Retningslinjer for risikovurdering og konsekvensanalyse

Når der er indgået en databehandleraftale med den leverandør, følger en række afledte opgaver, herunder pligten til at foretage en risikovurdering og føre tilsyn med databehandleren.

# Risikovurdering af databehandling

Et af grundprincipperne i databeskyttelsesforordningen (GDPR) er, at virksomheder og offentlige myndigheder skal have en risikobaseret tilgang til behandling af personoplysninger. Det fremgår af artikel 24 i GDPR, at det skal vurderes, hvilken risiko der er for de registrerede (dvs. dem der behandles oplysninger om) ved behandlingen af deres personoplysninger. På baggrund af den vurdering skal det sikres, at personoplysningerne beskyttes tilstrækkeligt via organisatoriske og tekniske foranstaltninger. Risikovurderingen skal dermed sikre at man dels lever op til reglerne og dels sikre at ens behandling af persondata ikke udgør en væsentlig risiko for de personer, hvis data man behandler. Hvis dette er tilfældet og der forekommer sikkerhedsbrud, så kan man blive ramt af hårde bødestraffe.

Der skal foretages en risikovurdering, hvis der f.eks. indkøbes et nyt it-system eller hvis man ændrer- eller påbegynder en ny arbejdsgang/proces. Kravene til niveauet for risikovurderingen afhænger af, hvad det er, der skal risikovurderes. Hvis der f.eks. skal tages et nyt fagsystem i brug, som skal behandle mange og følsomme personoplysninger, er det vigtigt at lave en grundig risikovurdering.

En risikovurdering afklarer forholdet mellem sandsynligheden for at den registreredes rettigheder bliver kompromitteret og en vurdering af konsekvensen af hvis det sker.

En risiko for en registreredes rettigheder kan eksempelvis være identitetstyveri, tab af ære og velfærd, men rettighederne dækker meget bredt. En forholdsregel kunne f.eks. være kryptering af kommunikation, kontroller der sikrer at e-mails kun afsendes til den tilsigtede modtager eller lignende.

## Kortlægning af de risici behandlingen medfører

Ved kortlægning af de risici der er forbundet med behandlingen af data, skal alle de forhold der kan påvirke fortrolighed, tilgængelighed eller integritet identificeres.

* Fortrolighed betyder, at informationer skal beskyttes mod uautoriseret adgang eller videregivelse således, at uvedkommende får adgang til oplysningerne (fx beskyttelse mod hackere eller videregivelse til forkerte).
* Tilgængelighed betyder, at væsentlige informationer skal være tilgængelige for de ansatte, som har retmæssig adgang til dem. Et brud på tilgængelighed kan således være, hvis et IT-system går ned, så væsentlige oplysninger om en bestemt borgergruppe ikke er tilgængelige for de ansatte i en periode.
* Integritet betyder, at det skal sikres, at personoplysninger ikke slettes eller ændres ved et uheld eller uautoriseret.

Udgangspunktet er, at behandling af personoplysninger, er forbundet med risici for de registrerede. Disse risici skal identificeres med det formål at etableres et sikkerhedsniveau af passende tekniske og organisatoriske foranstaltninger som passer til risikovurderingen.

Risikoidentifikation er en systematisk proces, hvor man med fordel kan overveje om databehandlingen kan have konsekvenser på følgende områder:

* Fysisk skade
* Materiel skade
* Immateriel skade
* Forskelsbehandling
* Identitetstyveri
* Identitetssvig
* Økonomiske konsekvenser
* Skade på omdømme
* Sociale konsekvenser
* Indflydelse på privatliv
* Skade på menneskelig værdighed
* Skade på legitime interesser
* Begrænsning/krænkelse af fundamentale rettigheder og frihedsrettigheder
* Forhindring i udøvelse af kontrol med egne personoplysninger

## Risikovurdering

Risikovurderingen skal måle størrelsen af de identificerede risici ud fra sandsynligheden for at risikoen indtræffer og en vurdering af konsekvensen hvis risikoen sker. Metodevalg og beskrivelser muliggør sammenlignelige og reproducerbare resultater.

Der er valgt en kvalitativ vurderingsmetode med en skala fra 1-4 til at rangordne og indplacere hændelser.

Skalaen er udarbejdet med inspiration fra ENISAs publikation ”Handbook on security of personal data processing” udgivet i december 2017 og dækker over følgende trin og vurderingsgrundlag til indplacering af sandsynlighed og konsekvens:

|  |  |  |
| --- | --- | --- |
|  | **Sandsynlighed** | **Konsekvens** |
| **1** | **Usandsynligt**Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme* Ingen erfaring med hændelsen
* Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark
 | **Ubetydelig (uvæsentlig)**De registrerede kan opleve få uhensigtsmæssigheder, der kan overkommes og imødegås uden større indsats * Konsekvenserne kan være ressourcetræk til at genindtaste oplysninger, dårlig brugeroplevelse, irritation og lignende
 |
| **2** | **Mindre sandsynligt**Hændelsen forventes ikke at komme* Ingen erfaring med hændelsen
* Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark
 | **Mindre alvorlig (generende)**De registrerede kan opleve betydelige uhensigtsmæssigheder, som de kan overkomme med en indsats og overvindelse af nogle få besværligheder* Konsekvenserne kan være ekstra omkostninger, manglende adgang til forretningsservices, frygt, mangel på forståelse, stress og mindre påvirkning af fysisk karakter og lignende
 |
| **3** | **Sandsynligt**Det er sandsynligt at hændelsen vil forekomme* Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder
* Kendes fra andre offentlige og private virksomheder i Danmark (omtales årligt i pressen)
 | **Meget alvorlig (kritisk)**De registrerede kan opleve betydelige konsekvenser, som kun kan overkommes med betydelig indsats og konsekvens for den enkelte * Konsekvenserne kan være betydelige økonomiske tab, fejlkontering af midler sortlistning eller nedgradering i kreditmuligheder, fysisk skade på aktiver påvirkning af arbejdssituationer stævning, dårligere helbred og lignende
 |
| **4** | **Forventet**Det ventes at hændelsen vil forekomme* Man har erfaring med hændelsen inden for de sidste 12 måneder
* Hænder jævnligt i andre offentlige og private virksomheder (omtales ofte i pressen)
 | **Graverende/ødelæggende (uacceptabelt)**De registrerede kan opleve betydelige og indgribende konsekvenser, som det ikke er muligt eller kun vanskeligt muligt at overkomme * Konsekvenserne kan være mistet erhvervsevne, langvarig fysiske og psykiske påvirkninger, død, og lignende
 |

Risikotallet opnås ved at gange værdien for den forventede sandsynlighed med værdien af den forventede konsekvens.

|  |  |
| --- | --- |
|  | **Sandsynlighed** |
| **Konsekvens** |  | Usandsynligt | Mindre sandsynligt | Sandsynligt | Forventet |
| Lav  | 1 | 2 | 3 | 4 |
| Middel | 2 | 4 | 6 | 8 |
| Høj | 3 | 6 | 9   | 12   |
| Meget høj | 4 | 8 | 12 | 16 |

## Risikotolerance

Indplacering af en risiko og dermed beregningen af risikotallet, bygger på den risikotolerance Ishøj Kommune har besluttet, og er ledelsens udtryk for hvad organisationen er villig til at påtage sig af risiko.

Risikotolerancen er valgt som en afvejning mellem et ønske om høj sikkerhed for de registrerede under hensyn til den værdi databehandling kan bidrage med.

Risikovurdering af sandsynlighed og konsekvens sker i en farveskala, baseret på kategorierne lav (grøn), mellem (gul) og høj (rød) og med en beregnet risiko fra 1-16.

Med udgangspunkt heri er der besluttet følgende risikotolerance:

* Grøn er udtryk for en lav risiko, på 5 eller derunder, hvor risici umiddelbart kan accepteres af ledelsen.
* Gul er udtryk for en mellem risiko, fra 6 til og med 8. Her vurderer ledelsen fra gang til gang, om man kan acceptere risikoen eller om man vil gøre noget for at nedbringe den, eksempelvis ved at indføre ekstra foranstaltninger.
* Rød er udtryk for en høj risiko, på 9 eller derover. Her skal der gøres noget for at håndtere risikoen.

## Risikohåndtering

Som en del af risikohåndteringen udarbejdes en plan for, hvordan de identificerede risici skal håndteres. Risici kan håndteres på fire måder:

### Accept

Organisationen accepterer at lever med risikoen og der foretages derfor ikke yderligere. Dette vælges når:

* Risikoen falder ind under risikotolerance
* Omkostningerne ved at reducere risikoen overstiger risikoens fordele
* Risikoen er stor, men der kan ikke identificeres passende foranstaltninger

### Flyt:

Risikoen overføres til en tredjepart, fx ved hjælp af forsikring, outsourcing eller lignende. Dette vælges oftest når det er den mest økonomisk fordelagtige løsning eller når der mangler kompetencer internt i organisationen.

### Undgå:

Risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen, hvorved eksponering for risikoen forsøges undgået. Dette vælges når:

* omkostningerne ved konsekvensen af en hændelse overstiger risikoens fordele
* risikoen er stor og der ikke kan identificeres passende foranstaltninger

### Forøg/mindske:

Risikoen kontrolleres ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne, hvorved risikoen håndteres. Dette vælges når det er muligt at implementere-, fjerne- eller rette på foranstaltninger.

## Foranstaltninger

Ifølge GDPR-forordningens princip nr. 6 om Integritet og fortrolighed skal der sikres passende tekniske og organisatoriske sikkerhedsforanstaltninger til at skabe tilstrækkelig sikkerhed for personoplysningerne.

Der findes fire typer foranstaltninger

* Organisatoriske (politiker og procedurer)
* Tekniske (firewall, kryptering, back-up, anti-virus, segmentering, Anonymisering/ pseudonymisering)
* Adfærdsmæssige (screening, awareness, ansvar, kompetencer)
* Fysiske (sikre zoner, aflåsning, adgangskontrol/adgangsbegrænsning, ryddeligt skrivebord)

Foranstaltningerne kan være forebyggende, opdagende, korrigerende eller en blanding af en eller flere af disse.

Har risikovurderingen vist, at der er behov for at implementere foranstaltninger til reducering af risici skal det overvejes hvilke foranstaltninger der med udgangspunkt i risikoprofilen set fra de registreredes perspektiv, skønnes nødvendige, for at bringe de registreredes risiko ved den dataansvarliges konkrete behandlinger ned på et acceptabelt niveau.

Foranstaltninger kan både implementeres hos dataansvarlig og databehandler, alt efter hvad der giver mening i det konkrete tilfælde.

Med ”passende” skal forstås, at udvælgelsen og implementeringen af foranstaltninger skal det ske ud fra en cost/benefit-vurdering, så kontrollernes effekt på risikoen vurderes i forhold til omkostningerne.

Der er ingen genveje i form af lister over foranstaltninger, som man bare kan implementere, for det vil være en konkret vurdering fra risici til risici, hvilke foranstaltninger man vurderer kan nedsætte risikoen til et acceptabelt niveau.

Der findes dog flere inspirationskilder til at udpege relevante foranstaltninger. En af disse kilder er Anneks A i ISO27001 Standarden (ISO 27002) som indeholder 114 foranstaltninger der omfatter anbefalinger til politikker, processer, procedurer, organisationsstrukturer samt software- og hardware-funktioner. Overblik over disse findes i Bilag 1.

Udvælgelsen af foranstaltninger bør foregå i en god dialog mellem dataansvarlig og databehandler.

**Opfølgning på foranstaltninger**

I forbindelse med beslutning om hvilke foranstaltninger der skal iværksættes er det vigtigt at beslutte, hvordan der følges på om foranstaltningerne sikrer den ønskede effekt, hvem der følger op og hvornår der følges op.

**Eksempel på risiko og foranstaltninger:**

**Fortrolighed**

Det har en høj konsekvens for en borger, som bor på krisecenter, hvis denne oplysning deles med uvedkommende, fx vedkommendes tidligere partner. Sandsynligheden for at dette sker afhænger af, hvor godt vi beskytter oplysningerne.

*Foranstaltninger:* For at nedsætte risikoen kan man vælge, at denne type information kun må opbevares i et sikret system (ikke fysisk), at meget få ansatte må have adgang til informationerne i systemet (adgangsbegrænsning) samt udarbejde konkrete procedurer for håndtering af disse oplysninger.

**Tilgængelighed**
Det har en høj konsekvens for borgerne på et plejehjem, hvis medarbejderne ikke kan tilgå deres medicinoplysninger. Det er samtidig sandsynligt, at systemet med medicinoplysninger går ned. Dette vil derfor have et højt risikotal.

*Foranstaltninger:* For at nedsætte risikoen kan man printe en fysiske medicinliste dagligt, så oplysningerne er tilgængelige, selvom systemet går ned. Herved nedsættes sandsynligheden (og derved også den samlede risiko) for, at vi ikke kan få fat i oplysningerne.

**Integritet**
Det har en høj konsekvens for børnene i et dagtilbud, hvis personalet ikke kan stole på rigtigheden af de oplysningerne de har omkring børnenes allergier. Det er samtidig sandsynligt, at de ikke kan huske alle allergier i hovedet.

*Foranstaltninger:* Risikoen kan nedsættes ved at have en liste med allergier hængende ude i køkkenet og en procedure omkring, at frokosten portionsanrettes af køkkenpersonalet på navngivne tallerkener til børn *med allergier.*

# Konsekvensanalyse

I forbindelse med visse behandlingsaktiviteter, hvor der via en risikovurdering er fundet frem til en høj risiko for de registreredes rettigheder, skal der udarbejdes en konsekvensanalyse, som også kaldes en DPIA (data protection impact assessment). I konsekvensanalysen går man i dybden med konsekvenserne for de registrerede og mulige foranstaltninger for at mindske risikoen. Hvis det ikke er muligt at mindske risikoen for de registrerede, skal man søge Datatilsynet om tilladelse til at udføre behandlingen.

Det er et krav i GDPR, at kommunens databeskyttelsesrådgiver (DPO) inddrages i forbindelse med konsekvensanalyser.

Konsekvensanalysen skal kun udarbejdes, når der er tale om behandlinger, som er særligt risikobetonede, og dette skal ske før, behandlingen af personoplysningerne starter.

Risikovurderingen skal dermed have vist, at der er en høj risiko for de registreredes rettigheder og frihedsrettigheder. Desuden skal et af nedenstående forhold være opfyldt:

* Der er en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person
* Der foretages behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10
* Der foretages systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Datatilsynet har udarbejdet en liste over, hvornår de vurderer, at det er obligatorisk at lave en konsekvensanalyse, som vægter følgende elementer:

* Behandling af biometriske data til identifikation.
* Behandling af genetiske data.
* Behandling af lokationsdata.
* Behandlingen leder til høj risiko for de registrerede.
* Behandlingen sker med innovativ teknologi.
* Behandling sker med det formål at træffe automatiske afgørelser i forhold til produkter, services, muligheder eller fordele.
* Behandlingen profilerer registrerede i stort omfang.
* Behandling af sårbare registrerede eller omfattende følsomme oplysninger til automatiserede afgørelser og behandlinger, hvor der kan være en direkte konsekvens for registreredes helbred eller sikkerhed.
* Tilsvarende har de andre EU-landes Datatilsyn lavet positivlister for, hvornår der skal laves konsekvensanalyser. Det vil være de færreste organisationer, som kommer til at lave større mængder af konsekvensanalyser.

**Indhold i konsekvensanalysen:**

I konsekvensanalysen skal der redegøres for:

* De planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige
* Om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene
* Risiciene for de registreredes rettigheder og frihedsrettigheder og
* De foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne forordning, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Hvis risiciene ikke kan reduceres tilstrækkeligt, skal der desuden foretages forudgående høring hos tilsynsmyndigheden (Datatilsynet). Tilsynet skal efterfølgende rådgive organisationen og kan kræve alle andre nødvendige oplysninger i sagen forelagt.

# Årlig gennemgang af risikovurderinger

Risikovurderinger bør gennemgås årligt for at sikre, at personoplysningerne fortsat er beskyttede. Hvis risikobilledet har ændret sig, kan det være nødvendigt at introducere nye foranstaltninger.

# Bilag 1: Foranstaltninger

ISO27001 standarden indeholder Anneks A som opstiller 14 risikoområder og 114 kontrolforanstaltninger der kan anvendes som inspiration, hvis risikovurderingen har vist det nødvendigt at implementere foranstaltninger.

|  |
| --- |
| **A.5 Informationssikkerhedspolitikker** |
| **A.5.1 retningslinjer for styring af informationssikkerhed**  |
| Formål: At give retningslinjer for og understøtte informationssikkerhed i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter. |
|  | *kontrol* |
| A.5.1.1 | Politikker for informationssikkerhed | Ledelsen skal fastlægge og godkende et sæt politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere of relevante eksterne parter. |
| A.5.1.2 | Gennemgang af politikker for informationssikkerhed  | Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkeligt og resultatrelaterede effektivitet. |

|  |
| --- |
| **A.6 Organisering af informationssikkerhed** |
| **A.6.1 Intern organisering** |
| Formål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen. |
|  | *Kontrol* |
| A.6.1.1 | Roller og ansvarsområder for informationssikkerhed | Alle ansvarsområder for informationssikkerhed skal defineres og fordeles. |
| A.6.1.2  | Funktionsadskillelse | Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver. |
| A.6.1.3 | Kontakt med myndigheder | Der skal opretholdes passende kontakt med særlige relevante myndigheder. |
| A.6.1.4 | Kontakt med særlige interessegrupper | Der skal opretholdes passende kontakt med særlige interessegrupper eller andre faglige organisationer. |
| A.6.1.5 | Informationssikkerhed ved projektstyring | Informationssikkerhed skal anvendes ved projektstyring, uanset projekttype. |
| **A.6.2 Mobilt udstyr og fjernarbejdspladser**  |
| Formål: At sikre fjernarbejdspladser og brugen af mobilt udstyr |
|  | *Kontrol* |
| A.6.2.1 | Politik for mobilt udstyr | Der skal vedtages en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr |
| A.6.2.2  | Fjernarbejdspladser | Der skal implementeres en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandler eller lagres på fjernarbejdspladser.  |

|  |
| --- |
| **A.7 Personalesikkerhed** |
| **A.7.1 Før ansættelse** |
| Formål: At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.  |
|  | *Kontrol* |
| A.7.1 | Screening | Efterprøvning af alle jobkandidaters baggrund skal udføres i overensstemmelse med relevante love, forskrifter og etiske regler og skal stå i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang, til, og de relevante risici |
| A.7.2 | Ansættelsesvilkår og betingelser | Kontakter med medarbejder og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed. |
| **A.7.2 Under ansættelsen** |
| Formål: At sikre, at medarbejdere og kontrahenter er bevidste om og levr op til deres informationssikkerhedsansvar. |
|  | *Kontrol* |
| A.7.2.1 | Ledelsesansvar | Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer |
| A.7.2.2 | Bevidsthed om, uddannelse og træning i informationssikkerhed | Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer |
| A.7.2.3 | Sanktioner | Der skal være etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud  |
| **A.7.3 Ansættelsesforholdets ophør eller ændring**  |
| Formål: At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør |
|  | *Kontrol* |
| A.7.3.1  | Ansættelsesforholdets ophør eller ændring | Informationssikkerhedsansvar og forpligtelser, som gælder efter ansættelsen ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten  |

|  |
| --- |
| **A.8 Styring af aktiver** |
| **A.8.1 Ansvar for aktiver** |
| Formål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse af heraf. |
|  | *Kontrol* |
| A.8.1.1  | Fortegnelse over aktiver | Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver. |
| A.8.1.2  | Ejerskab af aktiver | Der skal udpeges en ejer i organisationen for hvert aktiv. |
| A.8.1.3  | Accepter brug af aktiver | Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, dokumenteres og implementeres  |
| A.8.1.4  | Tilbagelevering af aktiver | Alle medarbejder og eksterne brugere skal aflevere alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophøre. |
| **A.8.2 Klassifikation af information** |
| Formål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen. |
|  | *Kontrol* |
| A.8.2.1  | Klassifikation af information | Information skal klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring. |
| A.8.2.2 | Mærkning af information | Der skal udarbejdes og implementeres et passende sæt af procedure til mærkning af information i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget. |
| A.8.3.3 | Håndtering af aktiver | Der skal udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget. |
| **A.8.3 Mediehåndtering** |
| Formål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier. |
|  | *Kontrol* |
| A.8.3.1 | Styring af bærbare medier | Der skal implementeres procedure til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget. |
| A.8.3.2 | Bortskaffelse af medier | Medier skal bortskaffes på forsvarlige vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.  |
| A.8.3.3 | Fysiske medier under transport | Medier, der indeholder information, skal beskyttes mod autoriseret adgang, misbrug eller ødelæggelse under transport. |

|  |
| --- |
|  **A.9 Adgangsstyring** |
| **A.9.1 Forretningsmæssige krav til adgangsstyring**  |
| Formål: At begrænse adgang til information oginformationsbehandlingsfaciliteter |
|  | *Kontrol* |
| A.9.1.1 | Politik for adgangsstyring | En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.  |
| A.9.1.2 | Adgang til netværk og netværkstjenester | Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.  |
| **A.9.2 Administration af brugeradgang**  |
| Formål: At sikre adgang for autoriserede bruger og forhindre uautoriseret adgang til systemer og tjenester  |
|  | *Kontrol* |
| A.9.2.1  | Brugerregistrering og - afmelding | Der skal implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder. |
| A.9.2.2  | Tildeling af brugeradgang | Der skal implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.  |
| A.9.2.3 | Styring af privilegerede adgangsrettigheder | Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænse og styres. |
| A.9.2.4 | Styring af hemmelig autentifikationsinformation om brugere | Tildeling af hemmelig autentifikationsinformation skal styres ved hjælp af en formel administrationsproces. |
| A.9.2.5 | Gennemgang af brugeradgangsrettigheder | Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder.  |
| A.9.2.6 | Inddragelse eller justering af adgangsrettigheder | Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når deres ansættelsesforhold, kontakt eller aftale ophører, eller skal tilpasses efter en ændring.  |
| **A.9.3 Brugernes ansvar** |
| Formål: At gøre brugere ansvarlige for at sikre deres autentifikationsformation. |
|  | *Kontrol* |
| A.9.3.1  | Bruger adgang til informationer. | Der skal være et krav, at brugere følger organisationens praksis ved anvendelsen af hemmelig autentifikationsformation. |
| **A.9.4 Styring af system- og applikationsadgang**  |
| Formål: At forhindre uautoriseret adgang til systemer og applikationer. |
|  | *Kontrol* |
| A.9.4.1  | Begrænset adgang til informationer | Adgang til information og applikationssystemers funktioner skal begrænses i overensstemmelse med politikken for adgangsstyring. |
| A.9.4.2  | Procedurer for sikker log-on | Hvis det kræves i henhold til politikken for adgangsstyring, skal adgang til systemer og applikationer styres af en procedure for sikker log-on. |
| A.9.4.3  | System for administration af adgangskoder | Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder med god kvalitet.  |
| A.9.4.4  | Brug af privilegerede systemprogrammer | Brugen af systemprogrammer, der kan omgå system- og applikation kontroller, skal begrænses og styres effektivt.  |
| A.9.4.5  | Styring af adgang til kildekoder til programmer | Adgang til kildekoder til programmer skal bægrenes. |

|  |
| --- |
| **A.10 Kryptografi** |
| **A.10.1 Kryptografiske kontroller** |
| Formål: At sikre korrekt og effektiv brug af kryptografi for at beskytte information fortrolighed, autenticitet og/eller integritet.  |
|  | *Kontrol* |
| A.10.1.1  | Politik for anvendelse af kryptografi | Der skal udarbejdes og implementeres en politik for anvendelse af kryptografi til beskyttelse af information. |
| A.10.1.2  | Administration af nøgler | Der skal udarbejdes og implementeres en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus. |

|  |
| --- |
| **A.11 Fysisk sikring og miljøsikring**  |
| **A.11.1 Sikre områder** |
| Formål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter. |
|  | *Kontrol* |
| A.11.1.1 | Fysisk perimetersikring | Der skal defineres og defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter. |
| A.11.1.2 | Fysisk perimetersikring | Sikre områder skal være beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang. |
| A.11.1.3 | Sikring af kontorer, lokaler og faciliteter | Fysisk sikring kontorer, lokaler og faciliteter skal tilrettelægges og etableres.  |
|  |
| A.11.1.4 | Beskyttelse mod eksterne og miljømæssige trusler | Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker skal tilrettelægges og etableres  |
| A.11.1.5 | Arbejd sikre områder | Procedure for arbejde i sikre områder skal tilrettelægges og etableres. |
| A.11.1.6 | områder til af- og pålæsning | Adgangssteder som fx områder til af- og pålæsning og andre steder, hvor uautoriseret personer kan komme ind på området, skal styres og så vidt muligt adskilles fra informationsbehandlingsfaciliteter for at undgå uautoriseret adgang.  |
| A.11.2.7  | Sikker bortskaffelse eller genbrug af udstyr | Alt udstyr med læringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelsen eller genbrug. |
| A.11.2.8  | Brugerudstyr og opsyn | Bruger skal sikre, at udstyr, som er uden opsyn, er passende beskyttet.  |
| A.11.2.9  | Politik for ryddeligt skrivebord og blank skærm | Der skal udarbejdes en politik om at holde skriveborde ryddet for papir og flyttebare læringsmedier og om blank på skærm på informationsbehandlingsfaciliteter. |

|  |
| --- |
| **A.12 Driftsikkerhed**  |
| **A.12.1 Drift procedure og ansvarsområder** |
| Formål: At sikre korrekt og sikker drift informationsbehandlingsfaciliteter  |
|  | *Kontrol* |
| A.12.1.1 | Dokumenterede driftsprocedure | Driftsprocedure skal dokumenteres og gøres tilgængelige for alle burgere, der har brug for dem. |
| A.12.1.2  | Ændringsstyring | Ændring af organisationen, forhindringsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, skal styres. |
| A.12.1.3  | Kapacitetsstyring | Anvendelsen af ressourcer skal overgås og tilpasses, og der skal foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet |
| **A.12.2 Beskyttelse mod malware**  |
| Formål: At sikre, at information og informationsbehandlingsfaciliteter  |
|  | *Kontrol* |
| A.12.2.1  | Kontroller mod malware | Der skal implementeres kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed. |
| **A.12.3 backup** |
| Formål: At beskytte mod tab og data |
|  | *Kontrol* |
| A.12.3.1 | Backup af information | Der skal tages backupkopier af information, software og system billeder, og disse skal testes regelmæssigt i overensstemmelse med den aftale backuppolitik. |
| **A.12.4 Login og overvågning** |
| Formål: At registrere hændelser og tilvejebringe bevis.  |
|  | *Kontrol* |
| A.12.4.1 | Hændelseslogin | Hændelseslogin til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser skal udføres, opbevares og gennemgås regelmæssigt. |
| A.12.4.2  | Beskyttelse af log- oplysninger | Logningsfaciliter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang. |
| A.12.4.3  | Administrator- og operatørlog  | Aktiviteter udført af systemadministrator og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang.  |
| A.12.4.4  | Tidssynkronisering | Urene i alle relevante informationsbehandling i en organisation eller et sikkerhedsdomæne skal være synkroniseret til en enkelt referencetidskilde.  |
| **A.12.5 Styring a driftssoftware** |
| Formål: At sikre integriteten af driftssystemer   |
|  | *Kontrol* |
| A.12.5.1  | Software installation på driftssystemer | Der skal implementeres procedure til styring af softwareinstallationen på driftssystemer. |
| **A.12.6 Sårbarhedsstyring**  |
| Formål: At forhindre, at tekniske sårbarheder udnyttes. |
|  | *Kontrol* |
| A.12.6.1  | Styring af tekniske sårbarheder | Der skal løbende indhentes informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksportering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende foranstaltninger for at håndterer den tilhørende risiko. |
| A.12.6.2  | begrænsninger på softwareinstallation | Der skal fastlægges og implementeres regler om softwareinstallation, som foretages af brugerne. |
| **A.12.7 Overvejelser i forbindelse med audit af informationssystemer**  |
| Formål: | At minimere virkning af auditaktiveret på driftssystemer. |
|  | *Kontrol* |
| A.12.7.1  | kontroller forbindelse med audit af informationssystemer | Auditkrav og -aktiviteter, der indebærer verifikation af driftssystemer, skal planlægges of aftales omhyggeligt for at minimere afbrydelser af forretningsprocesserne.  |

|  |
| --- |
| **A.13 Kommunikationssikkerhed**  |
| **A.13.1 styring af netværkssikkerhed**  |
| Formål: At sikre beskyttelse af informationer i netværk under understøttende informationsbehandlingsfaciliteter. |
|  | *Kontrol* |
| A.13.1.1  | Netværksstyringer | netværket skal styres og kontrolleres for at beskytte informationer i systemer og applikationer. |
| A.13.1.2  | sikring af netværkstjenester | Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester skal identificeres og indgå i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede. |
| A.13.1.3  | opdeling af netværk | Netværk skal styres og kontrolleres for at beskytte informationer i systemer og applikationer. |

|  |
| --- |
| **A.13 Kommunikationssikkerhed**  |
| **A.13.1 styring af netværkssikkerhed** |
| Formål: At sikre beskyttelse af informationer i netværk og af understøttende informations behandlingsfaciliteter. |
|  | *Kontrol* |
| A.13.1.1  | Netværksstyring | Netværk skal styres og kontrolleres for at beskytte informationer i systemer og applikationer. |
| A.13.1.2  | sikring af netværkstjenester | Sikkerhedsmekanismer, serviceniveauer og styringens krav til alle netværkstjenester skal identificeres og indgå i aftaler om netværkstjenester uanset om disse tjenester leveres intern eller er outsources. |
| A.13.1.3  | opdeling af netværk | Grupper af informationstjenester, brugere og informationssystemer skal opdeles i netværk. |
| **A.13.2 informationsoverførsel**  |
| Formål: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet  |
|  | *Kontrol* |
| A.13.2.1  | politikker og procedurer for informationsoverførsel | Der skal foreligge formelle politikker, procedure og kontroller for at overførsel for at beskytte informationsoverførsel ved brug af tomme former for kommunikationsudstyr. |
| A.13.2.2  | Aftaler om informationsoverførsel | Aftaler skal omhandle sikker overførsel for forretningsinformation mellem organisationen og eksterne partner. |
| A.13.2.3  | elektroniske meddelelser | Informationer i elektroniske meddelelser skal beskyttes på passende måde  |
| A.13.2.4  | Fortroligheds- og hemmeligholdelsesaftale | Krav til fortroligheds- og hemmeligholdelsesaftale, der afspejler organisationens behov for at beskytte information, skal identificeres, gennemgås regelmæssigt og dokumenteres. |

|  |
| --- |
| **A.14 Anskaffe, udvikling og vedligeholdelser af systemer**  |
| **A.14.1 Sikkerhedskrav til informationssystemer** |
| Formål: At sikre, at informationssikkerhed er en integreret del af informationssystemer og gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk. |
|  | *Kontrol* |
| A.14.1  | Analyse og specifikation af informations- sikkerhedskrav | Informationssikkerhedsrelateret krav skal være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer. |
| A.14.1.2  | Sikring er applikationstjenester på offentligt netværk | Informationer i forbindelse med applikationstjenester over offentlige netværk skal beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring |
| A.14.1.3  | Beskyttelse af handelsapplikationer og -tjenester | Informationer i forbindelse med handelsapplikationer og -tjenester skal beskyttes for at forhindre ufuldstændig transmission, fejlforsendelser, uautoriseret ændring af meddeler, uautoriseret offentliggørelse, uautoriseret kopiering eller retransmission af meddelelser. |
| **A.14.2 Sikkerhed i udviklings- og hjælpeprocesser**  |
| Formål: At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.  |
|  | *Kontrol* |
| A.14.2.1  | Sikker udviklingspolitik | Der skal fastlægges og anvendes regler for udvikling af software og systemer i organisationen. |
| A.14.2.2  | Procedure for styring af systemændringer | Ændringer af systemer inden for udviklingslivscyklussen skal styres ved hjælp af af formelle procedurer for ændringsstyring.  |
| A.14.2.3  | Teknisk gennemgang af applikationer efter ændring af driftsplatforme | Ved ændring af driftsplatforme skal forretningskritiske applikationer gennemgås og testes for at sikre, at ændringen ikke indvirker på negativt på organisationens drift eller sikkerhed.  |
| A.14.2.4  | Begrænsning af ændringer af softwarepakker | Ændringer af softwarepakker skal vanskeliggøres, begrænset til nødvendige ændringer, og alle ændringer skal styres effektivt. |
| A.14.2.5  | Principper for udvikling af sikre systemer | Principper for udvikling af sikre systemer skal fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med alle implementeringer af informationstyper.  |
| A.14.2.6  | Sikkert udviklingsmiljø | Organisationer sjal etablerer sikre udviklings miljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus. |
| A.14.2.7  | Outsourcet udvikling | Organisationen skal føre tilsyn med og overvåge systemudviklingsaktiviteter, der er outsourcet.  |
| A.14.2.8  | Systemsikkerhedstest | Der skal etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.  |
| **A.14.3 Testdata** |
| Formål: At sikre beskyttelse af data, som anvendes til test. |
|  | *Kontrol* |
| A.14.3.1  | Sikring af test data | Test data skal udvælges omhyggeligt og skal beskyttes og styres. |

|  |
| --- |
| **A.15 leverandørforhold** |
| **A.15.1 Informationssikkerhed i leverandørforhold** |
| Formål: At sikre beskyttelse af organisationens aktiver, som leverandør har adgang til |
|  | *Kontrol* |
| A.15.1  | Informationssikkerhed- politik for leverandørforhold | Informationssikkerhedskravende til at minimere risiciene forbundet med leverandørens adgang til organisationens aktiver skal aftales med leverandøren og skal dokumenteres. |
| A.15.1.2  | Håndtering af sikkerhed i leverandøraftaler | Alle relevante informationssikkerhedskrav skal fastlægges og aftales med hver enkel leverandør, som kun kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens information.  |
| A.15.1.3  | For syningskæde af sikkerhed i leverandøraftaler | Aftaler med leverandøren skal indeholde krav til håndtering af informationssikkerhedsrisici forbundet med forsyningskæden for IKT- tjenester og -produkter.  |
| **A.15.2 Styring af leverandørydelser**  |
| Formål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne  |
|  | *Kontrol* |
| A.15.2.1  | Overvågning og gennemgang af leverandørydelser | Organisationer skal regelmæssigt overvåge, gennemgå og auditere leverandørydelser. |
| A.15.2.2  | Styring af ændringer af leverandørydelser | Ændringer af leverandørydelser, herunder vedligeholdelse og forbedring af eksisterende Informationssikkerhedspolitikker, - procedurer og forretningsinformationer, -systemer og -processer er, og til en revurdering a risici. |

|  |
| --- |
| **A.16 Styring af informationssikkerhedsbrud** |
| **A.16.1 Styring af informationssikkerhedsbrug og forbedringer** |
| Formål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrug, herunder kommunikation om sikkerhedshændelser og -svagheder.  |
|  | *Kontrol* |
| A.16.1.1  | Ansvar og procedurer | Ledelsesansvar og procedurer skal fastlægges for a sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.  |
| A.16.1.2  | Rapportering af informationssikkerhed- hændelser | Informationssikkerhedshændelser skal rapporteres ad passende ledelseskanaler så hurtigt som muligt.  |
| A.16.1.3  | Rapportering af informationssikkerhed- svagheder | Medarbejder og kontrahenter, som bruger organisationens informationssystem og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistænker om svagheder i informationssystemer som informationssikkerhedsbrud. |
| A.16.1.4  | Vurdering af beslutning og informations- sikkerhedshændelser | Informationssikkerhedshændelser skal vurderes, og det skal besluttes, om de skal klassificeres som informationssikkerhedsbrud. |
| A.16.1.5  | håndtering af informationssikkerhedsbrud | Informationssikkerhedsbrud skal håndteres i overstemmes med de dokumenterede procedurer.  |
| A.16.1.6  | Erfaring fra informationssikkerhedsbrud | Den viden, der opnås ved at anylasere og håndtere informationssikkerhedsbrud, skal anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.  |
| A.16.1.7  | Indsamling af beviser | Organisationen skal definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som bevis. |

|  |
| --- |
| **A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring** |
| **A.17.1 informationssikkerhedskontinuitet**  |
| Formål: informationssikkerhedskontinuitetskal være forankret i organisationens ledelsessystemer for nød- beredskabs- og reetableringsstyring.  |
|  | *Kontrol* |
| A.17.1.1  | Planlægning af informationssikkerheds-kontinuitet | Organisationen skal fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.  |
| A.17.1.2  | implementering af informationssikkerheds-kontinuitet | Organisationen skal fastlægge dokumentere, implementeres og vedligeholde processer, procedure og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation. |
| A.17.1.3  | Verificere, gennemgå og evaluer informationssikkerheds-kontinuiteten | Organisationen skal verificere de etablerede implanterede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer. |
| **A.17.2 redundans**  |
| Formål: At sikre tilgængelighed af informationsbehandlingsfaciliteter. |
|  | *Kontrol* |
| A.17.2.1  | Tilgængelighed af informationsbehandlings-faciliteter | Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav. |

|  |
| --- |
| **A.18 Overensstemmelse** |
| **A. 18.1 Overensstemmelse med lov- og kontraktkrav** |
| Formål: At forhindre overtrædelse af love-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav  |
|  | *Kontrol* |
| A.18.1.1  | identifikation af gællende lovgivning og kontraktkrav | Alle relevante love-, myndigheds- og kontraktkrav samt organisationens metode til overholdelse af disse krav skal være klart identificeret, dokumenteret og opdateret for hvert informationssystem og for organisationen.  |
| A.18.1.2  | Immaterielle rettigheder | Der skal implementeres passende procedure til at sikre, at der er overensstemmelse med lov-, myndigheds- og kontraktkrav i relation til immaterielle rettigheder og anvendelse af beskyttede softwareprodukter.  |
| A.18.1.3  | Beskyttelse af registrering | Registrering skal beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overstemples med lov-m myndigheds- og kontrakt samt forretningsmæssige krav. |
| A.18.1.4  | Privatlivets fred og beskyttelse af personoplysninger | Privatlivets fred og personoplysninger skal beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter.  |
| A.18.1.5  | Regulering af kryptografi | Kryptografi skal anvendes i overensstemmelse med alle relevante aftaler, love og forskrifter. |
| **A.18.2 Gennemgang af informationssikkerhed** |
| Formål: At sikre, at informationssikkerhed er implanteres og drives i overensstemmelse med organisationens politiker og procedurer. |
|  | *Kontrol* |
| A.18.2.1  | Uafhændelig gennemgang af informationssikkerhed | Organisationens metode til styren af informationssikkerhed og implementering heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) skal gennemgås uafhændeligt med plantage mellemrum eller i tilfælde af væsentlige ændringer. |
| A.18.2.2  | Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder | Lederne skal regelmæssigt undersøge, om informationsbehandlingen og -procedurerne inden for deres ansvarsområder er i overstemmes med relevante sikkerhedspolitikker, standarter og andre sikkerhedskrav. |
| A.18.2.3  | Undersøgelse af teknisk overensstemmelse | Informationssystemer skal undersøges rejfmæssigt for, om de er i overensstemmelse med organisationens Informationssikkerhedspolitikker og -standarter.  |