Prioritet: Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

Sammenfatning af sikkerhedskrav

Følgende er en sammenfatning af de sikkerhedskrav, som fremgår af dokumentet "Særkrav1.docx". Desuden er der sat yderligere krav ind fra egne risikovurderinger, som er foretaget efterfølgende, og disse er markeret med grøn fremhævning i overskriften.

Alle sikkerhedskrav bør tage højde for opdelingen av sikrningsniveauer i henhold til Europa-Parlamentets og Rådets forordning 910/2014 – Artikel 8, hvor niveauerne opdeles i **»lav«**, **»betydelig«** og **»høj«** efter følgende metode:

1. En elektronisk identifikationsordning, der er anmeldt i henhold til artikel 9, stk. 1, skal angive sikringsniveauerne »lav«, »betydelig« og/eller »høj« for de elektroniske identifikationsmidler, der er udstedt under den pågældende ordning.

2. Sikringsniveauerne **»lav«**, **»betydelig«** og **»høj«** skal opfylde følgende kriterier:

    a. sikringsniveauet **»lav«** henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der udviser en begrænset grad af tillid til en persons påståede identitet, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten

    b. sikringsniveauet **»betydelig«** henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der udviser en middelstor grad af tillid til en persons påståede identitet, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten

    c. sikringsniveauet **»høj«** henviser til et elektronisk identifikationsmiddel i en elektronisk identifikationsordning, der giver en højere grad af tillid til en persons påståede identitet end elektroniske identifikationsmidler med sikringsniveauet »betydelig«, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for misbrug eller ændring af identiteten.

Sikkerhedskravene er opdelt efter strukturen i ISO/IEC 27002.

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

5 Informationssikkerhedspolitikker

5.1 Ledelse af informationssikkerhed

5.1.1 Informationssikkerhedspolitikker

- Et sæt politikker for informationssikkerhed børfastlægges, godkendes af ledelsen, offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.
- Følgende EU-regler skal tilgodeses:
  - Beskyttelse af datasikkerhed og fortrolighed i forbindelse med dataudveksling og vedligeholdelse af dataintegritet sikres ved hjælp af de bedste tilgængelige tekniske løsninger og beskyttelsespraksis.
  - Der skal tages stilling til, hvilke krav i ISO/IEC 27002 man vil følge og begrunde de, man evt. vælger fra.
- Databehandling og databeskyttelse
  - Behandling af personoplysninger skal udføres i overensstemmelse med direktiv 95/46/EF.
- Informationssikring og sikkerhedsstandarder
  - Det skal dokumenteres, at virksomheden opfylder kravene i standarden ISO/IEC 27001
  - Sikkerhedskritiske opdateringer skal udrulles uden unødig forsinkelse.
- Følgende OCES-regler bør overvejes:
  - Der skal tages stilling til behov for en sertificeringspraksis (a la OCES 7.1)

5.1.2 Gennemgang af sikkerhedspolitikker

- Informationssikkerhedspolitikkerne bør gennemgås efter planlagte intervaller eller såfremt væsentlige ændringer sker, der påvirker politikkernes anvendelighed.

6 Organisering af informationssikkerhed

6.1 Intern organisation

6.1.1 Roller og ansvarsområder for informationssikkerhed

- Alle ansvarsopgaver vedrørende informationssikkerhed bør være definerede og tildelte
- Følgende OCES-regler bør implementeres:
  - Der skal foreligge politikker og procedurer for håndtering af kundehenvendelser eller henvendelser fra signaturmodtagere.
  - Der skal foreligge skriftlige aftaler med alle underleverandører af CA- tjenester.
  - CA skal til enhver tid have tilstrækkelig med uddannet personale til at kunne drive alle udbudte tjenester på forsvarlig vis. Personalet skal til enhver tid have den kompetence, der foreskrives for de enkelte definerede betroede funktioner.
  - CA skal sikre, at der foreligger skriftlige aftaler med alle underleverandører af CA- tjenester.

- **Nøglepersoner (egen risikovurdering)**
  - Der bør undgås, at der opstår nøglepersonsafhængighed

6.1.2 Funktionsadskillelse

- Modstridende funktioner og ansvarsområder bør adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver

6.1.3 Kontakt til myndigheder

- Passende kontakt bør være til relevante myndigheder

6.1.4 Kontakt til særlige interessegrupper

- Passende kontakt bør være til særlige interessegrupper eller andre fora for sikkerhedsspecialister og professionelle netværk

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

6.1.5 Informationssikkerhed i projektledelse

- Informationssikkerhed bør adresseres i projektledelse, uanset type af projekter

6.2 Mobile enheder og fjernarbejde

6.2.1 Politik for mobile enheder

- Der bør foreligge en politik samt tilhørende sikkerhedstiltag for at reducere de risici, som anvendelse af mobile enheder medfører

6.2.2 Fjernarbejde

- Der bør foreligge en politik samt tilhørende sikkerhedstiltag for at beskytte informationer, som tilgås, behandles eller lagres på fjernarbejdspladser

7 HR sikkerhed

7.1 Før ansættelse

7.1.1 Efterprøvning

- Der skal udføres en efterprøvning af ansøgere, før en aftale indgås. Efterprøvningen skal foretages i overensstemmelse med gseldende lovgivning, regler og etik, og skal vurderes i forhold til virksomhedens kravtil informationssikkerhed og de relevante risici.
- Følgende OCES-regler bør implementeres:
    - Der skal kontrolleres, at ledere og medarbejdere, der udfører betroede opgaver i eller for CA, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv. Dette er ligeledes gældende for RA medarbejdere (7.4.3).

7.1.2 Ansættelsesvilkår

- Ansættelsesaftaler med medarbejdere eller aftaler med leverandører bør definere deres samt virksomhedens pligter i henhold til informationssikkerhed

7.2 Under ansættelsesforløbet

7.2.1 Ledelsens ansvar

- Ledelsen bør kræve, at alle ansatte og leverandører efterlever de krav, som virksomheden stiller til informationssikkerhed i henhold til gældende politikker og forretningsgange

7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed

- Alle virksomhedens ansatte og i relevant omfang også leverandører bør modtage passende undervisning og efteruddannelse om informationssikkerhed i forhold til deres arbejdsopgaver for virksomheden
- Følgende regler bør implementeres (både EU og OCES):
    - Der skal findes procedurer, som sikrer, at personale og underleverandører er tilstrækkeligt uddannede, kvalificerede og erfarne inden for de færdigheder, der er behov for, når de skal udfylde deres roller.
    - Der skal være tilstrækkeligt med personale og underleverandører til at drive og vedligeholde tjenesten i henhold til de relevante politikker og procedurer.

- **Borgenes sikkerhedsbevidsthed (egen risikovurdering)**
    - Det bør sikres, at borgerne oplyses om betydningen af at overholde grundlæggende sikkerhedsforskrifter.

7.2.3 Sanktioner

- Der bør være en formel proces for, hvorledes virksomheden reagerer på sikkerhedsbrud foranlediget af medarbejdere. Denne proces bør være kommunikeret til alle ansatte og leverandører

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

7.3 Ved ansættelsens ophør eller ved ændrede arbejdsområder

7.3.1 Ansættelsens ophør eller ændring

- Pligter vedrørende informationssikkerhed, som fortsat er aktuelle efter, at ansættelsen er ophørt, eller ved skifte af arbejdsområde, bør defineres og kommunikeres til vedkommende medarbejder eller leverandør og bør tilgodeses

8 Håndtering af aktiver

8.1 Ansvar for aktiver

8.1.1 Fortegnelse over aktiver

- Aktiver, som er tilknyttet information og informationsbehandling bør identificeres, og en oversigt over sådanne aktiver bør udarbejdes og vedligeholdes

8.1.2 Ejerskab af aktiver

- Aktiver, som indgår i oversigten, bør have en ejer

8.1.3 Acceptabel brug af aktiver

- Regler for acceptabel anvendelse af aktiver, som er tilknyttet information og informationsbehandling bør formaliseres og implementeres

8.1.4 Returnering af aktiver

- Alle ansatte og brugere hos eksterne parter bør returnere alle aktiver tilhørende virksomheden, som de måtte have i besiddelse, når et ansættelsesforhold, en kontrakt eller en aftale ophører

8.2 Klassifikation af informationer

8.2.1 Klassifikation af informationer

- Informationer bør klassificeres i forhold til krav i lovgivning, værdi, væsentlighed og følsomhed overfor fortrolighedsbrud eller uautoriserede ændringer

8.2.2 Mærkning af informationer

- Passende procedurer bør indføres for mærkning af informationer i henhold til virksomhedens regler for klassificering af informationer

8.2.3 Håndtering af aktvier

- Passende procedurer bør indføres for håndtering af aktiver i henhold til virksomhedens regler for klassificering af informationer

8.3 Håndtering af medier

8.3.1 Flytbare medier

- Passende procedurer bør indføres for håndtering af flytbare medier i henhold til virksomhedens regler for klassificering af informationer

8.3.2 Bortskaffelse af medier

- Medier bør bortskaffes på sikker vis og efter formelle procedurer, når disse ikke længere anvendes

8.3.3 Transport af fysiske medier

- Medier indeholdende informationer bør beskyttes imod uautoriseret tilgang, misbrug eller forvanskning under transport

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

9 Adgangskontrol

9.1 Virksomhedens behov for adgangskontrol

9.1.1 Politik for adgangsstyring

- En formel politik for adgangskontrol bør implementeres i henhold til virksomhedens behov for informationssikkerhed
- Følgende OCES-regler bør implementeres:
  - CA skal tilvejebringe RA systemer, som sikrer, at det kun er bemyndigede medarbejdere hos RA, der har adgang til at betjene disse

9.1.2 Adgang til netværk og netværkstjenester

- Brugere bør kun få adgang til netværk og netværkstjenester, som de specifikt er autoriseret til at benytte

9.2 Styring af brugerrettigheder

9.2.1 Brugerregistrering og -afmelding

- Der bør implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.

9.2.2 Tildeling af brugeradgang

- Der bør implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.

9.2.3 Styring af privilegerede adgangsrettigheder

- Tildeling og anvendelse af privilegerede adgangsrettigheder bør være begrænset og kontrolleret

- **Administration (egen risikovurdering)**
  - Administration bør i mest muligt omfang udføres lokalt på de respektive maskiner og enheder og i mindst muligt omfang via fjernadgang.

9.2.4 Styring af brugeres hemmelige autentificerings informationer

- Tildeling af brugeres hemmelige autentificerings informationer bør kontrolleres via en dokumenteret proces

9.2.5 Revurdering af brugeres adgangsrettigheder

- Ejere af aktiver bør regelmæssigt revurdere brugernes adgangsrettigheder

9.2.6 Sletning eller ændring af adgangsrettigheder

- Alle medarbejderes og eksterne parters brugeres adgangsrettigheder til informationer og systemer bør slettes, når ansættelsesforhold eller samarbejde ophører. Er der tale om ændringer i arbejdsforhold eller opgaver, bør adgangsrettighederne tilpasses

9.3 Brugernes ansvar

9.3.1 Anvendelse af hemmelige autentificerings informationer

- Virksomheden bør kræve, at brugere overholder virksomhedens retningslinjer for anvendelse af hemmelige autentificerings informationer

9.4 Adgangskontrol i systemer og applikationer

9.4.1 Begrænsning af adgang til informationer

- Adgang til informationer og funktioner i applikationer bør begrænses i henhold til adgangskontrolpolitikken

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

9.4.2 Sikre log-on procedurer

- Hvor adgangskontrolpolitikken kræver det, bør log-on til systemer og applikationer kontrolleres med sikre log-on procedurer

9.4.3 Systemer til administration af adgangskoder

- Systemer til administration af adgangskoder bør være interaktive og sikre adgangskoder med høj kvalitet

9.4.4 Anvendelse af stærke systemværktøjer

- Anvendelse af stærke systemværktøjer, som har mulighed for at overstyre kontroller i systemer og applikationer bør begrænses og være underlagt streng kontrol

9.4.5 Adgangskontrol til programmers kildekode

- Adgang til programmers kildekode bør begrænses

10 Kryptering

10.1 Kryptografiske kontroller

10.1.1 Politik for anvendelse af kryptering

- En politik for anvendelse af kryptering til beskyttelse af informationer bør indføres
- Følgende EU-regler bør implementeres (detaljerede krav fremgår af forordningen):
    - Krav til kvalificerede tillidstjenesteudbydere (detaljerede krav)
    - Kravene til avancerede elektroniske signaturer
    - Kvalificerede certifikater for elektroniske signaturer
- **Helpdesk (egen risikovurdering)**
    - Der bør være en passende helpdesk funktion til at varetage kommunikation og brugerservice til borgerne.

10.1.2 Nøgleadministration

- En politik for anvendelse, beskyttelse og levetid for krypteringsnøgler bør indføres og anvendes i hele livsforløbet
- Følgende OCES-regler bør implementeres:
    - Virksomheden skal anvende udførlige, skriftlige procedurer for:
        - Nøglehåndtering
        - Håndtering af kryptografiske moduler
        - Nøglehandtering leveret af CA
        - Certifikathåndtering
        - Udstedelse af certifikat og generering af certifikatindehavers nøgler
        - Certifikatfornyelse
        - Certfikatgenerering
        - Publicering af certifikater
        - Certifikatspærring
    - Kontrol bør udføres af digital signatur svarende til kravene i DS 844:
        - Kontrollen er en automatisk proces, hvorfor der ikke er noget krav om, at en digital signatur umiddelbart skal være læsbar for det menneskelige øje. Kontrollen gennemføres trinvist, således at informationer, der kan hentes direkte i certifikatet, anvendes, før der forespørges på spærrelister.
        - Kontrollernes rækkefølge bør følge anbefalingerne i DS 844
- Desuden bør følgende anbefalinger fra DS 844 tilgodeses:
    - Mængden af information i certifikat
    - Certifikat-serienummer

Prioritet: Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

- Stjålne eller bortkomne mobiltelefoner / nøglekort (egen risikovurdering)
    - Der bør udarbejders og implementeres procudurer for, hvorledes det skal reageres i tilfælde af at mobiltelefoner eller nøglekort mistes. Der bør også tages stilling til, hvem der er ansvarlig for mulige økonomiske tab i den forbindelse.

10.1.3 Krav til kvalificerede elektroniske signaturgenereringssystemer

- Systemer til generering av kvalificerede elektroniske signaturer bør følge kravene i Europa-Parlamentets og Rådets forordning 910/2014. Disse er opsummeret her i punktform.
    - Kvalificerede elektroniske signaturgenereringssystemer skal opfylde kravene i bilag II.
    - Krav til certificering af kvalificerede signaturgenereringssystemer
    - Krav til validering af kvalificerede elektroniske signaturer
    - Kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer
    - Krav til kvalificerede elektroniske tidsstempler

10.1.4 Tilmelding

- Procedurerne for tilmelding bør følge kravene i Europa-Parlamentets og Rådets gennemførelsesforordning 1502/2015. Disse krav, som i forordningen er opdelt i **»lav«**, **»betydelig«** og **»høj«**, er opsummeret her i punktform.
    - Ansøgning og registrering
        - Godtgørelse og kontrol af identitet (fysiske personer)
        - Godtgørelse og kontrol af identitet (juridiske personer)
        - Forbindelser mellem elektroniske identifikationsmidler for fysiske og juridiske personer
    - Håndtering af elektroniske identifikationsmidler
        - Elektroniske identifikationsmidler — egenskaber og udformning
        - Udstedelse, levering og aktivering
        - Suspendering, tilbagekaldelse og reaktivering
        - Fornyelse og erstatning
    - Autentifikation
        - Autentifikationsmekanismen
    - Håndtering og organisering
        - Generelle bestemmelser
        - Registerføring
        - Faciliteter og personale
        - Tekniske kontroller

11 Fysisk og miljømæssig sikkerhed

11.1 Sikre områder

11.1.1 Fysiske sikkerhedsbarrierer

- Sikkerhedsbarrierer bør defineres og anvendes for at beskytte områder, der indeholder enten sensitive eller kritiske informationer og systemer.

- Følgende EU-krav bør implementeres:
    - Faciliteter, kontrolleres løbende for og beskyttes mod skader forårsaget af miljøhændelser, uautoriseret adgang og andre faktorer, som kan påvirke tjenestens sikkerhed.
    - Faciliteter, sikrer, at adgang til de områder, hvor personlige, kryptografiske og andre følsomme oplysninger opbevares og behandles, er begrænset til autoriseret personale og autoriserede underleverandører.

- Følgende OCES-krav bør implementeress:

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

- CA skal tydeligt beskrive, på hvilke lokaliteter medarbejdere og datacentre i forbindelse med CA's virke er placeret. De lokaler, hvor udstyr til nøglegenerering er placeret, benævnes CA driftslokaler. Alle lokaler, der benyttes til medarbejdere hos CA, skal være defineret som særligt sikkerhedsområde, jf. 11.1.2 nedenfor.
- CA driftslokaler
  - CA driftslokalet skal være fysisk adskilt fra CA's øvrige lokaler.
  - I tilfælde af evakuering skal CA's driftslokaler kunne fungere med uændret drift via fjernbetjening. Ved fjernbetjening forstås mulighed for f.eks. via en PC at betjene CA-funktionerne fra et fra CA-driften fysisk adskilt lokale, f.eks. hvor CA har etableret reservesystem.

11.1.2 Fysiske adgangskontroller

- Sikre områder bør beskyttes med passende adgangskontroller til sikring af, at kun autoriseret personale får adgang
- Følgende krav fra OCES bør implementeres:

Fysisk adgang

- CA skal sikre, at alle lokaler har en perimeterbeskyttelse svarende til DS 471 eller bedre.
- CA skal sikre, at der etableres vagt 24 timer i døgnet.

Krav til fysisk sikkerhed (indbrudssikerhed - DS 471)

- Der skal defineres detaljerede krav til:
- Bygningslayout
- Adgangsveje og stier
- Krav til døre og porte i skallen
- Krav til vinduer og ruder i skallen
- Krav til gitre i skallen
- Vægkonstruktioner
- Tagkonstruktioner
- Etageadskillelse
- Krav til låse- og nøglesystemer
- Krav til adgangskontrolanlæg
- Kriminalpræventiv belysning
- Sammenstillede sikringsforanstaltninger
- Kategorisering af områder
- Fastlæggelse af barrierer

CA-driftslokaler

- CA skal sikre, at adgang til og ophold i de centrale driftslokaler videoovervåges.

11.1.3 Sikring af kontorer, lokaler og faciliteter

- Fysisk sikkerhed for kontorer, lokaler og faciliteter bør indføres
- **Ryddelige serverrum (egen risikovurdering)**
  - Alle serverrum bør holdes ryddelige, og alt unødvendigt materiale bør fjernes.

11.1.4 Sikring imod eksterne og miljømæssige trusler

- Fysisk sikring bør indføres imod naturkatastrofer, ondsindede angreb eller uheld

11.1.5 Arbejde i sikre områder

- Procedurer bør indføres for arbejde i sikre områder

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

11.1.6 Områder til lastning og aflevering

- Adgangspunkter som f.eks. områder til lastning og aflevering og andre adgangspunkter, hvor uautoriseret personale kan opnå adgang til virksomhedens lokaler, bør beskyttes og om muligt holdes adskilt fra informationsbehandlings systemer for at undgå uautoriseret adgang

11.1.3 Sikring af kontorer, lokaler og faciliteter

- Fysisk sikkerhed for kontorer, lokaler og faciliteter bør indføres

11.1.4 Sikring imod eksterne og miljømæssige trusler

- Fysisk sikring bør indføres imod naturkatastrofer, ondsindede angreb eller uheld

11.1.5 Arbejde i sikre områder

- Procedurer bør indføres for arbejde i sikre områder

11.1.6 Områder til lastning og aflevering

- Adgangspunkter som f.eks. områder til lastning og aflevering og andre adgangspunkter, hvor uautoriseret personale kan opnå adgang til virksomhedens lokaler, bør beskyttes og om muligt holdes adskilt fra informationsbehandlings systemer for at undgå uautoriseret adgang

11.2 Udstyr

11.2.1 Placering og beskyttelse af udstyr

- Udstyr bør placeres og beskyttes for at minimere risikoen for miljømæssige trusler og for mulighed for uautoriseret adgang

11.2.2 Kritiske forsyninger

- Udstyr bør beskyttes imod strømsvigt og andre driftsforstyrrelser forårsaget af kritiske forsyninger som f.eks. el, telekommunikation, vandforsyning, ventilation m.m.

11.2.3 Kabelsikkerhed

- El og telekommunikations kabler bør beskyttes imod aflytning, forstyrrelser og skader

11.2.4 Vedligeholdelse af udstyr

- Udstyr bør vedligeholdes på korrekt vis for at sikre fortsat tilgængelighed og integritet

11.2.5 Fjernelse af aktiver

- Udstyr, informationer og software bør ikke fjernes fra virksomheden uden tilladelse

11.2.6 Sikkerhed vedrørende udstyr og aktiver uden for virksomhedens lokaler

- Sikkerhed bør iværksættes for aktiver uden for virksomhedens lokaler, hvor der tages højde for de risici, der knytter sig til at arbejde uden for virksomhedens lokaler

11.2.7 Sikker bortskaffelse eller genbrug af udstyr

- Alt udstyr, der indeholder lagringsmedier, bør kontrolleres for at sikre, at sensitive informationer og licensbeskyttet software er fjernet eller overskrevet på sikker vis inden bortskaffelse eller genbrug

11.2.8 Udstyr uden opsyn

- Brugere bør sikre at udstyr er passende beskyttet, når det er uden opsyn

11.2.9 Politik for ryddeligt skrivebord og skærm

- En politik bør indføres for at skriveborde holdes ryddelige for papirer og transportable lagringsmedier, og for at computerskærme ikke afslører fortrolige informationer

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

12 Sikkerhed vedrørende drift

12.1 Driftsprocedurer og pligter

12.1.1 Dokumenterede driftsprocedurer

- Driftsprocedurer bør dokumenteres og være tilgængelige for alle, der har brug for dem
- Følgende EU krav bør implementeres:

Tekniske kontroller (1502)

Lav

- Der skal findes rimelige tekniske kontroller, som gør det muligt at afværge trusler mod tjenesternes sikkerhed og sikrer de behandlede oplysningers fortrolighed, integritet og tilgængelighed.
- Elektroniske kommunikationskanaler, der bruges til at udveksle personlige eller følsomme oplysninger, beskyttes mod aflytning, manipulation og gengivelse.
- Adgang til følsomt kryptografisk materiale er, hvis det bruges til at udstede elektroniske identifikationsmidler eller autentifikation, begrænset til de roller og anvendelsesområder, der absolut skal have adgang. Det skal sikres, at den slags materiale aldrig lagres permanent som klartekst.
- Der er indført procedurer, som garanterer, at sikkerheden bevares over tid, og at der er mulighed for at reagere på ændringer i risikoniveau, sikkerhedshændelser og brud på sikkerheden.
- Alle medier, som indeholder personlige, kryptografiske eller andre følsomme oplysninger, lagres, transporteres og bortskaffes på en sikker måde.

Betydelig

- Samme niveau som »lav«, samt:
- Følsomt kryptografisk materiale er, hvis det anvendes til at udstede elektroniske identifikationsmidler eller autentifikation, beskyttet mod manipulation.

- **Høj**
- Samme niveau som »betydelig«.

- Følgende krav fra OCES bør implementeres:

Opbevaring af certifikatinformation

- CA er ansvarlig for etablering af et datalagringssystem, der skal indeholde alle data, der er nødvendige for sikker drift af CA i overensstemmelse med denne CP. CA skal desuden sikre, at:
  - al information beskyttes mod uretmæssig adgang,
  - alle aktiviteter, der kræver deltagelse af mere end en person, logges,
  - alle informationer om registrering, herunder certifikatfornyelser, logges,
  - alle adgange og adgangsforsøg til områder, der skal beskyttes af adgangskontrol, logges,
  - al videoovervågning lagres,
  - der er skriftlige regler for regelmæssig gennemgang af alle logs,
  - alle audit-logs signeres elektronisk og tidsstemples,
  - audit-logs behandles som fortroligt materiale samt
  - der foretages backup af audit-logs med regelmæssige mellemrum.
- CA skal sikre, at back-up-data opbevares i overensstemmelse med kravene i jf. 12.3.1 nedenfor
- CA skal sikre, at IT- og Telestyrelsen informeres om væsentlige uregelmæssigheder i logningsproceduren samt notificeres en gang årlig i alle andre tilfælde.

- CA skal sikre, at følgende information arkiveres:
  - alle logs,
  - certifikatanmodninger og tilhørende kommunikation,
  - signerede ordrer og skriftlige aftaler,
  - certifikatfornyelser samt
  - CPS og CP.
- CA skal sikre, at arkiveret information kan gøres tilgængelig i tilfælde af tvister, og at alt arkiveret materiale opbevares i mindst løbende kalenderår + 5 år. Dette er også gældende for evt. data fra RA's it-systemer, som er relevante for dokumentation af CA's virke.

- CA og RA skal sikre, at alt materiale i arkiv opbevares i overensstemmelse med kravene i DS 484.

- CA og RA skal sikre, at alt elektronisk arkivmateriale sikkerhedskopieres med regelmæssige mellemrum.

- CA og RA skal sikre, at alt elektronisk arkivmateriale påføres elektronisk tidsstempling på arkiveringstidspunktet. Andet arkivmateriale indføres i en log.

12.1.2 Ændringsstyring

- Ændringer til organisation, forretningsprocesser, informationsbehandlingssystemer og systemer, som påvirker informationssikkerhed, bør kontrolleres

12.1.3 Kapacitetsstyring

- Anvendelse af ressourcer bør overvåges, justeres og vurderinger udføres af kommende behov for at sikre påkrævet stabilitet og ydelse

12.1.4 Adskillelse af udviklings-, test- og driftsmiljø

- Udviklings-, test- og driftsmiljøer bør holdes adskilt for at reducere risikoen for uautoriseret adgang eller ændringer til driftsmiljøet

12.2 Beskyttelse imod skadelig kode

12.2.1 Tiltag imod skadelig kode

- Der bør implementeres kontroller til opdagelse af, beskyttelse imod og genopretning efter skader fra skadelig kode. Disse kontroller bør suppleres med passende sikkerhedsbevidsthed fra brugernes side

12.3 Sikkerhedskopiering

12.3.1 Sikkerhedskopiering af informationer

- Sikkerhedskopiering af informationer, software og system "images" bør tages og testes regelmæssigt i henhold til en formel politik

- **Opbevaring af sikkerhedskopier (egen risikovurdering)**
  - Sikkerhedskopier bør forefindes i passende generationer tilbage i tid i henhold til en forretningsgang, således at gamle versioner af data kan genskabes.

12.4 Logning og overvågning

12.4.1 Logning af hændelser

- Brugeres aktivitet, undtagelser, fejl og sikkerhedshændelser bør logges. Loggene bør gemmes og gennemgås regelmæssigt

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

12.4.2 Beskyttelse af loginformationer

- Logningssystemer og loginformationer bør beskyttes impd forvanskning og uautoriseret adgang

Logning af anvendelse af Mobil ID (Risikovurdering)

- Anvendelse af Mobil ID logges i en central log. Der bør udarbejdes procedurer for, hvorledes denne log håndteres, arkiveres, gennemgås, hvorledes det sikres, at loggen ikke overskrives, og krav til fysisk og logisk sikkerhed.

12.4.3 Administrator- og operatørlogge

- Systemadministrator og systemoperatør aktivitet bør logges og loggene beskyttes og regelmæssigt gennemgås

12.4.4 Synkronisering af ure

- Ure/klokker i alle systemer i en virksomhed eller sikkerhedsdomæne bør synkroniseres imod én enkelt timeserver/kilde

12.5 Kontrol med operationelt software

12.5.1 Installation af software på systemer i drift

- Der bør være procedurer for kontrol med installation af software på systemer i drift

12.6 Styring af tekniske svagheder

12.6.1 Sårbarhedssikring

- Der bør løbende indhentes oplysninger om tekniske svgheder i anvendte systemer, og hvorledes virksomheden er påvirket af sådanne svagheder. Nødvendige sikkerhedsforanstaltninger bør iværksættes for at reducere de afledte risici

12.6.2 Kontroller med softwareinstallation

- Regler bør iværksættes for, hvorledes brugere kan installere software

12.7 Forhold vedrørende revision af systemer

12.7.1 Kontroller vedrørende revision af systemer

- Revisioner af systemer i drift bør tilrettelægges således, at disse mindst muligt forstyrrer forretningsprocesserne

13 Sikkerhed vedrørende kommunikation

13.1 Styring af netværkssikkerhed

13.1.1 Netværkskontroller

- Netværk bør være styret og kontrolleret for at beskytte informationer i systemer og applikationer
- Følgende EU krav bør implementeres:

Datasikkerhed og fortrolighed

- Beskyttelse af datasikkerhed og fortrolighed i forbindelse med dataudveksling og vedligeholdelse af dataintegritet mellem knudepunkterne sikres ved hjælp af de bedste tilgængelige tekniske løsninger og beskyttelsespraksis.
- Knudepunkterne lagrer ingen personlige data med undtagelse af dem, der er nødvendige til det i artikel 9, stk. 3, beskrevne formal.

Dataintegritet og kommunikationens ægthed

- Kommunikation mellem knudepunkter sikrer datas integritet og ægthed, samt at alle anmodninger og svar er ægte og ikke er blevet manipuleret. Med henblik herpå bruger knudepunkterne løsninger, som med succes er blevet anvendt til grænseoverskridende operationer.

Kommunikationens format

- Knudepunkter gør til syntaks brug af fælles beskedformater, der er baseret på standarder, som allerede er blevet anvendt i flere tilfælde mellem medlemsstater, og som har vist sig at virke i et operationelt miljø. Syntaksen giver mulighed for:
  a) korrekt behandling af det minimum af personidentifikationsdata, der entydigt repræsenterer en fysisk eller juridisk person
  b) korrekt behandling af det elektroniske identifikationsmiddels sikringsniveau
  c) at skelne mellem offentlige myndigheder og modtagerparter
  d) fleksibilitet til at opfylde kravene til yderligere attributter i forbindelse med identifikation.

Forvaltning af sikkerhedsoplysninger og metadata

- Knudepunktsoperatøren kommunikerer metadata vedrørende knudepunktets forvaltning pa en standardiseret made, hvor de kan behandles af en maskine, og pa en sikker og palidelig made.
- Som minimum kan de parametre, der er relevante for sikkerheden, indhentes automatisk.
- Knudepunktsoperatøren lagrer data, som i tilfælde af en hændelse giver mulighed for at gendanne beskedudveks- lingssekvensen med henblik pa at fastslå, hvor og hvordan hændelsen fandt sted. Disse data lagres i den periode, der er angivet i national lovgivning, og bestar som minimum af følgende elementer:
  a) identifikation af knudepunktet
  b) identifikation af beskeden
  c) dato og tidspunkt for beskeden.

- **Firewalls (egen risikovurdering):**
  - Netværksadgang bør sikres ved anvendelse af passende firewalls

- **Denial of service (egen risikovurdering)**
  - Der bør forberedes procedurer for omdirigering af netværkstrafik, såfremt virksomheden bliver udsat for denial of service angreb

13.1.2 Sikkerhed vedrørende netværkstjenester

- Sikkerhedsmekanismer, service niveauer og ledelseskrav bør identificeres og inkluderes i alle netværks serviceaftaler uanset om disse leveres in-house eller er outsourcet

13.1.3 Opdeling af netværk

- Netværk bør opdeles i segmenter, således at grupper af tjenester, brugere og systemer opdeles i segmenter

13.2 Informationsoverførsler

13.2.1 Politikker og procedurer for informationsoverførsler

- Formelle politikker og procedurer bør indføres for overførsler af information uanset hvilke kommunikationsformer anvendes

- **Krypteret datakommunikation (egen risikovurdering)**
  - Der bør anvendes stærk kryptering for datatrafik, som indeholder autenifikeringsoplysninger.

13.2.2 Aftaler om informationsoverførsler

- Aftaler bør tage højde for sikker overførsel of forretningsmæssig information mellem virksomheden og eksterne parter

13.2.3 Elektroniske meddelelser

- Informationer, der indgår i elekroniske meddelelser, bør sikres på passende vis

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

13.2.4 Fortroligheds- eller tavshedserklæringer

- Virksomhedens behov for fortroligheds- eller tavshedserklæringer bør identificeres, regelmæssigt revurderes og dokumenteres

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

14.1.1 Analyse og specifikation af krav til informationssikkerhed

- Krav til informationssikkerhed bør inkluderes i kravspecifikationer til nye informationssystemer eller forbedringer af eksisterende informationssystemer
- Følgende krav fra OCES bør implementeres:

Udvikling, anskaffelse og vedligeholdelse af it-systemer

  - CA skal benytte anerkendte systemer og produkter, som er beskyttet mod ændringer. Produkterne skal overholde en tilstrækkelig beskyttelsesprofil i henhold til ISO/IEC 15408 eller tilsvarende.

  - CA skal sikre, at der forud for enhver systemudvikling (dvs. egenudvikling eller udvikling ved tredjemand) foreligger en ledelsesgodkendt plan for indbygning af sikkerhed i systemerne.

- **Systemdokumentation (egen risikovurdering)**
  - For alle systemer bør der sikres, at der modtages passende systemdokumentation

14.1.2 Sikkerhed vedrørende applikationstjenester på offentlige netværk

- Informationer, der indgår i applikationstjenester, der passerer over offentlige netværk, bør sikres imod svindel, kontraktmæssige uoverensstemmelser samt uautoriseret videregivelse og ændringer

14.1.3 Beskyttelse af transaktioner fra applikationstjenester

- Informationer vedrørende transaktioner fra applikationstjenester (online transaktioner) bør beskyttes for at forhindre ufuldstændig transmission, fejl-routing, uautoriserede ændringer, uautoriseret videregivelse, uautoriseret duplikering af transmissioner eller gentagelse

14.2 Sikkerhed i udviklings- og supporttjenester

14.2.1 Politik for sikker udvikling

- Regler bør indføres for udvikling af software og systemer, som udvikles af organisationen

14.2.2 Procedurer for ændringsstyring

- Ændringer til systemer under udvikling bør kontrolleres ved formelle procedurer

14.2.3 Teknisk gennemgang af applikationer efter ændringer af operativsystemet

- Når operativsystemer ændres bør forretningskritiske applikationer gennemgås og testes for at sikre, at ændringerne ikke påvirker driften eller sikkerheden

14.2.4 Afgrænsninger til at ændre softwarepakker

- Det bør så vidt muligt undgås at ændre softwarepakker, der supporteres af leverandører, eller at afgrænse sig til kun nødvendige ændringer. Alle ændringer bør være underlagt streng kontrol.

14.2.5 Procedurer for udvikling af sikre systemer

- Procedurer for udvikling af sikre systemer bør indføres, dokumenteres og vedligeholdes. Disse bør gælde for al udvikling af informationssystemer

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

14.2.6 Sikre miljøer for systemudvikling

- Virksomheder bør indføre og behørigt beskytte sikre systemudviklingsmiljøer. Dette bør omfatte hele udviklingens forløb (lifecycle)

14.2.7 Outsourcet udvikling

- Virksomheden bør føre tilsyn med og overvåge outsourcede systemudviklingsaktiviteter

14.2.8 Sikkerhedstests af systemer

- Tester af sikkerhedsfunktionalitet bør udføres løbende i udviklingsfasen

14.2.9 Systemgodkendelsestest

- Der bør etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.

14.3 Testdata

14.3.1 Beskyttelse af testdata

- Testdata bør udvælges med forsigtighed, beskyttes og kontrolleres

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

15.1.1 Informationssikkerhedspolitik for leverandørforhold

- Informationssikkerhedskrav for at minimere risikoen ved at leverandører får adgang til virksomhedens aktiver bør aftales med leverandøren og dokumenteres
- Følgende krav fra OCES bør implementeres:

Kontrol af underleverandører
CA skal sikre, at personale hos underleverandører opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som CA's egne medarbejdere i de funktioner, underleverandørens personale varetager for CA.

  - CA skal ved adgangsprocedurerne sikre, at personale hos underleverandører ikke kan arbejde uovervåget hos CA.

  - RA personale skal gennemføre en uddannelse, som sætter dem i stand til at udføre deres arbejde korrekt og sikkert.

15.1.2 Adressering af sikkerhed i aftaler med leverandører

- Alle relevante sikkerhedskrav bør formuleres og aftales med hver af de leverandører, som får adgang til, behandler, arkiverer, kommunikerer eller leverer IT-infrastrukturkomponenter til virksomhedens informationer

15.1.3 Forsyningskæde for informations- og kommunikationsteknologi

- Aftaler med leverandører bør indeholde krav til håndtering af informationssikkerhedsrisici forbundet med forsyningskæden for IKT-tjenester og -produkter.

15.2 Styring av serviceydelser fra leverandører

15.2.1 Overvågning og gennemgang af serviceydelser fra leverandører

- Virksomheder bør regelmæssigt overvåge, gennemgå og revidere leverancer af serviceydelser fra leverandører

15.2.2 Styring af ændringer til serviceydelser

- Ændringer i leverancer af serviceydelser fra leverandører, inklusive vedligeholdelse og forbedringer af eksisterende informationssikkerhedspolitikker, procedurer og kontroller, bør styres under hensyntagen

til væsentligheden af involverede forretningsinformationer, systemer og processer og revurderinger af risici

16 Styring af sikkerhedshændelser

16.1 Styring af sikkerhedshændelser og forbedringer

16.1.1 Ansvarsområder og procedurer

- Ledelsesansvar og – procedurer bør etableres for at sikre en hurtig, effektiv og redelig respons på sikkerhedshændelser

16.1.2 Rapportering af sikkerhedshændelser

- Sikkerhedshændelser bør rapporteres via passende rapporteringskanaler hurtigst muligt
- Følgende EU krav fra bør implementeres:

Sikkerhedskrav til tillidstjenesteudbydere

- Kvalificerede og ikke kvalificerede tillidstjenesteudbydere skal træffe passende tekniske og organisatoriske foranstaltninger til at styre de sikkerhedsmæssige risici i forbindelse med de tillidstjenester, de udbyder. Under hensyn til den seneste teknologiske udvikling skal disse foranstaltninger garantere et sikkerhedsniveau, der svarer til risikoens omfang. Tillidstjenesteudbyderne bør navnlig tage skridt til at forhindre og minimere virkningen af sikkerhedsrelaterede hændelser og underrette de berørte parter om de negative virkninger af sådanne hændelser.

- De kvalificerede og ikkekvalificerede tillidstjenesteudbydere, der konstaterer et brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger, skal hurtigst muligt og under alle omstændigheder inden for 24 timer efter at være blevet opmærksomme på forholdet underrette tilsynsorganet, og eventuelt andre relevante organer som f.eks. det kompetente nationale organ for informationssikkerhed eller databeskyttelsesmyndigheden.

- Når det er sandsynligt, at et brud på sikkerheden eller tab af integritet vil krænke den fysiske eller juridiske person, som har modtaget tillidstjenesten, skal tillidstjenesteudbyderen også hurtigst muligt underrette den fysiske eller juridiske person om bruddet på sikkerheden eller tab af integritet.

16.1.3 Rapportering af svagheder

- Medarbejdere og eksterne samarbejdspartnere, som anvender virksomhedens informationssystemer og tjenester bør anmodes om at notere og rapportere enhver sikkerhedsmæssig svaghed i systemer eller tjenester, som de observerer eller har mistanke om

16.1.4 Vurderinger af og afgørelser om sikkerhedsmæssige begivenheder

- Alle sikkerhedsmæssige begivenheder bør vurderes, og det bør besluttes, om disse skal klassificeres som sikkerhedshændelser

16.1.5 Reaktion på sikkerhedshændelser

- Der bør reageres på alle sikkerhedshændelser i henhold til en dokumenteret procedure

16.1.6 Erfaring fra informationssikkerhedsbrud

- Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, bør anvendes til at nedsætte sand synligheden for eller virkningen af fremtidige brud.

16.1.7 Indsamling af beviser

- Virksomheden bør indføre procedurer for identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som beviser

Prioritet: Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

17 Informationssikkerhedsmæssige aspekter ved beredskabsstyring

17.1 Informationssikkerheds kontinuitet

17.1.1 Planlægning af informationssikkerheds kontinuitet

- Virksomheder bør fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe
- Følgende krav fra OCES bør implementeres:

Beredskabsplanlægning

Følgende hændelser skal betragtes som alvorlige:

- kompromittering af CA's private nøgle,
- mistanke om kompromittering af CA's private nøgle,
- nedbrud og kritiske fejl på CA's driftskomponenter (spærrelister etc.) samt
- stop af CA-driftsmiljøet som følge af brand, elforsyningssvigt osv.

- CA skal i tilfælde af kompromittering af CA's private nøgle eller mistanke herom straks informere alle certifikatindehavere via den registrerede e-mailadresse. CA skal ligeledes straks informere IT- og Telestyrelsen med en uddybende beskrivelse af den opstående situation.

- CA skal ligeledes på sin hjemmeside og i det omfang det vurderes relevant under hensyntagen til den opstående situation, via offentlige medier eller ved direkte kontakt, straks informere signaturmodtagere.

- CA skal i tilfælde af alvorlige hændelser på databehandlingsudstyr, programmel og/eller data orientere certifikatindehavere herom i det omfang, det er relevant for deres brug af CA-tjenesterne. Under hensyntagen til den opståede situation, skal signaturmodtagere informeres via offentlige medier og ved annoncering i dagspressen.

- CA skal sikre, at alle procedurer med relation til spærrelister, herunder anmodning om spærring, har højeste prioritet i forbindelse med retablering af forretningsgange efter et driftsnedbrud.

17.1.2 Implementering af informationssikkerheds kontinuitet

- Virksomheder bør fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre det nødvendige niveau af kontinuitet af informationssikkerhed i en skadelignende situation

- **No-break og generator (egen risikovurdering)**
  - Systemernes koninuerlige drift bør beskyttes med passende no-break anlæg og dieselgenerator.

17.1.3 Verificer, gennemgå og evaluer informationssikkerheds kontinuitet

- Virksomheder bør regelmæssigt verificere de etablerede og implementerede kontroller for informationssikkerheds kontinuitet for at sikre, at de er aktuelle og effektive i skadelignende situationer

17.2 Redundans

17.2.1 Tilgængelighed af faciliteter

- Informationsbehandlingsfaciliteter bør implementeres med tilstrækkelig redundans svarende til behovet for tilgængelighed

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

18 Overensstemmelse

18.1 Overensstemmelse med lov- og kontraktkrav

18.1.1 Identifikation af gældende lovgivnings- og kontraktmæssige krav

- Alle relevante lovgivnings- og kontraktmæssige krav og virksomhedens metoder for at overholde disse bør identificeres, dokumenteres og holdes ajour for hvert enkelt system samt for virksomheden
- Følgende krav fra OCES bør implementeres:

Overensstemmelse med lovgivningen

- CA og RA skal sikre overensstemmelse med lovgivningen, herunder særligt lov om behandling af personoplysninger.

Særlige forpligtelser med henblik på beskyttelse af fortrolig information

- Information, som ikke indgår i certifikater og spærrelister, anses som fortrolig. Information, som indgår i certifikater, anses som ikke fortrolig og ikke privat.

- Personrelateret information, som ikke indgår i certifikatet, anses som privat information. CA skal sikre, at en certifikatindehaver har mulighed for at kræve, at navne- og adresseinformation, herunder e-postadresse ikke fremgår af certifikatet (gælder kun personcertifikat). CA og RA skal sikre, at fortrolig information er beskyttet mod kompromittering og må ikke benytte fortrolig information til andet, end hvad der er påkrævet for driften af CA.

- CA og RA skal sikre, at privat information er beskyttet mod kompromittering og må ikke benytte privat information udover, hvad der er påkrævet for drift af CA.

- CA og RA skal sikre, at statistiske oplysninger om anvendelse af OCES- personcertifikater ikke kan henføres til det enkelte OCES-certifikat.

- Kan en tvist ikke løses forligsmæssigt, kan enhver af parterne vælge at indbringe tvisten for de almindelige domstole. Værneting er København. Dansk ret er gældende.

Placering af datacentre

- Kravene i denne CP gælder uanset, at CA placerer hele eller dele af driftsmiljøet i udlandet. Den løbende kontrol, der er fastsat i CP'en, skal således kunne gennemføres, uanset hvor CA geografisk er placeret.

18.1.2 Immaterielle rettigheder

- Passende procedurer bør indføres for at sikre overholdelse af lovgivnings- og kontraktmæssige krav relateret til immaterielle rettigheder og anvendelse af patenterede og navnebeskyttede softwareprodukter

18.1.3 Beskyttelse af registre

- Registre bør beskyttes imod tab, ødelæggelse, forfalskninger, uautoriseret adgang samt uautoriseret frigivelse i henhold til lovgivnings-, kontraktmæssige samt forretningsmæssige krav

18.1.4 Privatlivets fred og beskyttelse af personoplysninger

- Personlige oplysninger og beskyttelse af personhenførbare informationer bør sikres i henhold til krav i relevant lovgivning, som måtte være gældende

18.1.5 Regulering af kryptografi

- Privatlivets fred og personoplysninger bør beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter

Prioritet:		
Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

18.2 Gennemgang af informationssikkerhed

18.2.1 Uafhængig gennemgang af informationssikkerhed

- Virksomhedens tilgang til informationssikkerhedsstyring samt implementering af heraf (f.eks. kontrolmål, kontroller, politikker og procedurer for informationssikkerhed) bør gennemgås af uafhængige parter efter planlagte intervaller eller ved væsentlige ændringer

- Følgende EU krav bør implementeres:

Overholdelse og revision

Lav

- Der gennemføres jævnlige interne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.

Betydelig

- Der gennemføres jævnligt interne eller eksterne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.

Høj

- Der gennemføres jævnligt uafhængige eksterne revisioner, som omfatter alle de relevante dele til levering af den pågældende tjeneste, og som sikrer overholdelse af den relevante politik.

- Følgende krav fra OCES bør implementeres:

Systemrevision (OCES)

- Der skal gennemføres systemrevision hos CA. Ved systemrevision forstås revision af:
  - Generelle it-kontroller i virksomheden,
  - It-baserede brugersystemer m.v. til generering af nøgler og nøglekomponenter samt registrering, udstedelse, verificering, opbevaring og spærring af certifikater og
  - It-systemer til udveksling af data med andre.

Valg af systemrevisor - dennes beføjelser og pligter

- CA skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen hos CA. IT- og Telestyrelsen kan i særlige tilfælde dispensere fra kravet om, at systemrevisor skal være statsautoriseret revisor. CA skal senest en måned efter valg af systemrevisor anmelde dette til IT- og Telestyrelsen.

- CA skal udlevere de oplysninger, som er nødvendige for systemrevisionen i CA. Herunder skal CA give den valgte systemrevisor adgang til ledelsesprotokollen.

- CA skal give den valgte systemrevisor adgang til ledelsesmøder under behandling af sager, der har betydning for systemrevisionen. Ved et ledelsesmøde forstås et møde mellem den øverste ledelse af CA, i praksis ofte et bestyrelsesmøde. Ved udtrykket
- CA's ledelse forstås i denne sammenhæng den øverste ledelse af CA, dvs. bestyrelse eller tilsvarende ledelsesorgan afhængigt af, hvorledes CA er organiseret. CA skal sikre, at den valgte systemrevisor deltager i ledelsens behandling af pågældende sager, såfremt det ønskes af blot et ledelsesmedlem.

- I CA'er, hvor der afholdes generalforsamling, finder årsregnskabslovens bestemmelser om revisionens pligt til at besvare spørgsmål på et selskabs generalforsamling tilsvarende anvendelse for den valgte systemrevisor.

Prioritet: Sort: Krav, der bør opfyldes fra start	Grøn: Krav, der kan vente, indtil virksomheden er kommet i gang	Blå: Krav, der bør opfyldes, når det er relevant

- CA skal gøre den valgte systemrevisor bekendt med, at denne i overensstemmelse med god revisionsskik skal foretage den nedenfor nævnte systemrevision, herunder at påse, at:
  - CA's systemer er i overensstemmelse med kravene i denne CP,
  - CA's sikkerheds-, kontrol- og revisionsbehov tilgodeses i tilstrækkeligt omfang ved udvikling, vedligeholdelse og drift af CA's systemer,
  - CA's forretningsgange såvel de edb-baserede som de manuelle er betryggende i sikkerheds- og kontrolmæssig henseende og i overensstemmelse med CA's certificeringspraksis (CPS).

- CA skal sikre, at der i forbindelse med systemrevisionen foretages en sårbarheds- vurdering af logningsproceduren.

18.2.2 Overholdelse af sikkerhedspolitikker og sikkerhedsstandarder

- Lederne bør regelmæssigt undersøge, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav

18.2.3 Undersøgelse af teknisk overensstemmelse

- Informationssystemer bør undersøges regelmæssigt for, om de er i overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder