**Bilag 5**

**IT-sikkerhedskrav**

**GG!**

**Hetta skjal er úr eini avtalu, sum Gjaldstovan hevur við ein veitara og verður víst her sum eitt dømi um, hvussu eitt trygdarskjal kann síggja út.**

# 1 Formål og ansvar

Formålet med sikkerhedsbilaget er i forlængelse af hovedaftalen med bilag at klarlægge og uddybe ansvarsfordelingen mellem Kundi og Veitari af sikkerhedskrav.

## Anvendelsesområde

Bilaget om informationssikkerhedskontroller specificerer ansvar og opgaver fordelt mellem Kundi og Veitari vedrørende sikkerhedskontroller til beskyttelse af Kundi aktiver og informationer. Endvidere danner det grundlag for dokumentation af de af Veitari foreståede sikkerhedsydelser.

En uafhængig revision bør vurdere hvor­vidt sikkerhedskontrollerne på Veitari er tilstrækkelige.

Samtlige services og Kundi systemer administreret af Veitari under hovedaftalen med bilag bør leve op til kravene, der er defineret i dette bilag.

Dette bilag er et standard sikkerhedsbilag ved outsourcing, derfor omhandler det alle sikkerhedskrav. Bliver der f.eks. ikke udviklet på vegne af Kundi, er sikkerhedskravene vedrørende udvikling ikke relevante.

## Veitari arbeiðir bert eftir fyriskipan hjá Kundi.

Veitari, sum dátuviðgeri váttar, at halda ásetingarnar um trygd í § 31 í persónsupplýsingarlógini, (løgtingslóg nr. 73 frá 8. mai 2001 um viðgerð av persónsupplýsingum, sum broytt við løgtingslóg nr. 24 frá 17. mai 2004), og at reglurnar í § 31 stk. 3-5 eru eins galdandi fyri tann, sum fær persónsupplýsingarnar og fyri dátuábyrgdaran.

Dátuviðgerin tryggjar, at viðgerðin av upplýsingunum nøktar tær treytir, persónsupplýsingarlógin setir um trúnað, sjálvræðisrætt og innlit eins og við tekniskum og fyriskipanarligum tiltøkum skal tryggjast, at persónsupplýsingar ikki av tilvild ella ólógliga verða burturbeindar, burturmistar ella minka í virði, og at ikki óviðkomandi fáa kunnleika til persónsupplýsingarnar, misbrúka tær ella annars ólógliga viðgera tær. Skjalprógv um skipað tiltøk skulu vera atkomilig fyri starvsfólkum dátuábyrgdarans og Veitari eins og fyri dátueftirlitinum.

# 2 Definitioner

De samlede sikkerhedskrav

De samlede sikkerhedskrav udgøres af nærværende sikkerhedsbilag til hovedaftalen med bilag, Veitari sikkerhedspolitik og retningslinjer for it-sikkerhed. Der kan herudover på specifikke områder være yderligere styrende dokumenter såsom supplerende politikker, retningslinjer og procesbeskrivelser.

Sikkerhedssystemer

Sikkerhedssystemer omfatter softwaresystemer og hardware komponenter der varetager sikkerheden f.eks. IDS, IPS, firewall, router og antivirus.

Bør

Hovedregelen er, at kravene **skal** opfyldes. Undtagelse herfor kan kun gøres med Kundi skriftlige accept.

# 3 Opbygning af dette bilag

Dette bilag indeholder sikkerhedskrav samt ansvarsområder og deres fordeling mellem Kundi og Veitari. Selve dokumentet bygger strukturelt på standarden "ISO/IEC 27002: InformationTechnology – Code of Practice for Information Security Management", som danner rammerne for beskyttelse af information. Ifølge denne standard bør en informationssikkerhedspolitik fastsætte passende sikkerhedskontroller for hver af i alt 14 punkter baseret på følgende tre variable:

* risikovurdering
* forretningsprincipper og -målsætninger
* forpligtelser i henhold til love, regler, bekendtgørelser og kontrakter

De 14 punkter er opstillet nedenfor efter samme nummerering som disses afsnit i stan­darden ISO/IEC 27002:

1. Informationssikkerhedspolitikker
2. Organisering af informationssikkerhed
3. Medarbejdersikkerhed
4. Styring af aktiver
5. Adgangstyring
6. Kryptografi
7. Fysisk sikring og miljøsikring
8. Driftssikkerhed
9. Kommunikationssikkerhed
10. Anskaffelse, udvikling og vedligeholdelse af systemer
11. Leverandørforhold
12. Styring af informationssikkerhedsbrud
13. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
14. Overensstemmelse

#  4 Risikovurdering, trusler og forretningsmæssig påvirkning

Risikovurderinger skal identificere og prioritere de forretningsmæssige risici Kundi og Veitari er udsat for.

Dette bilag er ikke specifikt angående flere sikkerhedstiltag, derfor bør sikkerhedsmæssige afgørelser baseres på kvalificerede risikovurderinger, og f.eks. ISO/IEC 27002, hvor krav og implementeringsvejledninger forefindes.

Ud fra et samlet risikobillede af trusler, konsekvenser og sandsynligheder kan de relevante sikkerhedsbehov afdækkes og prioriteres.

Både Kundi og Veitari er ansvarlige for, at risikovurderingerne udføres.

# 5 Informationssikkerhedspolitikker

## Veitari ansvarsområder

### 5.1 Retningslinjer for styring af informationssikkerhed

Formålet er at give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med

forretningsmæssige krav og relevante love og forskrifter.

***5.1.1 Politikker for informationssikkerhed***

* kunne fremvise en ledelsesgodkendt it-sikkerhedspolitik der er kommunikeret til relevante personer og som indeholder relevante krav i henhold til en anerkendt standard
* IT-sikkerhedspolitikken børunderstøttes af emnespecifikke politikker
* overholde krav og sikkerhedsregler som er fastlagt i lov om behandling af personoplysninger
* placere et overordnet ansvar for Veitari it-sikkerhed og it-sikkerhedspolitik

***5.1.2 Gennemgang af politikker for informationssikkerhed***

* revidere Veitari it-sikkerhedspolitik en gang om året og når væsentlige ændringer er i miljøet
* gennemgå de samlede sikkerhedskrav (dette dokument, nye risici, lovkrav, krav fra standard, politikker m.m.) med Kundi mindst en gang om året
* gå i åben dialog med Kundi, hvis denne anmoder om ændringer i Veitari sikkerhedspolitik eller relevante retningslinjer. Dialogen bør fokusere på relevansen i anmodningerne og specielt lægge vægt på om ændringerne:
* kan implementeres uden at gå på kompromis med de fastsatte rammer for sikkerhed
* hvis de implementeres, vil udgøre en ny serviceydelse
* hvis de implementeres, vil frembringe nye risici.

## Kundi ansvarsområder

### 5.1 Retningslinjer for styring af informationssikkerhed

Formålet er at give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med

forretningsmæssige krav og relevante love og forskrifter.

***5.1.2 Gennemgang af politikker for informationssikkerhed***

* fastsætte passende sikkerhedskrav baseret på forretningsmål, risikovurdering samt fortolkning af lov/regel-bestemt og kontraktmæssige forpligtelser
* gennemgå de samlede sikkerhedskrav (dette dokument, nye risici, lovkrav, krav fra standard, politikker m.m.) med Veitari en gang om året. Dette bør forestås af Kundi sikkerhedsansvarlige
* holde sig orienteret om og acceptere de sikkerhedskontroller der er i Kundi miljø.
* informere Veitari om ændringer i Kundi sikkerhedskrav

# 6 Organisering af informationssikkerhed

## Veitari ansvarsområder

### 6.1 Intern organisering

Formålet er at etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed.

***6.1.1 Roller og ansvarsområder for informationssikkerhed***

* Opretholde en sikkerhedsorganisation
* Ansvarsområder bør angives til personer med tilstrækkelig kvalifikationer
* anvise en kontaktperson med relevante sikkerhedskompetencer hos Veitari for sikkerhedsrelaterede aktiviteter
* implementere og kontrollere sikkerhedskrav som beskrevet i aftalen
* koordinere og gennemføre audit-aktiviteter evt. i samarbejde med en revisor
* koordinere alle sikkerhedsaktiviteter udført af tredjemand for Veitari indenfor hovedkontraktens område
* samarbejde med Kundi vedrørende sikkerhedskrav og –hændelser
* levere og koordinere nødvendige sikkerhedsressourcer i forbindelse med aftalen
* sørge for sikkerhedsforanstaltninger, der beskytter Kundi data og systemer i forhold til fortrolighed, integritet og tilgængelighed
* tage fuldt ejerskab for alle krav til Veitari og retningslinjer i dette bilag
* give en skriftlig besvarelse på Kundi forespørgsler omkring sikkerhedskontroller i Kundi miljø
* sikre at etablering af nye tekniske miljøer og platforme er i overensstemmelse med de samlede sikkerhedskrav
* sikre at ændringer foretaget på Veitari initiativ er overensstemmende med de samlede sikkerhedskrav

 ***6.1.2 Funktionsadskillelse***

* Modstridende funktioner og ansvarsområder bør adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af Veitari/Kundi aktiver.
* der bør være person-/funktionsadskillelse mellem udvikling og drift.
Hvor dette ikke er praktisk muligt, skal begrænsninger og kompenserende kontroller etableres. Gevinsten af kontrollerne skal stå i forhold til omkostningerne.
Kundi skal godkende undtagelser fra funktionsadskillelsen samt godkende opfølgende kontroller.
* Veitari interne it-revisor må ikke være privilegeret bruger i Kundi systemer
* ingen person må gennem egne eller delte brugerkonti m.v. have fysisk og/eller logisk adgang til samtlige generationer af data

***6.1.3 Kontakt med myndigheder***

* Der bør opretholdes passende kontakt med relevante myndigheder, for eksempel Dátueftirlitið, således at der i tilfælde af f.eks. trusler fra internettet kan reageres hurtigt
* som hovedregel skal en henvendelse til en myndighed, som kun involverer Kundi systemer, gå via Kundi. Kundi skal informeres hurtigst muligt, hvis Kundi systemer eller data er involveret

***6.1.4 Kontakt med særlige interessegrupper***

* Der bør opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer
* Veitari bør sammen med Kundi hvert år gennemgå trusselbilledet, med særlig vægt på ændringer. Gennemgangen bør indeholde:
	+ identificerede trusler
	+ foreslåede handlinger til imødegåelse af hver enkel identificeret trussel
	+ foreslåede handlinger til hvert enkelt identificeret nyt eksternt krav
* bliver Veitari bekendt med betydende ændring i trusselsbilledet skal dette uden unødigt ophold meddeles Kundi

***6.1.5 Informationssikkerhed ved projektstyring***

* Der bør være fokus på informationssikkerheden ved projektstyring, uanset projekttype.

### 6.2 Mobilt udstyr og fjernarbejdspladser

Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.

***6.2.1 Politik for mobilt udstyr***

* Der bør vedtages en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.
* Der bør sikres, at opbevaring på mobile enheder som f.eks. bærbare pc'ere, smartphones og øvrige media håndteres i overensstemmelse med Kundi klassificering af data

***6.2.2 Fjernarbejdspladser***

* Der bør implementeres en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.

## Kundi ansvarsområder

### 6.1 Intern organisering

Formålet er at etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

***6.1.1 Roller og ansvarsområder for informationssikkerhed***

* Anvise et entydigt kontaktpunkt hos Kundi i forhold til alle sikkerhedsrelaterede aktiviteter og hændelser
* samarbejde med Veitari vedrørende sikkerhedskrav og –hændelser
* tage fuldt ejerskab for alle krav til Kundi og retningslinjer i dette bilag

 ***6.1.3 Kontakt med myndigheder***

* Der bør opretholdes passende kontakt med relevante myndigheder, således at der i tilfælde af f.eks. trusler fra internettet kan reageres hurtigt
* Kundi skal være Veitari behjælpelig med at etablere kontakter

***6.1.4 Kontakt med særlige interessegrupper***

* Der bør opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.
* Kundi bør sammen med Veitari hvert år gennemgå trusselbilledet, med særlig vægt på ændringer. Gennemgangen bør indeholde:
* identificerede trusler
* foreslåede handlinger til imødegåelse af hver enkel identificeret trussel
* foreslåede handlinger til hvert enkelt identificeret nyt eksternt krav
* bliver Kundi bekendt med betydende ændring i trusselsbilledet skal dette uden unødigt ophold meddeles Veitari

# 7 Medarbejdersikkerhed

## Veitari ansvarsområder

### 7.1 Før ansættelse

Formålet er at sikre, at medarbejdere og konsulenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.

**7.1.1 Screening**

* Ansættelse af nye medarbejdere bør foregå efter en fastlagt procedure
* Der bør være en process for godkendelse af konsulenter

**7.1.2 Ansættelsesvilkår og -betingelser**

* relevante medarbejdere på Veitari bør være bekendt med og overholde Veitari samlede sikkerhedskrav
* personale, der kan komme til at arbejde i Kundi miljø, bør påkræves en straffeattest uden forhold der er relevante for Kundi og dennes brugere. Straffeattesten bør rekvireres og vurderes ved ansættelse og ved eventuel usikkerhed om den aktuelle status. Uden begrundet mistanke, er det ikke pålagt Veitari at rekvirere straffeattest for værende medarbejdere
* Veitari personale bør iagttage ubetinget tavshed med hensyn til oplysninger vedrørende Kundi eller andres forhold, som kommer til deres kendskab i forbindelse med de i denne kontrakt omhandlede leverancer, tjenesteydelser m.v. Veitari personale bør acceptere dette ved at underskrive en generel tavshedserklæring
* ansatte ved Veitari underleverandører bør underskrive personlige tavshedserklæringer før de gives adgang til Kundi udstyr og informationer eller bør en skriftlig aftale med underleverandøren bekræfte de ansattes tavshedspligt

### 7.2 Under ansættelsen

Formålet er at sikre, at medarbejdere og konsulenter er bevidste om og lever op til deres

informationssikkerhedsansvar.

**7.2.1 Ledelsesansvar**

* Medarbejdere bør være grundigt orienteret om deres roller og ansvarsområder
* Der bør sikres, at medarbejderne fortsat har de nødvendige kvalifikationer og undervises med jævne mellemrum

**7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed**

* Der bør sørges for at medarbejdere, der direkte eller indirekte arbejder i Kundi miljø, deltager i awareness programmer, og er bekendt med Veitari sikkerhedsprocedurer og særlige sikkerhedskrav, som måtte være gældende for Kundi systemer
* Der bør sørges for at medarbejdere ved Veitari eventuelle underleverandører, der arbejder direkte eller indirekte med Kundi udstyr og informationer lever op til samme krav, som Kundi stiller til Veitari ansatte

**7.2.3 Sanktioner**

* Der bør sørges for passende ledelsesmæssige sanktioner overfor Veitari ansatte ved misbrug og/eller brud på sikkerhedsregler
* Der bør sørges for passende sanktioner overfor Veitari konsulenter ved misbrug og/eller brud på sikkerhedsregler

7.3Ansættelsesforholdets ophør eller ændring

Formålet er at beskytte parternes interesser som led i ansættelsesforholdets ændring eller ophør.

**7.3.1 Ansættelsesforholdets ophør eller ændring**

* Der bør sørges for at adgang til Kundi udstyr og informationer fjernes omgående når ansættelsesforholdet med Veitari eller dennes underleverandører ophører

## Kundi ansvarsområder

### 7.1 Før ansættelse

Formålet er at sikre, at medarbejdere og konsulenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.

**7.1.1 Screening**

* Ansættelse af nye medarbejdere bør foregå efter en fastlagt procedure
* Der bør være en screeningsprocess for konsulenter

**7.1.2 Ansættelsesvilkår og –betingelser**

* Kundi personale bør iagttage ubetinget tavshed med hensyn til oplysninger vedrørende Veitari eller andres forhold, som kommer til deres kendskab i forbindelse med de i denne kontrakt omhandlede leverancer, tjenesteydelser m.v.
* konsulenter og andre, der på Kundi vegne deltager i projekter med Veitari, pålægges ubetinget tavshed med hensyn til oplysninger vedrørende Veitari eller andres forhold, som kommer til deres kendskab i denne forbindelse. Dette bør accepteres ved at underskrive en tavshedserklæring

### 7.2 Under ansættelsen

Formålet er at sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres

informationssikkerhedsansvar.

**7.2.1 Ledelsesansvar**

* Medarbejdere/konsulenter bør være grundigt orienteret om deres roller og ansvarsområder
* Der bør sikres, at medarbejderne fortsat har de nødvendige kvalifikationer og undervises med jævne mellemrum

**7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed**

* kommunikere de generelle sikkerhedspolitikker og sikker­heds­procedurer til slutbrugere (for eksempel passwordkrav, brug af antivirusprogrammer, sikkerhedsprocedurer m.v.)
* sørge for at medarbejdere, der direkte eller indirekte arbejder sammen med Veitari, deltager i awareness programmer
* sørge for at medarbejdere ved Kundi eventuelle underleverandører, der arbejder direkte eller indirekte med Veitari lever op til samme krav, som Kundi stiller sine ansatte

**7.2.3 Sanktioner**

* sørge for passende ledelsesmæssige sanktioner overfor Kundi ansatte ved misbrug og/eller brud på sikkerhedsregler
* sørge for passende sanktioner overfor Kundi konsulenter ved misbrug og/eller brud på sikkerhedsregler

7.3Ansættelsesforholdets ophør eller ændring

Formålet er at beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.

**7.3.1 Ansættelsesforholdets ophør eller ændring**

* sørge for at adgang til Kundi udstyr og informationer fjernes omgående når ansættelsesforholdet med Kundi eller dennes underleverandører ophører

# 8 Styring af aktiver

## Veitari ansvarsområder

### 8.1 Ansvar for aktiver

Formålet er at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

**8.1.1 Fortegnelse over aktiver**

* Veitari bør have oversigt over egne aktiver i relation til Kundi

**8.1.2 Ejerskab af aktiver**

* Der bør udpeges en ansvarlig i organisationen for hvert aktiv i relation til Kundi

**8.1.3 Accepteret brug af aktiver**

* Aktiver, der indeholder Kundi systemer og data bør behandles i følge Kundi klassifikation

**8.1.4 Tilbagelevering af aktiver**

* Veitari skal sikre, at Kundi data ikke bliver udleveret på aktiver, som forhenværende medarbejdere og konsulenter får lov til at beholde
* Veitari bør sikre, at viden, som er vigtig for den videre drift ikke forsvinder med forhenværende medarbejdere og konsulenter

### 8.2 Klassifikation af information

Formålet er at sikre passende beskyttelse af information, der står i forhold til informationens betydning for Kundi

**8.2.1 Klassifikation af information**

* Veitari bør forholde sig til Kundi klassificering af systemer og data

**8.2.2 Mærkning af information**

* Veitari bør sikre, at uvedkommende ikke har adgang til Kundi data

**8.2.3 Håndtering af aktiver**

* håndtering af informationsaktiver bør ske i overensstemmelse med Kundi klassifikation af informationsaktiver
* passende sikkerhedskontrol bør implementeres til sikring av dataintegritet og tilgængelighed i overensstemmelse med de af Kundi fastsatte krav

### 8.3 Mediehåndtering

Formålet er at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

**8.3.1 Styring af flytbare medier**

* udprintet materiale, bærbare lagermedier, herunder ukrypterede harddiske i bærbare pc'ere m.v., der indeholder Kundi data, som er klassificeret som fortrolige, bør altid opbe­vares i fysisk kontrollerede områder og bør ikke flyttes her fra uden særlig tilladelse hertil.
Arbejdsrelateret flytning er dog tilladt f.eks. til og fra møder

**8.3.2 Bortskaffelse af medier**

* Medier der kan indeholde Kundi data skal bortskaffes på forsvarlig vis ved ødelæggelse efter formelle procedurer
* Veitari bør holde sig ajour med viden om ødelæggelsesmetoder

**8.3.3 Transport af fysiske medier**

* Der bør være en oversigt over medier, der bliver transporteret
* Som hovedregel bør transport foretages af Veitari personale og være direkte mellem lokationerne, dvs. uden unødvendigt ophold

## Kundi ansvarsområder

### 8.1 Ansvar for aktiver

Formålet er at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

**8.1.1 Fortegnelse over aktiver**

* Anmode Veitari om oversigt over aktiver, som er relateret til Kundi systemer og data

**8.1.4 Tilbagelevering af aktiver**

* sikre, at fortrolig data om eller fra Veitari ikke bliver udleveret på aktiver, som forhenværende medarbejdere og konsulenter får lov til at beholde
* sikre, at viden, som er vigtig for den videre drift ikke forsvinder med forhenværende medarbejdere og konsulenter

### 8.2 Klassifikation af information

Formålet er at sikre passende beskyttelse af information, der står i forhold til informationens betydning for Kundi

**8.2.1 Klassifikation af information**

* Udlevere Kundi klassifikation af systemer og data, herunder de specifikke krav til databeskyttelse, tilgængelighed m.v. som afledes af dataklassifikationen
* anvise hvem der er Kundi ansvarlige for informationsaktiver og såfremt det er nødvendigt, hvem der evt. yderligere er tildelt fuldmagt til at træffe beslutninger af betydning til informationsaktiverne
* at overholde Kundi forpligtelser som dataansvarlig i henhold til Persondataloven og informere Veitari, såfremt Veitari rolle som databehandler giver anledning til særlige forholdsregler

### 8.3 Mediehåndtering

Formålet er at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

**8.3.2 Bortskaffelse af medier**

* Medier der kan indeholde Kundi/Veitari data skal bortskaffes på forsvarlig vis ved ødelæggelse efter formelle procedurer
* Kundi bør holde sig ajour med viden om ødelæggelsesmetoder

#

# 9 Adgangsstyring

## Veitari ansvarsområder

### 9.1 Forretningsmæssige krav til adgangsstyring

Formålet er at begrænse adgangen til information og informationsbehandlingsfaciliteter.

Som udgangspunkt har Veitari ansvar for brugeradministration af privilegerede brugere og administratorer på netværkskomponenter, sikkerhedssystemer og servere, mens Kundi har brugeradministration af slutbrugere.

**9.1.1 Politik for adgangsstyring**

* på IT-systemer skal Kundi informationer samt medarbejderdata til stedse beskyttes gennem adgangskontrol

**9.1.2 Adgang til netværk og netværkstjenester**

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

### 9.2 Administration af brugeradgang

Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

**9.2.1 Brugerregistrering og -afmelding**

* autorisere og administrere egne bruger-ID'er
* sikre, at der ikke eksisterer delte brugeradgange, men at alle konti er personhenførbare. Hvor dette ikke er muligt skal dokumentation forefindes
* få Kundi accept før personer uden for Veitari får adgang til Kundi systemer
* fjerne adgange, når Veitari personale ikke længere har behov for adgang
* sikre, at konti m.m., der anvendes af leverandører til fjernadgang, kun er aktive i den påkrævede periode

**9.2.2 Tildeling af brugeradgang**

* tildeling og ændring af adgange bør altid følge en defineret og dokumenteret proces
* overholde Veitari standard for navngivning ved tilføjelse og ændring af Kundi brugerid’er

**9.2.3 Styring af privilegerede adgangsrettigheder**

* Tildeling og anvendelse af privilegerede adgangsrettigheder bør begrænses og styres
* have procedurer for at opbevare administrative passwords, og på Kundi anmodning kunne levere en ajourført oversigt over disse for Kundi systemer, der er under Veitari administration
* godkende anmodning om privilegeret adgang for Kundi personale til operativ­systemer, applikationer, softwareværktøjer, systemer og enheder under Veitari ansvar

**9.2.4 Styring af hemmelig autentifikationsinformation om brugere**

* brugere skal informeres om, at password er hemmelige og må ikke videregives. Passwords til delte bruger-id’er bør holdes indenfor gruppen
* altid og straks ændre default password leveret af leverandøren før systemet bliver taget i brug (såsom default passwords til applikationer, middleware, database­syste­mer og OS, SNMP community strings, herunder fjerne unødvendige konti). Nye pass­words bør overholde Veitari retningslinjer.
* opretholde egen proces for reset af passwords og aflevere disse på en sikker måde

**9.2.5 Gennemgang af brugernes adgangsrettigheder**

* udføre årlig gennemgang af bruger-ID'er, herunder:
* individuelt revurdere om Veitari privilegerede bruger-ID'er og andre brugere fortsat har et arbejdsbetinget behov for adgang
* efter revurdering at fremsende liste over Veitari bruger-ID'er til Kundi sikkerhedsfunktion til godkendelse

**9.2.6 Inddragelse eller justering af adgangsrettigheder**

* Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter bør inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.

### 9.3 Brugernes ansvar

Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.

**9.3.1 Brug af hemmelig autentifikationsinformation**

Det bør være et krav, at brugere følger Veitari praksis ved anvendelse af hemmelig

autentifikationsinformation

### 9.4 Styring af system- og applikationsadgang

Formålet er at forhindre uautoriseret adgang til systemer og applikationer.

**9.4.1 Begrænset adgang til informationer**

* Adgang til informationer og applikationssystemers funktioner bør begrænses

**9.4.2 Procedurer for sikker log-on**

* Der bør forefindes en sikker log-on procedure
* Behandle forespørgsler til password politikker fra Kundi
* håndhæve passwordregler for bruger-ID'er og konti for systemer, applikationer, enheder og netværksinfra­struktur som defineret
* afvigelser, f.eks. forårsaget af tekniske afhængigheder, skal godkendes af Kundi

**9.4.3 System for administration af adgangskoder**

* Systemer til administration af adgangskoder bør være interaktive og bør sikre, at koderne er af høj kvalitet

**9.4.4 Brug af privilegerede systemprogrammer**

* Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, bør begrænses og styres effektivt

**9.4.5 Styring af adgang til kildekoder til programmer**

* Adgang til kildekoder til programmer samt dokumentation bør begrænses.

## Kundi ansvarsområder

### 9.1 Forretningsmæssige krav til adgangsstyring

Formålet er at begrænse adgangen til information og informationsbehandlingsfaciliteter.

Som udgangspunkt har Veitari ansvar for brugeradministration af privilegerede brugere og administratorer på netværkskomponenter, sikkerhedssystemer og servere, mens Kundi har brugeradministration af slutbrugere.

**9.1.2 Adgang til netværk og netværkstjenester**

* admini­strere logisk adgang til eventuelle netværksinfrastruktursystemer og enheder under Kundi administration

### 9.2 Administration af brugeradgang

Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

**9.2.1 Brugerregistrering og -afmelding**

* i hvert enkelt tilfælde at give accept inden Veitari opretter en bruger uden for Veitari
* sikre, at konti m.m., der anvendes af leverandører til fjernadgang, kun er aktive i den påkrævede periode

**9.2.2 Tildeling af brugeradgang**

* administrere bruger-ID'er til applikationer, databaser og andre softwareværktøjer på systemer, som kontrolleres af Kundi

**9.2.3 Styring af privilegerede adgangsrettigheder**

* Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres
* have procedurer for at opbevare administrative passwords
* godkende anmodning om privilegeret adgang for Veitari personale til operativ­systemer, applikationer, softwareværktøjer, systemer og enheder under Kundi ansvar

**9.2.4 Styring af hemmelig autentifikationsinformation om brugere**

* brugere skal informeres om, at password er hemmelige og må ikke videregives. Passwords til delte bruger-id’er bør holdes indenfor gruppen
* altid og straks ændre default password leveret af leverandøren før systemet bliver taget i brug (såsom default passwords til applikationer, middleware, database­syste­mer og OS, SNMP community strings, herunder fjerne unødvendige konti). Nye pass­words bør overholde Kundi retningslinjer.

**9.2.5 Gennemgang af brugernes adgangsrettigheder**

* regelmæssigt revurdere liste fra Veitari over Veitaribrugere i Kundi systemer
* regelmæssigt sikre, at konti m.m., der anvendes af leverandører til fjernadgang, kun er aktive i den påkrævede periode

**9.2.6 Inddragelse eller justering af adgangsrettigheder**

* Alle eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter bør inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.

### 9.3 Brugernes ansvar

Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.

**9.3.1 Brug af hemmelig autentifikationsinformation**

* Det bør være et krav, at brugere følger Kundi praksis ved anvendelse af hemmelig

 autentifikationsinformation

### 9.4 Styring af system- og applikationsadgang

Formålet er at forhindre uautoriseret adgang til systemer og applikationer.

**9.4.2 Procedurer for sikker log-on**

* Der bør forefindes en sikker log-on procedure
* fastlægge og styre adgangskontrolkravene, herunder autoriseringsprocesser og bruger-ID'er og passwordregler til applikationer og systemer, som administreres af Kundi og informere Veitari om ændringer
* Behandle forespørgsler til password politikker fra Veitari

**9.4.3 System for administration af adgangskoder**

* Systemer til administration af adgangskoder bør være interaktive og bør sikre, at koderne er af høj kvalitet

**9.4.4 Brug af privilegerede systemprogrammer**

* Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, bør begrænses og styres effektivt

**9.4.5 Styring af adgang til kildekoder til programmer**

* Adgang til kildekoder til programmer samt dokumentation bør begrænses.

# 10 Kryptografi

## Veitari ansvar

### 10.1 Kryptografiske kontroller

Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.

**10.1.1 Politik for anvendelse af kryptografi**

* Bliver kryptering benyttet til kritiske systemer, bør der udarbejdes og implementeres en politik for anvendelse af kryptografi

**10.1.2 Administration af nøgler**

* Bliver kryptering benyttet til kritiske systemer, bør der udarbejdes og implementeres en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.

## Kundi ansvar

### 10.1 Kryptografiske kontroller

Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.

**10.1.1 Politik for anvendelse af kryptografi**

* Bliver kryptering benyttet til kritiske systemer, bør der udarbejdes og implementeres en politik for anvendelse af kryptografi

**10.1.2 Administration af nøgler**

* Bliver kryptering benyttet til kritiske systemer, bør der udarbejdes og implementeres en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.

# 11 Fysisk sikkerhed

## Veitari ansvarsområde

### 11.1 Sikre områder

Formålet er at forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af Kundi information og informationsbehandlingsfaciliteter.

**11.1.1 Fysisk perimetersikring**

* Der bør defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.

**11.1.2 Fysisk adgangskontrol**

* Der bør være fysisk adgangskontrol til begrænsning af adgang, så kun autoriseret personale har adgang til sikrede områder
* Adgang til sikre områder bør registreres
* Veitari skal regelmæssigt levere Kundi sikkerhedsansvarlige en oversigt over hvem har adgang til Veitari datacentre

**11.1.3 Sikring af kontorer, lokaler og faciliteter**

* Fysisk sikring af kontorer, lokaler og faciliteter bør tilrettelægges og etableres.

**11.1.4 Beskyttelse mod eksterne og miljømæssige trusler**

* Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker bør tilrettelægges og etableres.

**11.1.5 Arbejde i sikre områder**

* Procedurer for arbejde i sikre områder bør tilrettelægges og etableres.

**11.1.6 Områder til af- og pålæsning**

* Adgangssteder som fx områder til af- og pålæsning og andre steder, hvor uautoriserede personer kan komme ind på området, bør kontrolleres og så vidt muligt adskilles fra informationsbehandlingsfaciliteter for at undgå uautoriseret adgang.

### 11.2 Udstyr

Formålet er at undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse på Veitari

**11.2.1 Placering og beskyttelse af udstyr**

* Udstyr bør placeres og beskyttes, således at risikoen for miljøtrusler og farer samt muligheden for uautoriseret adgang nedsættes.
* overholde krav til fysisk og forsyningsmæssig sikkerhed, som står i forhold til Veitari betydning for Kundi aktiver på Veitari
* foretage periodiske gennemgange af fysisk kontrollerede områder, for hvilke Veitari er ansvarlig for

**11.2.2 Understøttende forsyninger (forsyningssikkerhed)**

* Udstyr bør beskyttes mod strømsvigt og andre forstyrrelser (f.eks. høj temperatur) som følge af svigt af understøttende forsyninger

**11.2.3 Sikring af kabler**

* Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, bør beskyttes mod aflytning, interferens og skader.

**11.2.4 Vedligeholdelse af udstyr**

* Udstyr bør vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet.

**11.2.5 Fjernelse af aktiver**

* Udstyr, information og software bør ikke fjernes fra Veitari uden forudgående tilladelse.

**11.2.6 Sikring af udstyr og aktiver uden for Veitari lokaler**

* Der bør etableres sikring af aktiver uden for Veitari under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for Veitari lokaler.

**11.2.7 Sikker bortskaffelse eller genbrug af udstyr**

* Kundi forventer at lagringsmedier, som kan indeholde Kundi oplysninger, bliver bortskaffet på en sikker måde, f.eks. bør diske knuses, således at det er umuligt at genetablere oplysningerne, og vedrørende bånd bør der sikres, at de bliver brændt.
* Genbrug af lagringsmedier, som kan indeholde Kundi oplysninger, må kun foregå indenfor Veitari regi.

**11.2.8 Brugerudstyr uden opsyn**

* Brugere bør sikre, at udstyr, som er uden opsyn, er passende beskyttet f.eks. bør der logges af når man går fra skærmen og pauseskærm bør være aktiveret

**11.2.9 Politik for ryddeligt skrivebord og blank skærm**

* Kundi forventer, at medier, der kan indeholde Kundi fortrolige oplysninger ikke er frit tilgængelige for uvedkommende, f.eks. papir, diske, bånd, usb og oplysninger på skærmen

## Kundi ansvarsområder

### 11.1 Sikre områder

Formålet er at forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af Kundi information og informationsbehandlingsfaciliteter.

**11.1.2 Fysisk adgangskontrol**

* Regelmæssigt gennemgå en oversigt over hvem har adgang til Veitari datacentre
* Tilvejebringe og styre den fysiske sikkerhedsinfrastruktur og de fysiske sikkerheds­kontroller på Kundi egne lokationer

### 11.2 Udstyr

Formålet er at undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.

**11.2.3 Sikring af kabler**

* Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, bør beskyttes mod aflytning, interferens og skader.

**11.2.7 Sikker bortskaffelse eller genbrug af udstyr**

* Veitari forventer at lagringsmedier, som kan indeholde Veitari oplysninger, bliver bortskaffet på en sikker måde, f.eks. bør diske knuses, således at det er umuligt at genetablere oplysningerne, og vedrørende bånd bør der sikres, at de bliver brændt.
* Genbrug af lagringsmedier, som kan indeholde Veitari oplysninger, må kun foregå indenfor Kundi regi.

**11.2.9 Politik for ryddeligt skrivebord og blank skærm**

* Veitari forventer, at medier, der kan indeholde Veitari fortrolige oplysninger ikke er frit tilgængelige for uvedkommende, f.eks. pappir, diske, bånd, usb og oplysninger på skærmen

# 12 Driftssikkerhed

## Veitari ansvarsområder

###

### 12.1 Driftsprocedurer og ansvarsområder

Formålet er at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

**12.1.1 Dokumenterede driftsprocedurer**

* At udarbejde og vedligeholde passende dokumentation for opsætning og driftsprocedurer, eksempelvis i driftshåndbøger for de systemer, Veitari er ansvarlig for
* at sikre, at al systemdokumentation til enhver tid er opbevaret således, at sandsynligheden for at denne skulle gå tabt eller komme uvedkommende i hænde, er på et kendt og accepteret niveau

**12.1.2 Ændringsstyring**

* Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, bør styres
* alle ændringer bør følge en godkendt change management-proces, herunder ændringer i det fysiske eller forsyningsmæssige miljø, der direkte eller indirekte kan have betydning for Kundi drift
* sikre, at alle ændringer som kan påvirke Kundi driftsstabilitet og netværkssikkerhed følger en change management-proces der som minimum bør blandt andet indeholde:
* en beskrivelse af formålet med ændringen
* angivelse af hvad og hvornår ændringen ønskes gennemført
* en vurdering af risikoen for driftsstabiliteten ved at gennemføre ændringen
* en vurdering af påvirkningen af ændringen på systemets svartider
* en realistisk fallback plan, inkl. kriterierne for at aktivere planen
* ændringer foreslået af Veitari bør gennemgås og godkendes af autoriseret person hos Kundi
* ændringer foreslået af Kundi bør procesmæssigt administreres af Veitari fra anmodning til implemen­tering
* alle ændringer, som skal implementeres uden for de aftalte servicevinduer, bør have en særskilt godkendelse fra Kundi
* gældende for operativsystemer, softwareværktøjer og systemer til netværksinfrastruktur under Veitari administration, bør der i serveroversigten dokumenteres på hvilke servere og hvilke systemer sikkerhedspatches skal implementeres og frekvens
* grundet strenge licensforhold skal Veitari være særlig opmærksom på, om en ændring kan påvirke Kundi licensforhold. Ved tvivlsspørgsmål skal Kundi altid involveres. Kundi licensforhold skal være beskrevet

**12.1.3 Kapacitetsstyring**

* foretage den fornødne overvågning af kapacitetsforbrug på systemer og infrastruktur således at kapacitetsproblemer konstateres rettidigt og driftsafbrydelser og performancedegraderinger dermed kan imødegås. Veitari bør på eget initiativ foreslå passende handlinger for at undgå ovennævnte

**12.1.4 Adskillelse af udviklings/test- og driftsmiljøer**

* Udviklings/test- og driftsmiljøer bør adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.
* testdata, klassificeret som fortrolige og hemmelige, bør sikres:
* kun autoriseret testpersonale må have adgang til testdata
* testpersonale bør være underlagt en tavshedserklæring
* adgangsstyring i test bør være på same niveau som i produktion

### 12.2 Malwarebeskyttelse

Formålet er at sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

**12.2.1 Kontroller mod malware**

* Der bør implementeres kontroller til detektering, forhindring og gendannelse med henblik på at beskytte mod malware, kombineret med passende brugerbevidsthed.
* installation af anti-malware software, signaturopdatering - når disse er tilgængelige - af alle servere i Kundi miljø og eventuelle arbejdsstationer, der benyttes til administration. Af f. eks. performance hensyn, vil der muligvis være fravalg, som skal dokumenteres
* gennemscanning for skadelig kode, f.eks. virus og andet malware ved hver fil-tilgang og gennemscanning af diske mindst hver måned. Undtagelser (f.eks. af performancehensyn) skal dokumenteres og godkendes af Kundi som dispensation
* inden brug scanne filer, som modtages over netværk eller via anden form for lagingsmedie, for malware
* under eventuelt angreb:
	+ rimelig reaktionstid på angreb og igangsætning af korrigerende handlinger.
	+ systemer der er inficeret med malware, skal fjernes fra Kundi netværk hurtigst muligt
	+ hurtigst muligt at informere Kundi om skadens omfang
	+ planlægge genetablering/genoprettelse
	+ løbende orientering til Kundi

### 12.3 Backup

Formålet er at beskytte mod tab af data

**12.3.1 Backup af information**

* udføre backup af operativsystemer og infrastruktursoftware ifølge bilag 4.
* udføre backup af data som foreskrevet af Kundi i den til enhver tid opdaterede serveroversigt og bilag 4 til hovedaftalen

* efterse backup rapport regelmæssigt, for at sikre at de foreskrevne backup rutiner beskrevet i bilag 4 overholdes og foretage nødvendige korrektioner og forebyggende tiltag
* foretage regelmæssige genetableringstests ud fra det spejlede miljø på alle udvalgte systemer inklusive data efter en med Kundi aftalt plan
* på anmodning at tilvejebringe rapporter vedrørende gennemførsel af genetableringstester
* at håndtere backupmedia herunder:
* vedligeholde en oversigt over backupmedier
* opbevare og beskytte lagringsmedier i overensstemmelse med informationsklassifikation (inkl. implementering af kryptering, hvis det foreskrives af Kundi retningslinjer for klassifikation)

### 12.4 Logning og overvågning

Formålet er at registrere hændelser og tilvejebringe bevis.

**12.4.1 Hændelseslogning**

* som minimum bør logges:
* brugerid’er
* logon og logoff samt handlinger, der kræver privilegeret adgang
* kritiske driftsaktiviteter (opsætningsændringer, ændringer i parametre filer m.m.) og sikkerhedshændelser
* alle fejl herunder uautoriseret forsøg på at få adgang
* aktiviteter på system og databaser
* logs bør gemmes sikkert
* logs bør gennemgås regelmæssigt manuelt eller automatisk for at identificere mistænkelig aktivitet
* der bør være aftalt, hvor længe logs skal gemmes
* udlevere logs til Kundi efter ønske

**12.4.2 Beskyttelse af log-oplysninger**

* Logningsfaciliteter og log-oplysninger bør beskyttes mod manipulation og uautoriseret adgang.

**12.4.3 Administrator- og operatørlogge**

* Aktiviteter udført af systemadministrator og systemoperatør bør logges, og loggene bør beskyttes og gennemgås regelmæssigt.

**12.4.4 Tidssynkronisering**

* Urene i alle relevante informationsbehandlingssystemer eller et sikkerhedsdomæne bør være synkroniseret til en enkelt referencetidsangivelseskilde.

### 12.5 Styring af driftssoftware

Formålet er at sikre integriteten af driftssystemer.

**12.5.1 Softwareinstallation i driftssystemer**

* Der bør implementeres procedurer til styring af softwareændringer i driftssystemer.
* Hvis Kundi systemer og/eller data berøres, bør Kundi involveres
* servere skal være hærdet, hvor det er muligt
* sammen med Kundi at definere et servicevindue til brug ved implementering af security patches
* få Kundi godkendelse, hvis sikkerhedsændringer skal udføres uden for de aftalte servicevinduer
* i god tid informere Kundi om planlagte security patches

### 12.6 Sårbarhedsstyring

Formålet er at forhindre, at sårbarheder udnyttes.

**12.6.1 Styring af sårbarheder**

* Sammen med sikkerhedslederen på Kundi, har sikkerhedslederen på Veitari ansvaret for, at der løbende indhentes informationer om sårbarheder.
Kundi og Veitari eksponering for sådanne sårbarheder bør evalueres, og der bør iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.

**12.6.2 Begrænsninger på softwareinstallation**

* Der bør være regler om, at kun kvalificerede personer kan installere software, og at disse installationer skal være behørigt godkendt.

### 12.7 Overvejelser i forbindelse med audit af informationssystemer

Formålet er at minimere virkningen af auditaktiviteter på driftssystemer.

**12.7.1 Kontroller i forbindelse med audit af informationssystemer**

* Hvis auditkrav og -aktiviteter, der indebærer verifikation af driftssystemer kan påvirke Kundi, skal dette planlægges og aftales omhyggeligt med Kundi for at minimere risikoen for afbrydelse af forretningsprocesserne.

## Kundi ansvarsområder

### 12.1 Driftsprocedurer og ansvarsområder

Formålet er at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

**12.1.1 Dokumenterede driftsprocedurer**

* udarbejde og vedligeholde passende dokumentation for opsætning og driftsprocedurer, eksempelvis i driftshåndbøger for de systemer, Kundi er ansvarlig for at udarbejde driftsdokumentation til
* sikre, at al systemdokumentation til enhver tid er opbevaret således, at sandsynligheden for at denne skulle gå tabt eller komme uvedkommende i hænde, er på et kendt og accepteret niveau
* godkende Veitari system- og driftsdokumentation

**12.1.2 Ændringsstyring**

* sikre, at alle ændringer som kan påvirke Veitari driftsstabilitet og netværkssikkerhed følger en change management-proces der som minimum bør indeholde:
* en beskrivelse af formålet med ændringen
* angivelse af hvad og hvornår ændringen ønskes gennemført
* en vurdering af risikoen for driftsstabiliteten ved at gennemføre ændringen
* en vurdering af påvirkningen af ændringen på systemets svartider
* en realistisk fallback plan, inkl. kriterierne for at aktivere planen

derudover bør
* Veitari have mulighed for at gøre bemærkninger til planlagde ændringer foreslået af Kundi
* alle ændringer, som skal implementeres uden for de aftalte servicevinduer, have en særskilt godkendelse fra Veitari
* gennemgå og godkende ændringsanmodninger fra Veitari
* grundet strenge licensforhold skal Kundi være særlig opmærksom på, om en ændring kan påvirke Kundi licensforhold.

**12.1.3 Kapacitetsstyring**

* sikre, at Veitari foretager den fornødne overvågning af kapacitetsforbrug på systemer og infrastruktur

**12.1.4 Adskillelse af udviklings/test- og driftsmiljøer**

* testdata, klassificeret som fortrolige og hemmelige, bør sikres:
* kun autoriseret testpersonale må have adgang til testdata
* testpersonale bør være underlagt en tavshedserklæring
* adgangsstyring i test bør være på samme niveau som i produktion
* Kundi systemer bør være logisk adskilt fra andre kunders systemer.

### 12.2 Malwarebeskyttelse

Formålet er at sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

**12.2.1 Kontroller mod malware**

* Der bør implementeres kontroller til detektering, forhindring og gendannelse med henblik på at beskytte mod malware, kombineret med passende brugerbevidsthed.
* installation af anti-malware software, signaturopdatering - når disse er tilgængelige - af alle arbejdstationer i Kundi miljø
* gennemscanning for skadelig kode, f.eks. virus og andet malware ved hver fil-tilgang og gennemscanning af diske mindst hver måned.
* inden brug scanne filer, som modtages over netværk eller via anden form for lagringsmedie, for malware
* under eventuelt angreb:
	+ rimelig reaktionstid på angreb og igangsætning af korrigerende handlinger.
	+ systemer der er inficeret med malware, skal fjernes fra Kundi netværk hurtigst muligt
	+ hurtigst muligt at informere Veitari om skadens omfang
	+ løbende orientering til Veitari

### 12.3 Backup

Formålet er at beskytte mod tab af data

**12.3.1 Backup af information**

* definere krav til backup, spejling, restore og genetableringsprocedurer for specifikke systemer og servere, inklusive data
* regelmæssigt sammen med Veitari at gennemgå backuprutiner
* sikre at der bliver foretaget regelmæssige genetableringstests ud fra det spejlede miljø på alle udvalgte systemer inklusive data, samt at der regelmæssigt bliver restoret en udvalgt fil fra backup

### 12.4 Logning og overvågning

Formålet er at registrere hændelser og tilvejebringe bevis.

**12.4.1 Hændelseslogning**

* på anmodning at samarbejde med Veitari om opsamling af logs

### 12.5 Styring af driftssoftware

Formålet er at sikre integriteten af driftssystemer.

**12.5.1 Softwareinstallation i driftssystemer**

* sammen med Veitari at definere et servicevindue til brug ved implementering af security patches
* godkende, hvis sikkerhedsændringer skal udføres uden for de aftalte servicevinduer
* godkende eller afvise ændringsanmodninger for security patches mindst en dag før planlagte implementeringsdato

### 12.6 Sårbarhedsstyring

Formålet er at forhindre, at sårbarheder udnyttes.

**12.6.1 Styring af sårbarheder**

* Sammen med sikkerhedslederen på Veitari, har sikkerhedslederen på Kundi ansvaret for, at der løbende indhentes informationer om sårbarheder i anvendte systemer.

Kundi og Veitari eksponering for sådanne sårbarheder bør evalueres, og der bør iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.

### 12.7 Overvejelser i forbindelse med audit af informationssystemer

Formålet er at minimere virkningen af auditaktiviteter på driftssystemer.

**12.7.1 Kontroller i forbindelse med audit af informationssystemer**

* Hvis auditkrav og -aktiviteter, der indebærer verifikation af driftssystemer kan påvirke Veitari, skal dette planlægges og aftales omhyggeligt med Veitari for at minimere risikoen for afbrydelse af forretningsprocesserne.

# 13 Kommunikationssikkerhed

## Veitari ansvarsområder

### 13.1 Styring af netværkssikkerhed

Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

**13.1.1 Netværksstyring**

* Netværk bør styres og kontrolleres for at beskytte informationer i systemer og applikationer.
* styre Veitari netværkskomponenter anvendt i forbindelse med Kundi infrastruktur og netværk herunder:
* etablere procedurer for logfiler, alarmering f.eks. IPS og rapportering i forbindelse med brud på netværkssikkerheden
* styre og vedligeholde firewalls, routere og gateways, der har forbindelse med Kundi miljø
* udøve aktiviteter med henblik på styring af netværkssikkerhed for den del der er under Veitari ansvarsområde, herunder:
* styre og drifte Kundi netværkskomponenter som gateways og firewalls
* konfigurere netværksinfrastrukturen i henhold til ændringsanmodninger og med hensyn til netværkets betydning
* ændring i opsætning af firewalls, applikationer og netværk, der kan påvirke Kundi systemer, må kun ske hvis den er godkendt af Kundi

**13.1.2 Sikring af netværkstjenester**

* Sikkerhedsmekanismer, serviceniveauer og styringskrav i relation til alle netværkstjenester bør identificeres og indgå i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede.

**13.1.3 Opdeling i netværk**

* Grupper af informationstjenester, brugere og informationssystemer bør opdeles i netværk efter anmodning fra Kundi
* efter anmodning fra Kundi at identificere alle eksisterende fjernadgange hos Veitari (såsom dial-in, VPN, etc) og samarbejde med Kundi om eventuelle ændringer

### 13.2 Informationsoverførsel

Formålet er at opretholde informationssikkerhed ved overførsel internt og til en ekstern entitet.

**13.2.1 Politikker og procedurer for informationsoverførsel**

* Der bør foreligge formelle overførselspolitikker, -procedurer og -kontroller for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.
* al overførsel af fortrolige data via åbne og offentligt tilgængelige netværk (såsom internet, telefonlinjer og lignende), bør foregå på en sikker vis f.eks. krypteret

**13.2.2 Aftaler om informationsoverførsel**

* Aftaler bør omhandle sikker overførsel af forretningsinformation mellem Veitari og eksterne parter.

**13.2.3 Veitariiske meddelelser**

* Fortrolige oplysninger bør ikke sendes ubeskyttet veitariisk

**13.2.4 Fortroligheds- og hemmeligholdelsesaftaler**

* Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler behov for at beskytte information, bør identificeres, gennemgås regelmæssigt og dokumenteres f.eks.:
	+ nødvendige handlinger, når aftalen udløber
	+ retten til at auditere
	+ betingelser for returnering eller destruktion af information ved aftalens ophør
	+ forventede handlinger, der skal iværksættes i tilfælde af aftalebrud

## Kundi ansvarsområder

### 13.1 Styring af netværkssikkerhed

Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

**13.1.1 Netværksstyring**

* give Veitari tilstrækkelig information til at definere firewallregler
* udøve aktiviteter med henblik på styring af netværkssikkerhed for den del der er under Kundi ansvarsområde, herunder:
* styre og drifte Kundi netværkskomponenter som gateways og firewalls
* konfigurere netværksinfrastrukturen i henhold til ændringsanmodninger og med hensyn til netværkets betydning

**13.1.2 Sikring af netværkstjenester**

* Sikkerhedsmekanismer, serviceniveauer og styringskrav i relation til alle netværkstjenester bør identificeres og indgå i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede.

### 13.2 Informationsoverførsel

Formålet er at opretholde informationssikkerhed ved overførsel internt og til en ekstern entitet.

**13.2.1 Politikker og procedurer for informationsoverførsel**

* Der bør foreligge formelle overførselspolitikker, -procedurer og -kontroller for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.
* al overførsel af fortrolige data via åbne og offentligt tilgængelige netværk (såsom internet, telefonlinjer og lignende), bør foregå på en sikker vis f.eks. krypteret

**13.2.2 Aftaler om informationsoverførsel**

* Aftaler bør omhandle sikker overførsel af forretningsinformation mellem Kundi og eksterne parter.

**13.2.3 Veitariiske meddelelser**

* Fortrolige oplysninger bør ikke sendes ubeskyttet veitariisk

**13.2.4 Fortroligheds- og hemmeligholdelsesaftaler**

* Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler behov for at beskytte information, bør identificeres, gennemgås regelmæssigt og dokumenteres f.eks.:
* nødvendige handlinger, når aftalen udløber
* retten til at auditere
* betingelser for returnering eller destruktion af information ved aftalens ophør
* forventede handlinger, der skal iværksættes i tilfælde af aftalebrud

#  14 Anskaffelse, udvikling og vedligeholdelse af systemer

## Veitari ansvarsområder

### 14.1 Sikkerhedskrav til informationssystemer

Formålet er at sikre, at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

**14.1.1 Analyse og specifikation af informationssikkerhedskrav**

* Informationssikkerhedsrelaterede krav bør være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.

**14.1.2 Sikring af applikationstjenester på offentlige netværk**

* Informationer i forbindelse med applikationstjenester over offentlige netværk bør beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring.

**14.1.3 Beskyttelse af handelsapplikationer og –tjenester**

* Informationer i forbindelse med handelsapplikationer og -tjenester bør beskyttes for at forhindre ufuldstændig transmission, fejlforsendelser, uautoriseret ændring af meddelelser, uautoriseret offentliggørelse, uautoriseret kopiering eller retransmission af meddelelser.

### 14.2 Sikkerhed i udviklings- og hjælpeprocesser

Formålet er at sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.

**14.2.1 Sikker udviklingspolitik**

* Der bør fastlægges og anvendes regler for udvikling af software og systemer i organisationen.
* nye systemer bør opfylde Veitari samlede sikkerhedskrav

**14.2.2 Procedurer for styring af systemændringer**

* Ændringer af systemer inden for udviklingslivscyklussen bør styres ved hjælp af formelle procedurer for ændringsstyring.

**14.2.3 Teknisk gennemgang af applikationer efter ændringer af driftsplatforme**

* Ved ændring af driftsplatforme bør forretningskritiske applikationer gennemgås og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed.

**14.2.4 Begrænsning af ændringer**

* Ændringer i systemer bør vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer bør styres effektivt.

**14.2.5 Principper for udvikling af sikre systemer**

* Principper for udvikling af sikre systemer bør fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med implementering af informationssystemer (udviklingsmodel).

**14.2.6 Sikkert udviklingsmiljø**

* Der bør være etableret sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus.

**14.2.7 Outsourcet udvikling**

* Veitari skal acceptere at Kundi fører tilsyn med og overvåger systemudviklingsaktiviteter

**14.2.8 Systemsikkerhedstest**

* Test af sikkerhedsfunktionalitet bør udføres ved udvikling.

**14.2.9 Systemgodkendelsestest**

* Der bør være aftalt, hvordan tester skal foregå.

### 14.3 Testdata

Formålet er at sikre beskyttelse af data, som anvendes til test.

**14.3.1 Sikring af testdata**

Testdata bør udvælges omhyggeligt og beskyttes og kontrolleres.

## Kundi ansvarsområder

### 14.1 Sikkerhedskrav til informationssystemer

Formålet er at sikre, at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

**14.1.1 Analyse og specifikation af informationssikkerhedskrav**

* Informationssikkerhedsrelaterede krav bør være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.

**14.1.2 Sikring af applikationstjenester på offentlige netværk**

* Informationer i forbindelse med applikationstjenester over offentlige netværk bør beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring.

**14.1.3 Beskyttelse af handelsapplikationer og –tjenester**

* Informationer i forbindelse med handelsapplikationer og -tjenester bør beskyttes for at forhindre ufuldstændig transmission, fejlforsendelser, uautoriseret ændring af meddelelser, uautoriseret offentliggørelse, uautoriseret kopiering eller retransmission af meddelelser.

### 14.2 Sikkerhed i udviklings- og hjælpeprocesser

Formålet er at sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.

**14.2.4 Begrænsning af ændringer**

* Ændringer i systemer bør vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer bør styres effektivt.

**14.2.5 Principper for udvikling af sikre systemer**

* Principper for udvikling af sikre systemer bør fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med implementering af informationssystemer (udviklingsmodel).
* sikre at sikkerhedskravene bliver adresseret ved systemanskaffelse og krav­specifikationer adresseret ved systemudvikling

**14.2.8 Systemsikkerhedstest**

* Test af sikkerhedsfunktionalitet bør udføres ved udvikling.

**14.2.9 Systemgodkendelsestest**

* Der bør være aftalt, hvordan tester skal foregå.

### 14.3 Testdata

Formålet er at sikre beskyttelse af data, som anvendes til test.

**14.3.1 Sikring af testdata**

* Testdata bør udvælges omhyggeligt og beskyttes og kontrolleres.

# 15 Leverandørforhold

## Veitari ansvarsområde

### 15.1 Informationssikkerhed i leverandørforhold

Formålet er at sikre beskyttelse af Kundi aktiver, som leverandører har adgang til.

**15.1.1 Informationssikkerhedspolitik for leverandørforhold**

* Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til Kundi aktiver bør aftales med Kundi og dokumenteres.

**15.1.2 Håndtering af sikkerhed i leverandøraftaler**

* Alle relevante informationssikkerhedskrav bør fastlægges og aftales med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til Kundi information.

**15.1.3 Forsyningskæde for informations- og kommunikationsteknologi (IKT)**

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

### 15.2 Styring af leverandørydelser

Formålet er at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til

leverandøraftalerne.

**15.2.1 Overvågning og gennemgang af leverandørydelser**

* Veitari bør regelmæssigt have mulighed for at overvåge, gennemgå og auditere leverandørers ydelser med hensyn til Kundi

**15.2.2 Styring af ændringer af leverandørydelser**

* Ændringer af leverandørers ydelser til Veitari med hensyn til Kundi, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, -procedurer og -kontroller, bør styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer, -systemer og -processer er, og til en revurdering af risici.

## Kundi ansvarsområde

### 15.1 Informationssikkerhed i leverandørforhold

Formålet er at sikre beskyttelse af Kundi aktiver, som leverandører har adgang til.

**15.1.1 Informationssikkerhedspolitik for leverandørforhold**

* Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til Kundi aktiver bør aftales mellem Veitari og Kundi og dokumenteres.

### 15.2 Styring af leverandørydelser

Formålet er at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til

leverandøraftalerne.

**15.2.1 Overvågning og gennemgang af leverandørydelser**

* Kundi bør regelmæssigt overvåge, gennemgå og auditere Veitari ydelser til Kundi

# 16 Styring af informationssikkerhedsbrud

## Veitari ansvarsområder

### 16.1 Styring af informationssikkerhedsbrud og forbedringer

Formålet er at sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder

kommunikation om sikkerhedshændelser og -svagheder.

**16.1.1 Ansvar og procedurer**

* Ledelsesansvar og procedurer bør fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.
* Procedurerne bør blandt andet indeholde krav om at identificere, logge, spore, afhjælpe, kommunikere og eskalere sikker­heds­hændelser

**16.1.2 Rapportering af informationssikkerhedshændelser**

* i tilfælde af et alvorligt brud på sikkerheden, skal Veitari straks iværksætte afhjælpende handlinger og straks informere Kundi sikkerhedsansvarlige om hændelsen
* hurtigst muligt informere Kundi om enhver identificeret hændelse ved Kundi systemer varetaget af Veitari eller hændelser, der kan påvirke Kundi systemer og anbefale mulige forebyggende og afhjælpende handlinger

**16.1.3 Rapportering af informationssikkerhedssvagheder**

* Medarbejdere på Veitari og konsulenter, som Veitari måtte anvende og som bruger Kundi systemer og -tjenester, bør have pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i informationssystemer og -tjenester.

**16.1.4 Vurdering af og beslutning om informationssikkerhedshændelser**

* Informationssikkerhedshændelser bør vurderes, og det bør besluttes, om de skal klassificeres som informationssikkerhedsbrud.
* assistere Kundi med indledende vurdering af hændelsen, herunder tildeling af prioritet og ejerskab
* assistere Kundi med at definere sikkerhedshændelsers prioriteringsniveauer og til­hø­ren­de eskaleringsprocedurer
* tage beslutninger om handlinger til at løse sikkerhedshændelser der kan påvirke Kundi, det være sig Veitari netværk, Veitari system, Veitari personale eller Veitari data, herunder passende indsamling af beviser

**16.1.5 Håndtering af informationssikkerhedsbrud**

* Informationssikkerhedsbrud bør håndteres i overensstemmelse med de dokumenterede procedurer.
* undersøge it-sikkerhedsbrud og indsamle beviser ved at levere teknisk infor­ma­tion i relation til it-sikkerhedsbrud og assistere Kundi med informationsanalyse og problemidentifikation

**16.1.6 Erfaring fra informationssikkerhedsbrud**

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

**16.1.7 Indsamling af beviser**

* Veitari bør definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som beviser.
* Sammen med Kundi prioritere sikkerhedshændelser efter systemernes vigtighed og hændelsens konsekvens indenfor følgende kategorier:

Høj
Der er risiko for datatab eller større og længerevarende driftsstop på væsentlige systemer og/eller der er risiko for kompromittering af persondata eller højt klassificerede data.

Medium
Der er risiko for væsentlige driftsforstyrrelser og/eller kompromittering af medium klassificerede data

Lav
Der er risiko for driftsforstyrrelser for enkelte brugere og sekundære systemer. Der er ingen risiko for permanent tab eller kompromittering af data.

* sikre at medium og højt prioriterede sikkerhedshændelser efterfølgende bliver rapporteret skriftligt, og at problemanalyse og plan for fremtidig imødegåelse, tilsvarende bliver rapporteret til Kundi på førstkommende SLA møde

## Kundi ansvarsområder

### 16.1 Styring af informationssikkerhedsbrud og forbedringer

Formålet er at sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder

kommunikation om sikkerhedshændelser og -svagheder.

**16.1.1 Ansvar og procedurer**

* Ledelsesansvar og procedurer bør fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.
* Procedurerne bør blandt andet indeholde krav om at identificere, logge, spore, afhjælpe, kommunikere og eskalere sikker­heds­hændelser

**16.1.2 Rapportering af informationssikkerhedshændelser**

* i tilfælde af et alvorligt brud på sikkerheden, som kan påvirke Veitari, skal Kundi straks iværksætte afhjælpende handlinger og straks informere Veitari sikkerhedsansvarlige om hændelsen
* hurtigst muligt informere Veitari om enhver identificeret hændelse som kan påvirke Veitari

**16.1.4 Vurdering af og beslutning om informationssikkerhedshændelser**

* Informationssikkerhedshændelser bør vurderes, og det bør besluttes, om de skal klassificeres som informationssikkerhedsbrud.
* Kundi bør assistere Veitari i håndtering af sikkerhedshændelser

**16.1.5 Håndtering af informationssikkerhedsbrud**

* Informationssikkerhedsbrud bør håndteres i overensstemmelse med de dokumenterede procedurer.
* Kundi bør assistere Veitari i håndtering af sikkerhedsbrud

**16.1.6 Erfaring fra informationssikkerhedsbrud**

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

**16.1.7 Indsamling af beviser**

* Kundi bør definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som beviser.
* Sammen med Veitari prioritere sikkerhedshændelser efter systemernes vigtighed og hændelsens konsekvens indenfor følgende kategorier:

Høj
Der er risiko for datatab eller større og længerevarende driftsstop på væsentlige systemer og/eller der er risiko for kompromittering af persondata eller højt klassificerede data.

Medium
Der er risiko for væsentlige driftsforstyrrelser og/eller kompromittering af medium klassificerede data

Lav
Der er risiko for driftsforstyrrelser for enkelte brugere og sekundære systemer. Der er ingen risiko for permanent tab eller kompromittering af data.

* være ansvarlig for at beslutte, om en sikkerhedshændelse har resulteret i kompromittering af personfølsomme eller fortrolige oplysninger
* om nødvendigt forestå dialog med eksterne enheder såsom juridiske eller regulerende organer

# 17 Informationssikkerhedsaspekter ved nød-, beredskabs- og

#  reetableringsstyring

## Veitari ansvarsområder

### 17.1 Informationssikkerhedskontinuitet

Formålet er at informationssikkerhedskontinuiteten bør være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

**17.1.1 Planlægning af informationssikkerhedskontinuitet**

* Veitari bør fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.
* vedligeholde et beredskab såvel teknisk som organisatorisk, der i tilfælde af en katastrofesituation sikrer at den maksimale nedetid for de kritiske systemer bliver overholdt. De kritiske systemer er oplyst i klassificationsmatrixen bilag 3.
Med arbejdsdøgn forstås de døgn hvor Kundi er på arbejde, dvs. at fridage ikke tæller med.
Detaljerne om de enkelte klassificationskrav ses i ‘Flokkingarásetingar’, som er vedhæftet klassificationsmatrixen.
* sikre, at Kundi har en kontaktperson i Veitari beredskabsgruppe, som har løbende kontakt med Kundi
* efter anmodning at være Kundi behjælpelig i en beredskabssituation

**17.1.2 Implementering af informationssikkerhedskontinuitet**

* Veitari bør fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.
* sikre, at medarbejdere med roller i krisestaben kender deres opgaver og ansvar
* straks meddele Kundi om enhver situation, som Veitari mener, repræsenterer en katastrofe eller kan udvikle sig som en sådan
* meddele Kundi om alle ændringer til driftsmiljøet udført af Veitari, som kan/vil påvirke beredskabsplanen

	+ 1. **Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten**

Veitari bør

* verificere de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.
* anvende og teste funktionalitet og driftsprocedurer i beredskabsplanen regelmæssigt, herunder at teste beredskabsledelsernes kommunikationsevner
* deltage i Kundi planlægning af de årlige beredskabsplansaktiviteter
* Veitari bør bistå og indgå i Kundi test af beredskabet
* udføre aktivitet i forbindelse med de årlige revurderinger og katastrofeberedskabstest som er Veitari ansvar og fastlagt i en plan
* levere dokumentation af resultater fra aktiviteterne i forbindelse med test af katastrofeberedskabet

### 17.2 Redundans

Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

**17.2.1 Tilgængelighed af informationsbehandlingsfaciliteter**

* Informationsbehandlingsfaciliteter bør implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.
* Veitari bør have backupdatacenter med nødvendige faciliteter.

## Kundi ansvarsområder

### 17.1 Informationssikkerhedskontinuitet

Formålet er at informationssikkerhedskontinuiteten bør være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

**17.1.1 Planlægning af informationssikkerhedskontinuitet**

* Kundi bør fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.
* sikre, at Veitari har en kontaktperson i Kundi beredskabsledelse, som har løbende kontakt med Veitari
* efter anmodning at være Veitari behjælpelig i en beredskabssituation
* være ansvarlig for at erklære en hændelse for en katastrofe
* være ansvarlig for beredskabet af Kundi serviceydelser, herunder vurdering, planlægning og vedligeholdelse
* udlevere en prioriteret liste til Veitari over systemer og applikationer, der skal være indeholdt i katastrofeberedskabsplanen og årligt revurdere og opdatere denne liste
* definere eventuelle særlige beredskabskrav ved specifikke systemer
* være bekendt med Veitari overordnede beredsskabsplan

**17.1.2 Implementering af informationssikkerhedskontinuitet**

* straks meddele Veitari om enhver situation, som Kundi mener, repræsenterer en katastrofe eller kan udvikle sig som en sådan

**17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten**

Kundi bør

* verificere de etablerede og implementerede kontroller vedrørende

informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.

* anvende og teste funktionalitet og driftsprocedurer i beredskabsplanen regelmæssigt, herunder at teste beredskabsledelsernes kommunikationsevner
* udføre aktivitet i forbindelse med de årlige revurderinger og katastrofeberedskabstest
* samarbejde med Veitari om den del som berører Kundi, herunder at udvælge og beskrive scenarier som grundlag for Veitari tekniske planer og beredskab
* sammen med Veitari udarbejde en årlig testplan til katastrofeberedskab og omfanget af testaktiviteter
* godkende dokumentationen for de årlige katastrofeberedskabstests

### 17.2 Redundans

Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

**17.2.1 Tilgængelighed af informationsbehandlingsfaciliteter**

* Oplyse Veitari om Kundi krav til redundans

# 18 Overensstemmelse

## Veitari ansvarsområder

### 18.1 Overensstemmelse med lov- og kontraktkrav

Formålet er at forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav.

**18.1.1 Identifikation af gældende lovgivning og kontraktkrav**

* Veitari bør overholde alle relevante lov-, myndigheds- og kontraktkrav.

**18.1.2 Immaterielle rettigheder**

* Der bør implementeres passende procedurer til at sikre, at der er overensstemmelse med lov-, myndigheds- og kontraktkrav i relation til immaterielle rettigheder og anvendelse af beskyttede softwareprodukter.

**18.1.3 Beskyttelse af registreringer**

* Registreringer bør beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overensstemmelse med lov-, myndigheds- og kontraktkrav samt forretningsmæssige krav.

**18.1.4 Privatlivets fred og beskyttelse af personoplysninger**

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

**18.1.5 Regulering af kryptografi**

* Kryptografi bør anvendes i overensstemmelse med alle relevante aftaler, love og forskrifter.

### 18.2 Gennemgang af informationssikkerhed

Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med Veitari politikker og procedurer.

**18.2.1 Uafhængig gennemgang af informationssikkerhed**

* Veitari metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) bør gennemgås uafhængigt og separat med planlagte mellemrum eller i tilfælde af væsentlige ændringer.
* anvise en kontaktperson i forhold til revision med ansvar for at koordinere de it-revisionsmæssige support­aktiviteter
* Veitari skal årligt ved Kundi anmodning, levere en revisionserklæring omkring Veitari sikkerhedsforhold, underskrevet af en statsautoriseret revisor.
Revisionserklæringen bør udtale sig om Veitari samlede data-, system- og driftssikkerhed efter gældende revisionsstandard.
* Kundi revisor, sikkerhedsrådgiver eller sikkerhedsleder, har fri adgang til at foretage varslet sikker­heds­revision/inspektion hos Veitari. Veitari skal i den forbindelse stille alle relevante informationer og logninger til rådighed for Kundi sikkerhedsgennemgang.
Alle sikkerhedsforhold vedrørende kontraktens opfyldelse kan undersøges i forbindelse hermed.
* udvikle og implementere handlingsplaner for observationer fundet under revision, som Veitari er ansvarlig for:
* lukke observationer hurtigst muligt efter aftale med Kundi
* rapportere lukning af anbefalinger til Kundi

**18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder**

* Veitari bør regelmæssigt undersøge, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.
* Der bør være aftalt hvor længe dokumentation, herunder beskrivelser, estimater, risikovurderinger, testresultater og godkendelser skal opbevares

**18.2.3 Undersøgelse af teknisk overensstemmelse**

* varsle og iværksætte periodiske sårbarhedsscanninger og penetrationstest af systemer under Veitari driftsansvar
* være Kundi behjælpelig med at udføre sårbarhedsscanninger og penetrationstester og sørge for ekstern penetrationtest af den del af Veitari miljø der kan påvirke Kundi miljø
* ved egen periodisk gennemgang at sikre, at opsætningen af det tekniske miljø overholder Kundi og Veitari tekniske og sikkerhedsmæssige krav og specifikationer.
* meddele Kundi om eventuelle mangler og sammen med Kundi udarbejde en plan for afhjælpning af disse

## Kundi ansvarsområder

### 18.1 Overensstemmelse med lov- og kontraktkrav

Formålet er at forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav.

**18.1.1 Identifikation af gældende lovgivning og kontraktkrav**

* identificere og tolke specifikke juridiske, regulerende og kontraktmæssige sikkerheds­krav, som gælder for Kundi og informere Veitari om ændrede krav
* gennemgå generelle juridiske og regulerende ændringer til sikkerhedskrav som er identificeret af Veitari

### 18.2 Gennemgang af informationssikkerhed

Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med Kundi politikker og procedurer.

**18.2.1 Uafhængig gennemgang af informationssikkerhed**

* I tilfælde af at Kundi revisor eller rådgiver vedrørende it-sikkerhed, ønsker at foretage sikker­heds­revision hos Veitari bør dette meddeles i god tid.
* Der bør laves en skriftlig aftale med Veitari uafhængige it-revisor vedrørende revision af generelle kontroller i Kundi miljø på Veitari. Derudover kan der laves særskilt aftale om revision af andre områder

**18.2.3 Undersøgelse af teknisk overensstemmelse**

* anmode Veitari om at iværksætte sårbarhedsscanninger og penetrationstest

* være Veitari behjælpelig med at udføre sårbarhedsscanninger og penetrationstester
* ved periodisk gennemgang at sikre, at opsætningen af det tekniske miljø overholder Kundi og Veitari tekniske og sikkerhedsmæssige krav og specifikationer.
* meddele Veitari om eventuelle mangler