8.7.6).

12.1.3 Beskyttelse av organisasjonens lagrede informasjon

Viktig informasjon om organisasjonen bør beskyttes mot tap, ødeleggelse og forfalskning. Noe virksomhetsinformasjon bør oppbevares trygt for å imøtekomme juridiske krav i tillegg til å støtte viktige forretningsprosesser. Eksempler på dette er informasjon som kan bli krevd fremlagt som bevis for at organisasjonen opererer innenfor lovens rammer, for å forsvare organisasjonen mot mulige rettslige forføyninger, eller for å bekrefte dens finansielle status overfor aksjonærer, partnere og revisorer. Arkivfristen og datainnholdet i informasjonen som skal oppbevares, kan bli bestemt av nasjonale lover eller vedtekter.

Arkivert informasjon bør kategoriseres etter type, for eksempel regnskapsarkiv, databasearkiv, transaksjonslogger, revisjonslogger og driftsprosedyrer, hver av dem med detaljer om arkivfrist og type lagringsmedium, for eksempel papir, mikrokort, magnetisk eller optisk. Alle kryptografiske nøkler i tilknytning til krypterte arkiver eller digitale signaturer (se 10.3.2 og 10.3.3), bør oppbevares trygt og gjøres tilgjengelig for autorisert personell ved behov.

Oppmerksomhet bør også vies til muligheten for forringelse av lagringsmedia for informasjon. Lagrings- og håndteringsprosedyrer bør utarbeides i henhold til produsentens anbefalinger.

Dersom elektroniske lagringsmedia velges, bør det utvikles prosedyrer for å sikre tilgang til data (lesbarhet for både media og format) i hele oppbevaringsperioden, for på den måten å beskytte mot tap som følge av fremtidige teknologiske endringer.

Lagringsystemer for data bør velges slik at nødvendige data kan gjenopprettes på en måte som er akseptabel for en domstol, for eksempel slik at alle arkiver kan gjenopprettes innenfor en akseptabel tidsfrist og i et akseptabelt format.

Systemet for lagring og håndtering bør sikre tydelig merking av registre og av lovfestede eller vedtektsmessige arkiveringsfrister. Det bør tillate hensiktsmessig ødeleggelse av registre etter denne fristens utløp hvis organisasjonen ikke har bruk for den.

For å imøtekomme disse forpliktelsene bør organisasjonen gjennomføre følgende tiltak:

- a) Det bør utstedes retningslinjer for oppbevaringstid, lagring, bruk og makulering av dokumenter og informasjon.
- b) Det bør utarbeides lagringsplaner som identifiserer viktige typer av dokumenter og spesifiserer hvor lenge de skal oppbevares.
- c) Det bør utarbeides en oversikt over kilder til viktig informasjon.
- d) Det bør iverksettes hensiktsmessige forholdsregler for å beskytte viktig dokumenter og informasjoner mot tap, ødeleggelse og forfalskning.

12.1.4 Sikring av data og beskyttelse av personopplysninger

En rekke land har innført lovgivning som regulerer behandling og overføring av persondata (vanligvis informasjon om levende mennesker som kan identifiseres ut fra denne informasjonen). Slike kontroller kan medføre forpliktelser for dem som samler inn, behandler og sprer personinformasjon, og kan også begrense mulighetene for å overføre slike data til andre land.

Overholdelse av lovgivning om databeskyttelse krever hensiktsmessige strukturer og kontrolltiltak fra ledelsens side. Ofte oppnås dette best ved å utnevne én person som står ansvarlig for databeskyttelse, og som skal gi rettleiding til ledere, brukere og tjenesteleverandører om deres individuelle ansvar og om prosedyrene som skal følges. Det bør være dataeierens ansvar å informere vedkommende person om eventuelle forslag om å oppbevare personinformasjon i strukturerte filer, så vel som å sørge for nødvendig bevissthet omkring prinsippene for databeskyttelse som er definert i det aktuelle lovverket.

12.1.5 Sikringstiltak mot misbruk av informasjonssystemene

Informasjonssystemene i en organisasjon er utviklet for virksomhetsformål. Bruken av disse bør autoriseres av ledelsen. Enhver bruk av disse systemene for ikke-virksomhetsrelaterte eller uautoriserte

formål uten godkjenning fra ledelsen bør betraktes som utilbørlig bruk av systemene. Hvis slik aktivitet avdekkes gjennom overvåkning eller på andre måter, bør ledelsen informeres slik at nødvendige disiplinære tiltak kan iverksettes.

Lovgivningen som regulerer overvåkning av arbeidstakere, varierer fra land til land og kan kreve at de ansatte blir informert om slik overvåkning, eller at deres tillatelse innhentes. Juridiske råd bør innhentes før overvåkningsprosedyrer iverksettes.

Mange land har etablert, eller er i ferd med å etablere, lovgivning for å beskytte mot datakriminalitet. Det kan være en forbrytelse å bruke en datamaskin til uautoriserte formål. Det er derfor viktig at alle brukere er oppmerksomme på nøyaktig hva deres tilgangsrettigheter omfatter. Dette kan man for eksempel gjøre ved å gi brukerne skriftlig autorisasjon som de signerer en kopi av og leverer tilbake til organisasjonen for forsvarlig oppbevaring. Ansatte i organisasjonen og tredjeparts brukere bør gjøres oppmerksomme på at ingen tilgang er tillatt ut over den som er autorisert.

Ved pålogging bør det komme opp en advarsel på dataskjermen som forteller at systemet man har logget seg på, er privat, og at uautorisert tilgang er forbudt. Brukeren bør godta og svare bekreftende på beskjeden på skjermen for å kunne fortsette påloggingen.

12.1.6 Regulering av kryptografisk kontroll

Enkelte land har iverksatt avtaler, lover, reguleringer eller andre tiltak for å kontrollere tilgangen til eller bruken av kryptografiske kontroller. Slike sikringstiltak kan omfatte:

- a) import og/eller eksport av maskinvare og programvare for å utføre kryptografiske funksjoner;
- b) import og/eller eksport av maskinvare og programvare som er utformet for å kunne utvides med kryptografiske funksjoner;
- c) obligatoriske eller frivillige metoder som gir landene tilgang til informasjon som er kryptert av maskinvare eller programvare for å sikre innholdets konfidensialitet.

Juridiske råd bør innhentes for å sikre at nasjonale lover overholdes. Juridiske råd bør også søkes før kryptert informasjon eller kryptografiske kontroller flyttes til et annet land.

12.1.7 Innsamling av bevis

12.1.7.1 Regler for bevisførsel

Det er nødvendig å sikre tilstrekkelig bevis for å begrunne sanksjoner mot enkeltpersoner eller organisasjoner. Når disse sanksjonene er et internt disiplinært anliggende, er kravene til bevisførsel beskrevet i interne rutiner.

I de tilfeller der loven trekkes inn - enten det dreier seg om sivilrett eller straffelov - bør bevisene som legges frem, være i overensstemmelse med reglene for bevisførsel i den aktuelle loven eller for den enkelte domstolen der saken skal prøves. Generelt omfatter disse reglene:

- a) regler for hva som kan legges frem som bevis, hvorvidt bevisene kan brukes i en rettssal eller ei;
- b) vekten av bevis: bevisenes kvalitet og fullstendighet;
- c) tilstrekkelig bevis for at kontrollmekanismene har fungert korrekt og konsekvent (dvs. bevis for prosesskontroll) i den perioden da bevisene som skal hentes frem, ble lagret og behandlet av systemet.

12.1.7.2 Bevisenes gyldighet

For at bevisene skal kunne legges frem for en domstol, bør organisasjonen sikre at informasjonssystemene er i overensstemmelse med alle offentlige standarder og prosedyrer for fremleggelse av gyldige bevis.

12.1.7.3 Bevisenes kvalitet og fullstendighet

For å sikre bevisenes kvalitet og fullstendighet behøves dekkende revisjonsspor. I allminnelighet kan slike spor etableres under følgende forhold:

- a) For papirdokumenter: Originalen blir forsvarlig oppbevart, og det føres journal over hvem som fant den, når den ble funnet, og hvem som var vitne til oppdagelsen. En eventuell etterforskning bør sikre at originalene ikke blir endret eller tuklet med.
- b) For informasjon som er lagret på datamedia: Det bør tas kopier av alle flyttbare media, innholdet på harddisker og i minnet for å sikre tilgjengelighet. Logg over alle handlinger under kopieringsprosessen bør oppbevares, og det bør være vitner til stede under prosessen. En kopi av mediet og loggen bør oppbevares forsvarlig.

Når en hendelse blir oppdaget, er det kanskje ikke tydelig at den vil ende med mulig søksmål. Det er derfor en fare for at avgjørende bevis blir forspilt ved et uhell før hendelsens omfang blir avdekket. Det anbefales å koble inn advokat eller politi tidlig i eventuelle planlagte søksmål og innhente råd om hvilke typer bevis som kreves.

12.2 Gjennomgang av sikkerhetspolitikk og samsvar med tekniske krav

Mål: Å sikre samsvar mellom informasjonssystemene og virksomhetens sikkerhetspolitikk og standarder.

Informasjonssystemenes sikkerhet bør revideres jevnlig.

Slike revisjoner bør ta utgangspunkt i organisasjonens sikkerhetspolitikk, og de tekniske plattformene og informasjonssystemene bør kontrolleres for å sikre overensstemmelse med iverksatte sikkerhetsstandarder.

12.2.1 Samsvar med sikkerhetspolicy

Ledere bør sørge for at alle sikkerhetsprosedyrer innenfor deres ansvarsområde blir korrekt utført. Dessuten bør alle områder innenfor organisasjonen revideres jevnlig for å sikre at de er i overensstemmelse med organisasjonens sikkerhetspolicy og -standarder. Disse bør omfatte følgende:

- a) informasjonssystemer;
- b) systemleverandører;
- c) eiere av data og informasjonsaktiva;
- d) brukere;
- e) ledelsen.

Informasjonssystemenes eiere (se 5.1) bør sørge for regelmessig revisjon av sine informasjonssystemer for å sikre at de er i overensstemmelse med organisasjonens sikkerhetspolitikk, standarder og eventuelle andre sikkerhetskrav. Driftsovervåking av systembruk er dekket i 9.7.

12.2.2 Samsvar med tekniske krav

Informasjonssystemer bør kontrolleres jevnlig for å sikre at de er i samsvar med kravene i de vedtatte sikkerhetsstandardene. Teknisk kompatibilitetskontroll omfatter inspeksjon av produksjonssystemene for å sikre at maskin- og programvarebaserte kontroller er gjennomført på korrekt måte. Denne typen kompatibilitetskontroll krever teknisk spesialkompetanse. Den bør utføres manuelt (støttet av egnede programvareredskaper) av en erfaren systemingeniør, eller ved hjelp av en automatisert programvarepakke som genererer en teknisk rapport som danner grunnlag for videre undersøkelser av en teknisk ekspert.

Kompatibilitetskontroll omfatter dessuten bl.a. infiltrasjonstester, som kan utføres av uavhengige eksperter som er spesielt innleid for dette formålet. Dette kan være nyttig for å avdekke svakheter i systemet, og for å undersøke hvor effektive kontrolltiltakene er til å hindre uautorisert tilgang som følge

av de avdekkede svakhetene. Det bør utvises forsiktighet i tilfelle en slik vellykket infiltrasjonstest skulle kompromittere systemets sikkerhet eller uforvarende utnytte andre svakheter.

Slike tekniske kompatibilitetskontroller bør bare utføres eller overvåkes av kvalifisert personell.

12.3 Hensyn ved systemrevisjon

Mål: Å redusere forstyrrelser på/fra systemrevisjonsprosessen og maksimere dens effektivitet.

Det bør foretas kontroller for å sikre produksjonssystemer og revisjonsverktøy i forbindelse med systemrevisjon.

Sikringstiltak er også nødvendig for å beskytte integriteten til og unngå misbruk av revisjonsverktøyene.

12.3.1 Revisjonskontroller

Revisjonskrav og -aktiviteter som innebærer kontroll av produksjonssystemer, bør planlegges nøye og avtales på forhånd for å redusere faren for forstyrrelser i den daglige driften. Følgende punkter bør tas i betraktning:

- a) Revisjonskravene bør avtales med den relevante ledelsen.
- b) Målet med revisjonen bør være avtalt og kontrollert.
- c) Kontrollene bør bare ha lesetilgang til programmer og data.
- d) Andre typer tilgang (enn lesetilgang) bør bare tillates på separate kopier av systemfiler, som skal slettes etter at revisjonen er gjennomført.
- e) IT-ressursene som kreves for å utføre kontrollene, bør på forhånd identifiseres og gjøres tilgjengelige.
- f) Behov for spesiell eller ytterligere behandling bør identifiseres og avtales på forhånd.
- g) All tilgang bør overvåkes og loggføres for å sikre referansespor.
- h) Alle prosedyrer, krav og ansvarsforhold bør dokumenteres.

12.3.2 Beskyttelse av revisjonsverktøy

Tilgang til revisjonsverktøy, dvs. programvare eller datafiler, bør beskyttes for å hindre mulig misbruk eller kompromittering. Disse verktøyene bør holdes adskilt fra utviklings- og produksjonssystemer og ikke oppbevares i tapearkiv eller brukeroråder med mindre de gis et tilfredsstillende nivå av ekstra sikkerhetsbeskyttelse.