Fylgiskjal V

**Trygdarkrøv til veitaran av skjalhaldskipan til undirvísingarverkið**

|  |  |  |
| --- | --- | --- |
| Trygdarkrøv grundað á ISO 27001 |  |  |
| Krøvini, ið veitarin skal lúka, eru merkt við **X** í teiginum **JA**. Krøv sum ikki eru viðkomandi, eru merkt við **X** í teiginum **N/A** (not applicable).  Ein partur av krøvunum snúgva seg um veitararan sjálvan og hvussu hesin skipar seg sum veitara, meðan onnur krøv eru knýtt til sjálva veitingina og skipanina, ið veitt verður. |  |  |
| **5. Informationssikkerhedspolitikker** | **Ja** | **N/A** |
|  |  |  |
| kunne fremvise en ledelsesgodkendt it-sikkerhedspolitik der er kommunikeret til relevante personer og som indeholder relevante krav i henhold til en anerkendt standard | X |  |
| IT-sikkerhedspolitikken børunderstøttes af emnespecifikke politikker | X |  |
| overholde krav og sikkerhedsregler som er fastlagt i lov om behandling af personoplysninger | X |  |
| placere et overordnet ansvar for leverandøren’s it-sikkerhed og it-sikkerhedspolitik | X |  |
| revidere leverandøren’s it-sikkerhedspolitik en gang om året og når væsentlige ændringer er i miljøet | X |  |
| gennemgå de samlede sikkerhedskrav (dette dokument, nye risici, lovkrav, krav fra standard, politikker m.m.) med UVS mindst en gang om året | X |  |
| gå i åben dialog med UVS, hvis denne anmoder om ændringer i leverandøren’s 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. | X |  |

Viðmerkingar:

|  |
| --- |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **6. Organisering af informationssikkerhed** | **Ja** | **N/A** |
|  |  |  |
| Opretholde en sikkerhedsorganisation   * Ansvarsområder bør angives til personer med tilstrækkelige kvalifikationer * anvise en kontaktperson med relevante sikkerhedskompetencer hos leverandøren 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 leverandøren inden for hovedkontraktens område * samarbejde med UVS vedrørende sikkerhedskrav og –hændelser * levere og koordinere nødvendige sikkerhedsressourcer i forbindelse med aftalen * sørge for sikkerhedsforanstaltninger, der beskytter UVS data og systemer i forhold til fortrolighed, integritet og tilgængelighed * tage fuldt ejerskab for alle krav til leverandøren og retningslinjer i dette bilag * give en skriftlig besvarelse på UVS forespørgsler omkring sikkerhedskontroller i UVS miljø * sikre at etablering af nye tekniske miljøer og platforme er i overensstemmelse med de samlede sikkerhedskrav * sikre at ændringer foretaget på leverandøren’s initiativ er overensstemmende med de samlede sikkerhedskrav | X |  |
| ***6.1.2 Funktionsadskillelse*** |  |  |
| Modstridende funktioner og ansvarsområder bør adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af leverandøren’s/UVS aktiver. | X |  |
| 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. UVS skal godkende undtagelser fra funktionsadskillelsen samt godkende opfølgende kontroller. | X |  |
| Leverandøren’s interne it-revisor må ikke være privilegeret bruger i UVS systemer | X |  |
| ingen person må gennem egne eller delte brugerkonti m.v. have fysisk og/eller logisk adgang til samtlige generationer af data | X |  |
| ***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 | X |  |
| som hovedregel skal en henvendelse til en myndighed, som kun involverer UVS systemer, gå via UVS. UVS skal informeres hurtigst muligt, hvis UVS systemer eller data er involveret | X |  |
| ***6.1.4 Kontakt med særlige interessegrupper*** |  |  |
| Der bør opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer | X |  |
| Leverandøren bør sammen med UVS 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 | X |  |
| bliver leverandøren bekendt med betydende ændring i trusselsbilledet skal dette uden unødigt ophold meddeles UVS | X |  |
| ***6.1.5 Informationssikkerhed ved projektstyring*** |  |  |
| Der bør være fokus på informationssikkerheden ved projektstyring, uanset projekttype | X |  |
| ***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 |  | X |
| Der bør sikres, at opbevaring på mobile enheder som f.eks. bærbare pc'ere, smartphones og øvrige media håndteres i overensstemmelse med UVS klassificering af data |  | X |
| ***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 | X |  |

Viðmerkingar:

|  |
| --- |
| 6.1.3: Hetta merkir her, at veitarin skal vita, hvørjir relevantir myndugleikar skulu kunnast, tá okkurt er áfatt |
| 6.1.4: ’særlige interessegrupper’ merkir her at halda seg dagførdan um kt-trygd t.d. við at fylgja við í tí, sum verður skrivað á netinum, luttaka í NC3 og øðrum ERFA bólkum, sum kanska koma |
| 6.2.1: Gingið verður útfrá at data hjá UVS kemur ikki at liggja á mobilum eindum hjá veitaranum. |
| 6.2.2: Meginreglan er, at VPN atgongd bert skal vera í Føroyum. Í serligum førum, kann atgongd verða loyvd uttanlands. UVS skal tá loyva hesum. |
|  |

|  |  |  |
| --- | --- | --- |
| **7. Medarbejdersikkerhed** | **Ja** | **N/A** |
|  |  |  |
| **7.1.1 Screening** |  |  |
| Ansættelse af nye medarbejdere bør foregå efter en fastlagt procedure | X |  |
| Der bør være en process for godkendelse af konsulenter | X |  |
| **7.1.2 Ansættelsesvilkår og -betingelser** |  |  |
| relevante medarbejdere på leverandøren bør være bekendt med og overholde leverandøren’s samlede sikkerhedskrav | X |  |
| personale, der kan komme til at arbejde i UVS miljø, bør påkræves en straffeattest uden forhold der er relevante for UVS 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 leverandøren at rekvirere straffeattest for værende medarbejdere | X |  |
| Leverandøren’s personale bør iagttage ubetinget tavshed med hensyn til oplysninger vedrørende UVS eller andres forhold, som kommer til deres kendskab i forbindelse med de i denne kontrakt omhandlede leverancer, tjenesteydelser m.v. leverandøren’s personale bør acceptere dette ved at underskrive en generel tavshedserklæring | X |  |
| ansatte ved leverandøren’s underleverandører bør underskrive personlige tavshedserklæringer før de gives adgang til UVS udstyr og informationer eller bør en skriftlig aftale med underleverandøren bekræfte de ansattes tavshedspligt | X |  |
| **7.2.1 Ledelsesansvar** |  |  |
| Medarbejdere bør være grundigt orienteret om deres roller og ansvarsområder | X |  |
| Der bør sikres, at medarbejderne fortsat har de nødvendige kvalifikationer og undervises med jævne mellemrum | X |  |
| **7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed** |  |  |
| Der bør sørges for at medarbejdere, der direkte eller indirekte arbejder i UVS miljø, deltager i awareness programmer, og er bekendt med leverandøren’s sikkerhedsprocedurer og særlige sikkerhedskrav, som måtte være gældende for UVS systemer | X |  |
| Der bør sørges for at medarbejdere ved leverandøren’s eventuelle underleverandører, der arbejder direkte eller indirekte med UVS udstyr og informationer lever op til samme krav, som UVS stiller til leverandøren’s ansatte | X |  |
| **7.2.3 Sanktioner** |  |  |
| Der bør sørges for passende ledelsesmæssige sanktioner overfor leverandøren’s ansatte ved misbrug og/eller brud på sikkerhedsregler | X |  |
| Der bør sørges for passende sanktioner overfor leverandøren’s konsulenter ved misbrug og/eller brud på sikkerhedsregler | X |  |
| **7.3.1 Ansættelsesforholdets ophør eller ændring** |  |  |
| Der bør sørges for at adgang til UVS udstyr og informationer fjernes omgående når ansættelsesforholdet med leverandøren eller dennes underleverandører ophører | X |  |

Viðmerkingar:

|  |
| --- |
| 7.1.2: Kann verða trupult serliga í samband við størri feilir og t.d. tá MS skal inn. Stór virkir hava sum oftast sjálvi ein politikk um tagnarskyldu, tvs at starvsfólkini har hava longu undirskrivað tagnarskyldu, tá er ikki neyðugt aftur at undirskriva. |
| 7.2.2: Her meinast t.d. við relevant krøv úr starvsfólkaleiðreglunum hjá veitaranum |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **8. Styring af aktiver** | **Ja** | **N/A** |
|  |  |  |
| **8.1.1 Fortegnelse over aktiver** |  |  |
| Leverandøren bør have oversigt over egne aktiver i relation til UVS |  | X |
| **8.1.2 Ejerskab af aktiver** |  |  |
| Der bør udpeges en ansvarlig i organisationen for hvert aktiv i relation til UVS |  | X |
| **8.1.3 Accepteret brug af aktiver** |  |  |
| Aktiver, der indeholder UVS systemer og data bør behandles i følge UVS klassifikation |  | X |
| **8.1.4 Tilbagelevering af aktiver** |  |  |
| Leverandøren skal sikre, at UVS data ikke bliver udleveret på aktiver, som forhenværende medarbejdere og konsulenter får lov til at beholde |  | X |
| Leverandøren bør sikre, at viden, som er vigtig for den videre drift ikke forsvinder med forhenværende medarbejdere og konsulenter | X |  |
| **8.2.1 Klassifikation af information** |  |  |
| Leverandøren bør forholde sig til UVS klassificering af systemer og data | X |  |
| **8.2.2 Mærkning af information** |  |  |
| Leverandøren bør sikre, at uvedkommende ikke har adgang til UVS data | X |  |
| **8.2.3 Håndtering af aktiver** |  |  |
| håndtering af informationsaktiver bør ske i overensstemmelse med UVS klassifikation af informationsaktiver | X |  |
| passende sikkerhedskontrol bør implementeres til sikring av dataintegritet og tilgængelighed i overensstemmelse med de af UVS fastsatte krav | X |  |
| **8.3.1 Styring af flytbare medier** |  |  |
| udprintet materiale, bærbare lagermedier, herunder ukrypterede harddiske i bærbare pc'ere m.v., der indeholder UVS 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 |  | X |
| **8.3.2 Bortskaffelse af medier** |  |  |
| Medier der kan indeholde UVS data skal bortskaffes på forsvarlig vis ved ødelæggelse efter formelle procedurer |  | X |
| Leverandøren bør holde sig ajour med viden om ødelæggelsesmetoder |  | X |
| **8.3.3 Transport af fysiske medier** |  |  |
| Der bør være en oversigt over medier, der bliver transporteret |  | X |
| Som hovedregel bør transport foretages af leverandøren’s personale og være direkte mellem lokationerne, dvs. uden unødvendigt ophold |  | X |

Viðmerkingar:

|  |
| --- |
| **8.3.1-8.3.3** Veitarin hevur dátur hjá UVS liggjandi. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **9. Adgangsstyring** | **Ja** | **N/A** |
|  |  |  |
| **9.1.1 Politik for adgangsstyring** |  |  |
| På IT-systemer skal UVS informationer samt medarbejderdata til stedse beskyttes gennem adgangskontrol. | X |  |
| **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. | X |  |
| **9.2.1 Brugerregistrering og -afmelding** |  |  |
| autorisere og administrere egne bruger-ID'er | X |  |
| sikre, at der ikke eksisterer delte brugeradgange, men at alle konti er personhenførbare. Hvor dette ikke er muligt skal dokumentation forefindes | X |  |
| få UVS accept før personer uden for leverandøren får adgang til UVS systemer | X |  |
| fjerne adgange, når leverandørens personale ikke længere har behov for adgang | X |  |
| sikre, at konti m.m., der anvendes af leverandører til fjernadgang, kun er aktive i den påkrævede periode | X |  |
| **9.2.2 Tildeling af brugeradgang** |  |  |
| tildeling og ændring af adgange bør altid følge en defineret og dokumenteret proces | X |  |
| overholde leverandørens standard for navngivning ved tilføjelse og ændring af UVS brugerid’er |  | X |
| **9.2.3 Styring af privilegerede adgangsrettigheder** |  |  |
| Tildeling og anvendelse af privilegerede adgangsrettigheder bør begrænses og styres | X |  |
| have procedurer for at opbevare administrative passwords, og på UVS anmodning kunne levere en ajourført oversigt over disse for UVS systemer, der er under leverandørens administration | X |  |
| godkende anmodning om privilegeret adgang for UVS personale til operativ­systemer, applikationer, softwareværktøjer, systemer og enheder under leverandørens ansvar |  | X |
| **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 | X |  |
| 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 leverandørens retningslinjer. | X |  |
| opretholde egen proces for reset af passwords og aflevere disse på en sikker måde | X |  |
| **9.2.5 Gennemgang af brugernes adgangsrettigheder** |  |  |
| udføre årlig gennemgang af bruger-ID'er, herunder:   * individuelt revurdere om leverandørens privilegerede bruger-ID'er og andre brugere fortsat har et arbejdsbetinget behov for adgang * efter revurdering at fremsende liste over leverandørens bruger-ID'er til UVS sikkerhedsfunktion til godkendelse | X |  |
| **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. | X |  |
| **9.3.1 Brug af hemmelig autentifikationsinformation** |  |  |
| Det bør være et krav, at brugere følger leverandørens praksis ved anvendelse af hemmelig autentifikationsinformation. | X |  |
| **9.4.1 Begrænset adgang til informationer** |  |  |
| Adgang til informationer og applikationssystemers funktioner bør begrænses. | X |  |
| **9.4.2 Procedurer for sikker log-on** |  |  |
| Der bør forefindes en sikker log-on procedure | X |  |
| Behandle forespørgsler til password politikker fra UVS |  | X |
| håndhæve passwordregler for bruger-ID'er og konti for systemer, applikationer, enheder og netværksinfra­struktur som defineret | X |  |
| afvigelser, f.eks. forårsaget af tekniske afhængigheder, skal godkendes af UVS | X |  |
| **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. |  | X |
| **9.4.4 Brug af privilegerede systemprogrammer** |  |  |
| Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, bør begrænses og styres effektivt | X |  |
| **9.4.5 Styring af adgang til kildekoder til programmer** |  |  |
| Adgang til kildekoder til programmer samt dokumentation bør begrænses. | X |  |

Viðmerkingar:

|  |  |  |
| --- | --- | --- |
| 9.2.3 godkende anmodning om privilegeret adgang for UVS personale til operativ­systemer, applikationer, softwareværktøjer, systemer og enheder under everandørens ansvar:  UVS biður ikki veitaran um privilegaða atgongd. UVS/KTL umsitur sjálvt administrator atgongd til starvsfólk og gevur brúkaraatgongd. | | |
| **10. Kryptografi** | **Ja** | **N/A** |
|  |  |  |
| **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 |  | X |
| **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. |  | X |

Viðmerkingar:

|  |
| --- |
| Upplýst er, at kryptografi er ikki eitt krav til skipanina |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **11. Fysisk sikkerhed** | **Ja** | **N/A** |
|  |  |  |
| **11.1.1 Fysisk perimetersikring** |  |  |
| Der bør defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter. |  | X |
| **11.1.2 Fysisk adgangskontrol** |  |  |
| Der bør være fysisk adgangskontrol til begrænsning af adgang, så kun autoriseret personale har adgang til sikrede områder |  | X |
| Adgang til sikre områder bør registreres |  | X |
| Leverandøren skal regelmæssigt levere UVS sikkerhedsleder en oversigt over hvem har adgang til leverandørens datacentre |  | X |
| **11.1.3 Sikring af kontorer, lokaler og faciliteter** |  |  |
| Fysisk sikring af kontorer, lokaler og faciliteter bør tilrettelægges og etableres. | X |  |
| **11.1.4 Beskyttelse mod eksterne og miljømæssige trusler** |  |  |
| Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker bør tilrettelægges og etableres. |  | X |
| **11.1.5 Arbejde i sikre områder** |  |  |
| Procedurer for arbejde i sikre områder bør tilrettelægges og etableres. |  | X |
| **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. |  | X |
| **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. |  | X |
| overholde krav til fysisk og forsyningsmæssig sikkerhed, som står i forhold til leverandørens betydning for UVS aktiver på leverandøren. |  | X |
| foretage periodiske gennemgange af fysisk kontrollerede områder, for hvilke leverandøren er ansvarlig for. |  | X |
| **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. |  | X |
| **11.2.3 Sikring af kabler** |  |  |
| Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, bør beskyttes mod aflytning, interferens og skader. |  | X |
| **11.2.4 Vedligeholdelse af udstyr** |  |  |
| Udstyr bør vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet. |  | X |
| **11.2.5 Fjernelse af aktiver** |  |  |
| Udstyr, information og software bør ikke fjernes fra leverandøren uden forudgående tilladelse. |  | X |
| **11.2.6 Sikring af udstyr og aktiver uden for leverandørens lokaler** |  |  |
| Der bør etableres sikring af aktiver uden for leverandøren under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for leverandørens lokaler. |  | X |
| **11.2.7 Sikker bortskaffelse eller genbrug af udstyr** |  |  |
| UVS forventer at lagringsmedier, som kan indeholde UVS 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. |  | X |
| Genbrug af lagringsmedier, som kan indeholde UVS oplysninger, må kun foregå indenfor leverandørens regi. |  | X |
| **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 | X |  |
| **11.2.9 Politik for ryddeligt skrivebord og blank skærm** |  |  |
| UVS forventer, at medier, der kan indeholde UVS fortrolige oplysninger ikke er frit tilgængelige for uvedkommende, f.eks. papir, diske, bånd, usb og oplysninger på skærmen. |  | X |

Viðmerkingar:

|  |
| --- |
| Tað skulu ongar upplýsingar hjá UVS liggja hjá veitaranum. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **12. Driftssikkerhed** | **Ja** | **N/A** |
| **12.1.1 Dokumenterede driftsprocedurer** |  |  |
| At udarbejde og vedligeholde passende dokumentation for opsætning og driftsprocedurer, eksempelvis i driftshåndbøger for de systemer, leverandøren er ansvarlig for | X |  |
| 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 | X |  |
| **12.1.2 Ændringsstyring** |  |  |
| Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, bør styres | X |  |
| 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 UVS drift | X |  |
| sikre, at alle ændringer som kan påvirke UVS driftsstabilitet 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 | X |  |
| ændringer foreslået af leverandøren bør gennemgås og godkendes af autoriseret person hos UVS | X |  |
| ændringer foreslået af UVS bør procesmæssigt administreres af leverandøren fra anmodning til implemen­tering | X |  |
| alle ændringer, som skal implementeres uden for de aftalte servicevinduer, bør have en særskilt godkendelse fra UVS | X |  |
| gældende for operativsystemer, softwareværktøjer og systemer til netværksinfrastruktur under leverandørens administration, bør der i serveroversigten dokumenteres på hvilke servere og hvilke systemer sikkerhedspatches skal implementeres og frekvens |  | X |
| grundet strenge licensforhold skal leverandøren være særlig opmærksom på, om en ændring kan påvirke UVS licensforhold. Ved tvivlsspørgsmål skal UVS altid involveres. UVS licensforhold skal være beskrevet | X |  |
| **12.1.3 Kapacitetsstyring** |  |  |
| foretage den fornødne overvågning af applikationer og databaser i forhold til fejl og performance leverandøren bør på eget initiativ foreslå passende handlinger for at undgå ovennævnte | X |  |
| **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. | X |  |
| * 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 | X |  |
| **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. |  | X |
| installation af anti-malware software, signaturopdatering - når disse er tilgængelige - af alle servere i UVS miljø og eventuelle arbejdsstationer, der benyttes til administration. Af f. eks. performance hensyn, vil der muligvis være fravalg, som skal dokumenteres |  | X |
| 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 UVS som dispensation |  | X |
| inden brug scanne filer, som modtages over netværk eller via anden form for lagingsmedie, for malware |  | X |
| under eventuelt angreb:   * + rimelig reaktionstid på angreb og igangsætning af korrigerende handlinger.   + systemer der er inficeret med malware, skal fjernes fra UVS netværk hurtigst muligt   + hurtigst muligt at informere UVS om skadens omfang   + planlægge genetablering/genoprettelse   + løbende orientering til UVS |  | X |
| **12.3.1 Backup af information** |  |  |
| udføre backup af operativsystemer og infrastruktursoftware. |  | X |
| udføre backup af data som foreskrevet af UVS i en til enhver tid opdateret serveroversigt |  | X |
| efterse backup rapport regelmæssigt, for at sikre at foreskrevne backup rutiner hos leverandøren overholdes |  | X |
| Deltage i regelmæssige genetableringstests | X |  |
| på anmodning at tilvejebringe rapporter vedrørende gennemførsel af genetableringstester | X |  |
| 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 UVS retningslinjer for klassifikation) |  | X |
| **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 | X |  |
| logs bør gemmes sikkert | X |  |
| logs bør gennemgås regelmæssigt manuelt eller automatisk for at identificere mistænkelig aktivitet | X |  |
| der bør være aftalt, hvor længe logs skal gemmes | X |  |
| udlevere logs til UVS efter ønske | X |  |
| **12.4.2 Beskyttelse af log-oplysninger** |  |  |
| Logningsfaciliteter og log-oplysninger bør beskyttes mod manipulation og uautoriseret adgang. | X |  |
| **12.4.3 Administrator- og operatørlogge** |  |  |
| Aktiviteter udført af systemadministrator og systemoperatør bør logges, og loggene bør beskyttes og gennemgås regelmæssigt. Her er tale om loggs i forbindelse med journalsystemet. | X |  |
| **12.4.4 Tidssynkronisering** |  |  |
| Urene i alle relevante informationsbehandlingssystemer eller et sikkerhedsdomæne bør være synkroniseret til en enkelt referencetidsangivelseskilde. |  | X |
| **12.5.1 Softwareinstallation i driftssystemer** |  |  |
| Der bør implementeres procedurer til styring af softwareændringer i driftssystemer. | X |  |
| Hvis UVS systemer og/eller data berøres, bør UVS involveres | X |  |
| servere skal være hærdet, hvor det er muligt |  | X |
| sammen med UVS at definere et servicevindue til brug ved implementering af security patches | X |  |
| få UVS godkendelse, hvis sikkerhedsændringer skal udføres uden for de aftalte servicevinduer | X |  |
| i god tid informere UVS om planlagte security patches | X |  |
| **12.6.1 Styring af sårbarheder** |  |  |
| Sammen med sikkerhedslederen på UVS, har sikkerhedslederen på leverandøren ansvaret for, at der løbende indhentes informationer om sårbarheder. UVS og leverandørens eksponering for sådanne sårbarheder bør evalueres, og der bør iværksættes passende foranstaltninger for at håndtere den tilhørende risiko. | X |  |
| **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. | X |  |
| **12.7.1 Kontroller i forbindelse med audit af informationssystemer** |  |  |
| Hvis auditkrav og -aktiviteter, der indebærer verifikation af driftssystemer kan påvirke UVS, skal dette planlægges og aftales omhyggeligt med UVS for at minimere risikoen for afbrydelse af forretningsprocesserne. | X |  |
|  |  |  |

Viðmerkingar:

|  |
| --- |
| 12.1.3 Kapacitetsstyring: CPU, RAM og Disk nýtsla er við í standard yvirvakingini hjá KTL. Hetta sigur tó ikki altíð so nógv um applikatiónina ella databasan. |
| 12.1.4 Adskillelse af udviklings/test- og driftsmiljøer:  Skal UVS hava eitt test umhvørvi. |
| 12.3.1 Backup af information: Elektron ger bara restore/recovery og so er tað leverandøren, sum fer inn og verificerar, at data/skipanin er reetablerað |
| 12.4.1 Hændelseslogning: Av tí at viðkvæmir persónsupplýsingar verða viðgjørdir í skipanin er neyðugt at skipanin loggar alla lesing. |
| 12.4.3 Administrator- og operatørlogge: Hetta meinast við administrator og operatør loggar í skjalhaldskipanini og ikki operativsystem, tí tað verður gjørt aðrastaðni. |
| 12.5.1 Softwareinstallation i driftssystemer: Veitarin skal leggja dagføringar inn til alt, sum ikki er operativsystem t.d. í journalskipanini |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **13 Kommunikationssikkerhed** | **Ja** | **N/A** |
| **13.1.1 Netværksstyring** |  |  |
| Netværk bør styres og kontrolleres for at beskytte informationer i systemer og applikationer. |  | X |
| styre leverandørens netværkskomponenter anvendt i forbindelse med UVS 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 UVS miljø |  | X |
| udøve aktiviteter med henblik på styring af netværkssikkerhed for den del der er under leverandørens ansvarsområde, herunder:   * styre og drifte UVS 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 UVS systemer, må kun ske hvis den er godkendt af UVS |  | X |
| **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. |  | X |
| **13.1.3 Opdeling i netværk** |  |  |
| Grupper af informationstjenester, brugere og informationssystemer bør opdeles i netværk efter anmodning fra UVS |  | X |
| efter anmodning fra UVS at identificere alle eksisterende fjernadgange hos leverandøren (såsom dial-in, VPN, etc) og samarbejde med UVS om eventuelle ændringer |  | X |
| **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. | X |  |
| 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 | X |  |
| **13.2.2 Aftaler om informationsoverførsel** |  |  |
| Aftaler bør omhandle sikker overførsel af forretningsinformation mellem leverandøren. | X |  |
| **13.2.3 Elektroniske meddelelser** |  |  |
| Fortrolige oplysninger bør ikke sendes ubeskyttet elektronisk | X |  |
| **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 | X |  |

Viðmerkingar:

|  |
| --- |
| 13.2.1 Politikker og procedurer for informationsoverførsel:  **Kann nakað yvirførast, og í so fall, hvat?**  Hetta punktið sigur eisini, at veitarin kann ikki tilganga skipanirnar ókrypterað |
| 13.2.2 Aftaler om informationsoverførsel: Nakað tað sama sum omanfyri |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **14. Anskaffelse, udvikling og vedligeholdelse af systemer** | **Ja** | **N/A** |
|  |  |  |
| **14.1.1 Analyse og specifikation af informationssikkerhedskrav** |  |  |
| Informationssikkerhedsrelaterede krav bør være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer. | X |  |
| **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. |  | X |
| **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. |  | X |
| **14.2.1 Sikker udviklingspolitik** |  |  |
| Der bør fastlægges og anvendes regler for udvikling af software og systemer i organisationen. | X |  |
| nye systemer bør opfylde leverandørens samlede sikkerhedskrav | X |  |
| **14.2.2 Procedurer for styring af systemændringer** |  |  |
| Ændringer af systemer inden for udviklingslivscyklussen bør styres ved hjælp af formelle procedurer for ændringsstyring. | X |  |
| **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. | X |  |
| **14.2.4 Begrænsning af ændringer** |  |  |
| Ændringer i systemer bør vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer bør styres effektivt. | X |  |
| **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). |  | X |
| **14.2.6 Sikkert udviklingsmiljø** |  |  |
| Der bør være etableret sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus. |  | X |
| **14.2.7 Outsourcet udvikling** |  |  |
| leverandøren skal acceptere at UVS fører tilsyn med og overvåger systemudviklingsaktiviteter. | X |  |
| **14.2.8 Systemsikkerhedstest** |  |  |
| Test af sikkerhedsfunktionalitet bør udføres ved udvikling. | X |  |
| **14.2.9 Systemgodkendelsestest** |  |  |
| Der bør være aftalt, hvordan tester skal foregå. | X |  |
| **14.3.1 Sikring af testdata** |  |  |
| Testdata bør udvælges omhyggeligt og beskyttes og kontrolleres. | X |  |

Viðmerkingar:

|  |
| --- |
| 14.2.3 Teknisk gennemgang af applikationer efter ændringer af driftsplatforme:  T.d. tá skipanin verður dagførd, tá verða nýggir servarar gjørdir og broytir man driftplatformin, tá eigur veitarin at gjøgnumganga, at tingini eru í ordan |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **15. Leverandørforhold** | | |
|  | **Ja** | **N/A** |
| **15.1.1 Informationssikkerhedspolitik for leverandørforhold** |  |  |
| Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til UVS aktiver bør aftales med UVS og dokumenteres |  | X |
| **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 UVS information. |  | X |
| **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. |  | X |
| **15.2.1 Overvågning og gennemgang af leverandørydelser** |  |  |
| Leverandøren bør regelmæssigt have mulighed for at overvåge, gennemgå og auditere leverandørers ydelser med hensyn til UVS |  | X |
| **15.2.2 Styring af ændringer af leverandørydelser** |  |  |
| Ændringer af leverandørers ydelser til leverandøren med hensyn til UVS, 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. |  | X |

Viðmerkingar:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **16 Styring af informationssikkerhedsbrud** | | |
|  | **Ja** | **N/A** |
| **16.1.1 Ansvar og procedurer** |  |  |
| Ledelsesansvar og procedurer bør fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud. | X |  |
| Procedurerne bør blandt andet indeholde krav om at identificere, logge, spore, afhjælpe, kommunikere og eskalere sikker­heds­hændelser | X |  |
| **16.1.2 Rapportering af informationssikkerhedshændelser** |  |  |
| I tilfælde af et alvorligt brud på sikkerheden, skal leverandøren straks iværksætte afhjælpende handlinger og straks informere UVS sikkerhedsleder om hændelsen. | X |  |
| hurtigst muligt informere UVS om enhver identificeret hændelse ved UVS systemer varetaget af leverandøren eller hændelser, der kan påvirke UVS systemer og anbefale mulige forebyggende og afhjælpende handlinger | X |  |
| **16.1.3 Rapportering af informationssikkerhedssvagheder** |  |  |
| Medarbejdere på leverandøren og konsulenter, som leverandøren måtte anvende og som bruger UVS systemer og -tjenester, bør have pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i informationssystemer og -tjenester. | X |  |
| **16.1.4 Vurdering af og beslutning om informationssikkerhedshændelser** |  |  |
| Informationssikkerhedshændelser bør vurderes, og det bør besluttes, om de skal klassificeres som informationssikkerhedsbrud. | X |  |
| assistere UVS med indledende vurdering af hændelsen, herunder tildeling af prioritet og ejerskab. | X |  |
| assistere UVS med at definere sikkerhedshændelsers prioriteringsniveauer og til­hø­ren­de eskaleringsprocedurer. | X |  |
| tage beslutninger om handlinger til at løse sikkerhedshændelser der kan påvirke UVS, det være sig leverandørens netværk, leverandørens system, leverandørens personale eller leverandørens data, herunder passende indsamling af beviser | X |  |
| **16.1.5 Håndtering af informationssikkerhedsbrud** |  |  |
| Informationssikkerhedsbrud bør håndteres i overensstemmelse med de dokumenterede procedurer. | X |  |
| undersøge it-sikkerhedsbrud og indsamle beviser ved at levere teknisk infor­ma­tion i relation til it-sikkerhedsbrud og assistere UVS med informationsanalyse og problemidentifikation | X |  |
| **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. | X |  |
| **16.1.7 Indsamling af beviser** |  |  |
| Leverandøren bør definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som beviser. | X |  |
| Sammen med UVS prioriterer 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. | X |  |
| sikre at medium og højt prioriterede sikkerhedshændelser efterfølgende bliver rapporteret skriftligt, og at problemanalyse og plan for fremtidig imødegåelse, tilsvarende bliver rapporteret til UVS sikkerhedsleder | X |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Viðmerkingar:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring** | | |
|  | **Ja** | **N/A** |
| **17.1.1 Planlægning af informationssikkerhedskontinuitet** |  |  |
| Leverandøren bør fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe. |  | X |
| sikre, at UVS’ systemer bliver prioriteret i tilfælde af en katastrofesituation, | X |  |
| sikre, at UVS har en kontaktperson i leverandørens beredskabsgruppe, som har løbende kontakt med UVS | X |  |
| efter anmodning at være UVS behjælpelig i en beredskabssituation | X |  |
| **17.1.2 Implementering af informationssikkerhedskontinuitet** |  |  |
| Leverandøren bør fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation. | X |  |
| sikre, at medarbejdere med roller i krisestaben kender deres opgaver og ansvar | X |  |
| straks meddele UVS om enhver situation, som leverandøren mener, repræsenterer en katastrofe eller kan udvikle sig som en sådan | X |  |
| meddele UVS om alle ændringer til driftsmiljøet udført af leverandøren, som kan/vil påvirke beredskabsplanen | X |  |
| **17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten** |  |  |
| Leverandøren 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. |  | X |
| anvende og teste funktionalitet og driftsprocedurer i beredskabsplanen regelmæssigt, herunder at teste beredskabsledelsernes kommunikationsevner |  | X |
| deltage i UVS planlægning af de årlige beredskabsplansaktiviteter |  | X |
| Leverandøren bør bistå og indgå i UVS test af beredskabet | X |  |
| udføre aktivitet i forbindelse med de årlige revurderinger og katastrofeberedskabstest som er leverandørens ansvar og fastlagt i en plan | X |  |
| levere dokumentation af resultater fra aktiviteterne i forbindelse med test af katastrofeberedskabet. | X |  |
| **17.2.1 Tilgængelighed af informationsbehandlingsfaciliteter** |  |  |
| Informationsbehandlingsfaciliteter bør implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav. |  | X |
| Leverandøren bør have backupdatacenter med nødvendige faciliteter. |  | X |

Viðmerkingar:

|  |  |  |
| --- | --- | --- |
| 17.1.2 Implementering af informationssikkerhedskontinuitet: veitarin má gera hetta m.a. við úrslitinum av recovery test osv. | | |
| 17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten:  veitarin fær onkrar uppgávur í samband við, at UVS ynskir at testa t.d. restore/recovery av skipanini ella pørtum av henni | | |
| **18 Overensstemmelse** | | |
|  | **Ja** | **N/A** |
| * + 1. **Identifikation af gældende lovgivning og kontraktkrav** |  |  |
| Leverandøren bør overholde alle relevante lov-, myndigheds- og kontraktkrav. | X |  |
| **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. | X |  |
| **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. | X |  |
| **18.1.4 Privatlivets fred og beskyttelse af personoplysninger** |  |  |
| Privatlivets fred og personoplysninger bør beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter. | X |  |
| **18.1.5 Regulering af kryptografi** |  |  |
| Kryptografi bør anvendes i overensstemmelse med alle relevante aftaler, love og forskrifter. | X |  |
| **18.2.1 Uafhængig gennemgang af informationssikkerhed** |  |  |
| Leverandørens 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. | X |  |
| anvise en kontaktperson i forhold til revision med ansvar for at koordinere de it-revisionsmæssige support­aktiviteter | X |  |
| Leverandøren skal årligt ved UVS anmodning, levere en revisionserklæring omkring leverandørens sikkerhedsforhold, underskrevet af en statsautoriseret revisor. Revisionserklæringen bør udtale sig om leverandørens samlede data-, system- og driftssikkerhed efter gældende revisionsstandard. | X |  |
| UVS revisor, sikkerhedsrådgiver eller sikkerhedsleder, har fri adgang til at foretage varslet sikker­heds­revision/inspektion hos leverandøren. Leverandøren skal i den forbindelse stille alle relevante informationer og logninger til rådighed for UVS sikkerhedsgennemgang.  Alle sikkerhedsforhold vedrørende kontraktens opfyldelse kan undersøges i forbindelse hermed. | X |  |
| Leverandøren bør udvikle og implementere handlingsplaner for observationer fundet under revision, som leverandøren er ansvarlig for:   * lukke observationer hurtigst muligt efter aftale med UVS * rapportere lukning af anbefalinger til UVS | X |  |
| **18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder** |  |  |
| Leverandøren bør regelmæssigt undersøge, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav. | X |  |
| Der bør være aftalt hvor længe dokumentation, herunder beskrivelser, estimater, risikovurderinger, testresultater og godkendelser skal opbevares. | X |  |
| **18.2.3 Undersøgelse af teknisk overensstemmelse** |  |  |
| varsle og iværksætte periodiske sårbarhedsscanninger og penetrationstest af systemer under leverandørens driftsansvar |  | X |
| være UVS behjælpelig med at udføre sårbarhedsscanninger og penetrationstester og sørge for ekstern penetrationtest af den del af leverandørens miljø der kan påvirke UVS miljø |  | X |
| ved egen periodisk gennemgang at sikre, at opsætningen af det tekniske miljø overholder UVS og leverandørens tekniske og sikkerhedsmæssige krav og specifikationer. |  | X |
| meddele UVS om eventuelle mangler og sammen med UVS udarbejder en plan for afhjælpning af disse. | X |  |

Viðmerkingar:

|  |
| --- |
| 18.2.3 Undersøgelse af teknisk overensstemmelse: Veitarin skal ikki gera veikleika skanning, men tað verður gjørt, og so er tað veitarin, sum mugu hjálpa UVS at rætta trupulleikarnar |
|  |
|  |
|  |
|  |

Váttað verður, at omanfyri útvaldu krøv við møguligu viðmerkingum eru góðtikin.

Fyri veitaran:

Dagfesting:

Undirskrift: