|  |
| --- |
| Sådan stiller du krav til leverandører om informationssikkerhed   * *Katalog* |
| December 2017 |

Kravkataloget er udviklet af parterne i regi af  
Den fællesoffentlige digitaliseringsstrategi 2016 - 2020  
og udarbejdet i samarbejde med  
Kammeradvokaten Advokatfirmaet Poul Schmith

Kravkataloget bygger på   
standarden fra Dansk Standard og   
rammeværktøjet CIS Center for Internet Security

*ISO27001, Anneks A er gengivet med tilladelse fra Fonden Dansk Standard.   
Ledelsessystemer for informationssikkerhed © Dansk Standard.*

*SANS CIS Critical Security Controls er gengivet med tilladelse fra Center for Internet Security. Rammeværkets kontroller er oversat fra engelsk til dansk af Digitaliseringsstyrelsen og Kammeradvokaten til brug for Kravkataloget. CIS har ikke verificeret oversættelsen.*



Indhold

Vejledning 5

Læsevejledning 5

Øvrige anvendelsesområder for kravkataloget 5

Beskrivelse af sammenhængende processer 6

Ordregivers fremgangsmåde 7

Opmærksomhedspunkter ved implementering i en kontrakt 8

Grundlaget for kravene i Kravkataloget 9

Kravkatalogets overordnede struktur - generelle og specifikke krav 10

De specifikke krav - kravtabellernes opbygning og indhold 10

Bilag 1: Kravkatalog baseret på ISO27001 12

1. Generelle krav 12

2. Specifikke krav baseret på ISO27001, Anneks A 13

2.1 Informationssikkerhedspolitikker – ISO27001, Anneks A, punkt 5 13

2.2 Organisering af informationssikkerhed – ISO27001, Anneks A, punkt 6 13

2.3 Personalesikkerhed – ISO27001, Anneks A, punkt 7 14

2.4 Styring af aktiver - ISO27001, Anneks A, punkt 8 15

2.5 Adgangsstyring - ISO27001, Anneks A, punkt 9 16

2.6 Kryptografi - ISO27001, Anneks A, punkt 10 18

2.7 Fysisk sikring og miljøsikring - ISO27001, Anneks A, punkt 11 18

2.8 Driftssikkerhed - ISO27001, Anneks A, punkt 12 20

2.9 Kommunikationssikkerhed - ISO27001, Anneks A, punkt 13 22

2.10 Anskaffelse, udvikling og vedligeholdelse af systemer - ISO27001, Anneks A, punkt 14 23

2.11 Leverandørforhold - ISO27001:2013, Anneks A, punkt 15 25

2.12 Styring af informationssikkerhedsbrud - ISO27001, Anneks A, punkt 16 26

2.13 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring - ISO27001, Anneks A, punkt 17 27

2.14 Overensstemmelse - ISO27001, Anneks A, punkt 18 27

Bilag 2: Kravkatalog baseret på SANS CIS 29

1. Specifikke krav baseret på SANS CIS Critical Security Controls 29

1.1 SANS CIS 1: Inventory of Authorized and Unauthorized Devices 29

1.2 SANS CIS 2: Inventory of Authorized and Unauthorized Software 30

1.3 SANS CIS 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers 31

1.4 SANS CIS 4: Continuous Vulnerability Assessment and Remediation 34

1.5 SANS CIS 5: Controlled Use of Administrative Privileges 36

1.6 SANS CIS 6: Maintenance, Monitoring, and Analysis of Audit Logs 38

1.7 SANS CIS 7: Email and Web Browser Protections 39

1.8 SANS CIS 8: Malware Defenses 41

1.9 SANS CIS 9: Limitation and Control of Network Ports, Protocols, and Services 42

1.10 SANS CIS 10: Data Recovery Capability 43

1.11 SANS CIS 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches 44

1.12 SANS CIS 12: Boundary Defense 46

1.13 SANS CIS 13: Data Protection 48

1.14 SANS CIS 14: Controlled Access Based on the Need to Know 50

1.15 SANS CIS 15: Wireless Access Control 51

1.16 SANS CIS 16: Account Monitoring and Control 53

1.17 SANS CIS 17: Security Skills Assessment and Appropriate Training to Fill Gaps 55

1.18 SANS CIS 18: Application Software Security 56

1.19 SANS CIS 19: Incident Response and Management 58

1.20 SANS CIS 20: Penetration Tests and Red Team Exercises 59

Bilag 3: Mapning mellem ISO27001, SANS CIS og Kravkataloget 62

|  |
| --- |
|  |
| Vejledning |
|  |

Det primære formål med dette ”Kravkatalog” er at hjælpe og inspirere til at stille relevante, hensigtsmæssige sikkerhedskrav ved eksempelvis udbud og indgåelse af it-kontrakter med leverandører. Kravkataloget kan desuden være relevant i enhver kontrakt, hvor leverandøren behandler information for kunden.

Anvendelsen af Kravkataloget forudsætter, at brugeren udvælger krav på baggrund af risikovurderinger, der bør understøtte ledelsens til- og fravalg af sikkerhedsmæssige tiltag.

Kravene i kataloget er formuleret generisk, og kravene skal derfor tilpasses den konkrete kontraktuelle kontekst. Eksempelvis skal begrebsanvendelsen afstemmes med kontraktens definitioner. Der er desuden ikke tale om en udtømmende liste af krav, og der kan derfor være behov for at stille yderligere krav, der ikke fremgår af Kravkataloget.

Læsevejledning

Kravkataloget består af denne vejledning samt ”Bilag 1: Kravkatalog baseret på ISO27001” og ”Bilag 2: Kravkatalog baseret på SANS CIS”.

Vejledningen beskriver opbygningen af Kravkataloget og indeholder generelle oplysninger, om hvilke forudsætninger der skal være til stede for at arbejde med Kravkataloget, herunder bl.a. sammenhæng til risikovurderinger, tekniske og organisatoriske sikkerhedstiltag, forretningsmæssige beslutninger samt kontraktuelle begreber.

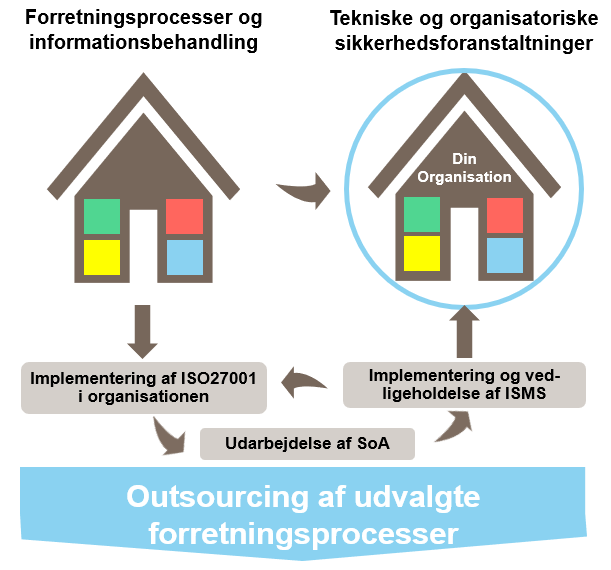
De to bilag indeholder krav baseret på *ISO27001:2013*, der er en standard for informationssikkerhedsledelse, samt krav baseret på rammeværktøjet *SANS CIS Critical Security Controls v. 6.1*, der har særligt fokus på operationel it-sikkerhed. Bilag 1 og Bilag 2 indeholder tilsammen 286 kontraktuelle krav, som kunden (ordregiver) efter behov kan vælge imellem og indarbejde i sit samarbejde med leverandøren.

Øvrige anvendelsesområder for kravkataloget

Kravkatalogets primære formål er som anført ovenfor at understøtte udarbejdelsen af kravspecifikationer vedrørende informationssikkerhed i kontrakter. Kravkataloget kan dog også understøtte en række øvrige aktiviteter, herunder kan Kravkataloget:

* Understøtte forventningsafstemning mellem ordregiver og leverandøren, fx hvis der vælges krav, der præciserer roller og ansvar.
* Anvendes i ordregivers leverandørstyring, herunder fordi Kravkataloget indeholder konkrete krav, der kan være meget håndgribelige at følge op på.
* Tjene som dokumentation (eksempelvis ved tilsyn) for, at der stilles relevante sikkerhedskrav til leverandører, fx krav om logning eller adgangsstyring.
* Tjene som dokumentation for, at lovkrav, øvrig regulering samt standarder mv. efterleves.
* Anvendes ved ekstern og intern auditering eller ved tilsyn og revision.
* Tjene som generel inspiration til sikkerhedsarbejdet.

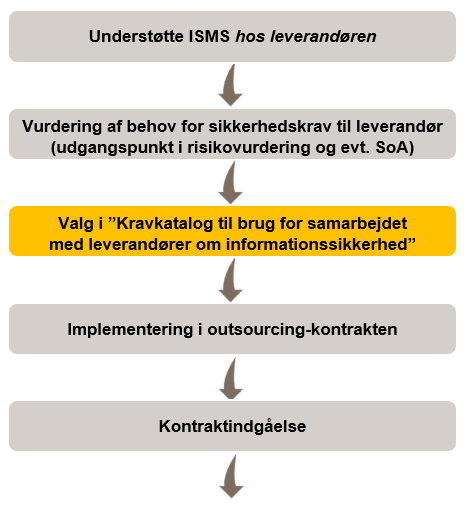
Beskrivelse af sammenhængende processer

I figuren nedenfor illustreres sammenhængen mellem en organisations arbejde med informationssikkerhed, outsourcing af udvalgte forretningsprocesser og understøttelse af sikkerheden hos outsourcingleverandøren vha. kontraktuelle krav. De orange bokse illustrerer, hvor Kravkataloget er relevant.

**Outsourcing**

Outsourcing er i sin enkelthed at overføre varetagelse af en opgave/dele af en opgave til et andet firma.  
*Kilde: Dansk IT ”Sikkerhed ved it-outsourcing”*

Arbejdet med informationssikkerhed starter internt i organisationen fx med udgangspunkt i ISO27001. Dette indebærer, at der udarbejdes en risikovurdering, og ledelsen beslutter et Statement of Applicability (SoA) og implementerer og vedligeholder et Ledelsessystem for informationssikkerhed (ISMS). Læs de efterfølgende faktabokse med uddybende beskrivelser af SoA og ISMS.



Figuren til højre illustrerer endvidere, at der ved outsourcing af udvalgte forretningsprocesser og informationsbehandling opstår et behov for at regulere informationssikkerheden hos leverandøren. Dette behov kan understøttes ved at anvende Kravkataloget i forbindelse med indgåelse af kontrakten.

Ordregivers fremgangsmåde

**ISMS**

ISMSstår for ”Information Security Management System”, der på dansk er oversat til ”ledelsessystem for informationssikkerhed”.

*Kilde: Digitaliseringsstyrelsen ”Vejledning i informationssikkerhedsstyring (ISMS)”*

Det er ordregiver, der beslutter, hvilke krav fra Kravkataloget der er relevante at implementere i den konkrete kontrakt. Anvendelse af Kravkataloget indebærer dermed, at der træffes tekniske og forretningsmæssige beslutninger i relation til udvælgelsen af, hvilke krav der skal stilles til en leverandør.

I mange organisationer, eksempelvis organisationer der efterlever ISO27001, vil der imidlertid allerede være truffet en række sikkerhedsmæssige beslutninger af ledelsen, som kan danne udgangspunkt for valget af krav til en outsourcingleverandør. Valget af krav i Kravkataloget kan således ske på baggrund af en risikovurdering vedrørende den information og de aktiviteter, der er omfattet af outsourcingkontrakten, ligesom der kan hentes inspiration i ordregivers *Statement of Applicability (SoA)*.

**Statement of Applicability (SoA)**

SoA kan frit oversat forstås som en erklæring af, hvilket sikkerhedsniveau organisationen aktivt har besluttet sig for og hvorfor. SoA-dokumentet kan ses som en statusopgørelse for organisationens arbejde med informationssikkerhed og som beslutningsdokumentation for dens til- og fravalg af sikkerhedsmæssige indsatser.

*Kilde: Digitaliseringsstyrelsen ”Vejledning i informationssikkerhedsstyring (ISMS)”*

Fremgangsmåden kan herefter være, at hvis ordregiver, jf. ordregivers SoA, har implementeret en given ISO27001-kontrol, og denne kontrol er relevant for outsourcingkontraktens genstand, så skal denne kontrol understøttes med et kontraktkrav til leverandøren. Samtlige kontroller fra ISO27001, Anneks A er omsat til krav i Kravkataloget (se Bilag 1, afsnit 2). På baggrund af kontrollens nummer i ISO27001, Anneks A identificeres herefter det relevante kontraktkrav at stille til leverandøren.

**ISO27001**

ISO27001 version 2013 er en international standard, hvis formål er at opstille krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS).

*Kilde: Dansk Standard "DS/ISO/IEC 27001”.*

Derudover skal ordregiver tage stilling til, hvordan der følges op på kravene til leverandøren, herunder om dette skal ske ved en revisorerklæring og/eller ved et kontraktreguleret test- og KPI-regime til løbende opfølgning på kravenes effektivitet.

**Kontraktregulering af test- og KPI-regime i relation til sikkerhed**

Med henblik på at kontraktregulere et test- og KPI-regime kan der bl.a. hentes inspiration i udgivelsen ”A Measurement Companion to the CIS Controls”, der angiver ”Measures”, ”Metrics” og ”Effectiveness Tests” til opfølgning på SANS CIS-kontrollerne.   
*Kilde:* [*https://www.cisecurity.org/white-papers/a-measurement-companion-to-the-cis-critical-controls/*](https://www.cisecurity.org/white-papers/a-measurement-companion-to-the-cis-critical-controls/)..

Opmærksomhedspunkter ved implementering i en kontrakt

Kravkataloget er generisk, og de krav, som ordregiver udvælger, skal tilpasses den konkrete kontekst, hvori de skal indgå.

Såfremt kravene i Kravkataloget skal implementeres i en kontrakt, vil de, der er ansvarlige for at skrive kontrakten, ofte vælge at placere sikkerhedskravene i et dedikeret ”sikkerhedsbilag” til kontrakten (fx ”*Bilag X – Sikkerhed”*). Sikkerhedskravene vil dog typisk indgå i et samlet kontraktgrundlag med en hovedkontrakt og en række andre kontraktbilag. Det er derfor nødvendigt, at kravene fra Kravkataloget tilpasses denne kontekst.

I Kravkatalogets krav er en række begreber forudsat kontraktuelt defineret. Disse begreber, eller varianter heraf, indgår ofte i kontrakter, hvor informationssikkerhed er relevant. Det drejer sig om:

* Informationsaktiver: Aktiver som indgår i informationsbehandlingen.
* Infrastruktur: Hardware, netværk (LAN, WAN, switches, routere, kabler), storage, basissoftware, herunder operativsystemer, middleware mv.
* Programmel: Kode, funktionalitet, brugergrænseflade samt integrationer.

Ovenstående begreber i Kravkataloget skal således forstås på denne måde. I konkrete kontrakter kan der imidlertid være valgt en anden begrebsanvendelse. På den baggrund skal begrebsanvendelsen i de valgte krav fra Kravkataloget derfor afstemmes med den konkrete kontrakts definitioner i forbindelse med implementering.

I Kravkatalogets krav er ligeledes forudsat referencer til en række bilag, der ofte indgår i kontrakter, hvor informationssikkerhed er relevant. Det drejer sig om:

* Bilag [X] Dokumentation: Fastlægger kravene til den dokumentation, som er nødvendig for at anvende, idriftsætte, drive, vedligeholde og videreudvikle systemet.
* Bilag [X] Drift: Beskriver kravene til leverandørens ydelser vedrørende it-drift.

Ved implementering af krav fra Kravkataloget skal det sikres, at eventuelle henvisninger til kontraktbilag er korrekte og relevante. Det kan i den konkrete kontekst ligeledes være relevant at henvise til andre kontraktbilag, end dem der er indeholdt i Kravkataloget.

Endeligt bemærkes det i relation til formuleringen af Kravkatalogets krav, at kravene er formuleret med henblik på at afgrænse disse til alene at vedrøre den konkrete kontrakt. Det skyldes, at sikkerhedsforanstaltninger ofte har en organisatorisk eller generel karakter. Stilles denne type krav til en leverandør, kan det være vanskeligt at afgrænse en kontraktuel forpligtelse. Hvis et krav er rettet mod ”organisationen”, kan det eksempelvis være vanskeligt at afgrænse, om kravet omfatter hele leverandørens internationale koncern eller en bestemt division. Dette kan have utilsigtede kommercielle konsekvenser.

I flere af Kravkatalogets krav indgår derfor formuleringen ”i relation til Kontraktens opfyldelse” eller lignende. Årsagen til formuleringen er den ovenfor anførte intention om at begrænse Leverandørens forpligtelse til kun at omfatte de dele af Leverandørens organisation, infrastruktur mv., som anvendes til at opfylde kontrakten. Et krav, som leverandøren ellers kunne betragte som uforholdsmæssigt byrdefuldt, søges derved begrænset uden at gå på kompromis med kravene til informationssikkerheden i relation til kontrakten.

Grundlaget for kravene i Kravkataloget

Kravkataloget er baseret på standarden *ISO27001:2013* (ISO27001), der suppleres med krav fra rammeværket *SANS CIS Critical Security Controls v. 6.1* (SANS CIS). Disse er omsat til generiske kontraktkrav, som fremgår af Kravkataloget i Bilag 1 og Bilag 2.

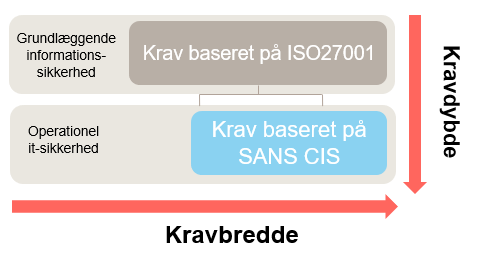
**SANS CIS Critical Security Controls**

SANS CIS er et internationalt rammeværk for it-sikkerhed, der opsætter en række prioriterede, velfunderede og understøttede aktiviteter, som en organisation kan iværksætte med henblik på at vurdere og forbedre sit sikkerhedsniveau.

*Kilde: SANS "CIS Critical Security Controls – Version 6.1”.*

Krav baseret på ISO27001, Anneks A, findes i Bilag 1, afsnit 2. Disse krav har karakter af brede grundlæggende krav til leverandørens informationssikkerhed, herunder både organisatorisk og teknisk sikkerhed.

Såfremt ordregiveren vurderer, at yderligere kontrol med leverandørens sikkerhedsydelser er relevant, er der i Kravkatalogets Bilag 2, afsnit 1 inkluderet krav baseret på SANS CIS. Disse krav er dybere og mere operationelle. SANS CIS har dog ikke samme bredde som ISO27001, idet SANS CIS fokuserer på operationel (teknisk) it-sikkerhed. Der er således ikke en SANS CIS-kontrol for alle ISO-kontroller. Dette er illustreret i nedenstående figur:



Se endvidere ”Bilag 3 Mapning mellem ISO27001, SANS CIS og Kravkataloget”.

Kravkatalogets overordnede struktur - generelle og specifikke krav

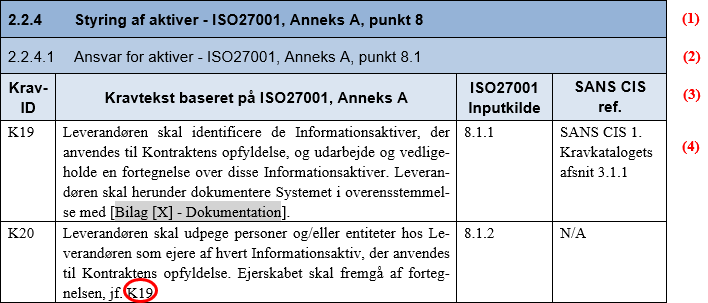
Kravkatalogets Bilag 1, afsnit 1 indeholder de generelle krav. De generelle krav forpligter leverandøren til at arbejde risikobaseret (jf. krav K2) med informationssikkerhed i henhold til ISO27001 eller tilsvarende standard (jf. krav K1). De generelle krav kombineres typisk med specifikke krav til informationssikkerhed. Koblingen mellem de generelle krav og de specifikke krav er fastlagt i krav K3.

Kravkatalogets Bilag 1 og Bilag 2 indeholder et katalog over de specifikke krav, der kan udvælges af ordregiver i forbindelse med udarbejdelsen af kravspecifikationen om informationssikkerhed. De i Bilag 1, afsnit 2 og Bilag 2, afsnit 1 indeholdte kravtabeller forklares nærmere nedenfor.

De specifikke krav - kravtabellernes opbygning og indhold

Kravkatalogets specifikke krav er bygget op af en tabel i henholdsvis Bilag 1, afsnit 2 og Bilag 2, afsnit 1. Tabellen i Bilag 1, afsnit 2 indeholder specifikke krav baseret på ISO27001, Anneks A. Tabellen i Bilag 2, afsnit 1 indeholder specifikke krav baseret på SANS CIS.

Kravtabellen i Bilag 1, afsnit 2 har følgende opbygning, der illustreres med afsæt i et eksempel på et krav baseret på en kontrol i ISO27001, Anneks A, punkt 8:



Række **(1)** henviser til det overordnede emne i ISO27001, Anneks A.

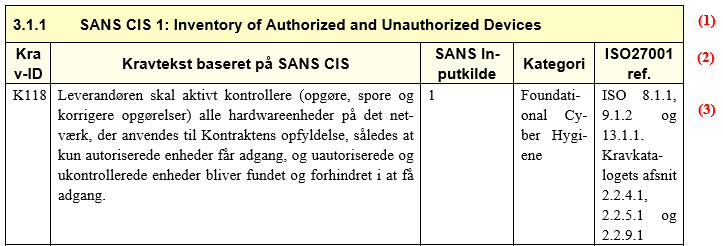
Række **(2)** henviser til underemnet i ISO27001, Anneks A.

Række **(3)** indeholder kolonnerne:

* Krav-ID: Udgør Kravkatalogets interne fortløbende kravnumre, som anvendes til Kravkatalogets interne henvisninger (eksemplificeret ved **O** ovenfor).
* Kravtekst baseret på ISO27001 Anneks A: Kravkatalogets krav.
* ISO27001 Inputkilde: Reference til den kontrol i ISO27001, Anneks A, som kravet er baseret på.
* SANS CIS ref.: Reference til eventuelle dybere kontroller inden for emnet i SANS CIS samt reference til krav i Kravkataloget baseret på pågældende SANS CIS kontroller. Hvis der ikke foreligger en SANS CIS kontrol for den pågældende ISO-kontrol fremgår dette som ”N/A”.

Række **(4)** indeholder et eksempel på, hvorledes kolonnerne er udfyldt i Kravkataloget.

Kravtabellen i bilag 2, afsnit 1 har følgende opbygning, der illustreres med afsæt i et eksempel på et krav baseret på SANS CIS 1:



Række **(1)** henviser til afsnit og emne i SANS CIS.

Række **(2)** indeholder kolonnerne:

* Krav-ID: Udgør Kravkatalogets interne fortløbende kravnumre, som anvendes til Kravkatalogets interne henvisninger.
* Kravtekst baseret på SANS CIS: Kravkatalogets krav.
* SANS Inputkilde: Reference til den kontrol eller sub-kontrol i SANS CIS, som kravet er baseret på. En kontrol angives med ét tal fx ”1”, mens en sub-kontrol angives med to tal separeret af et punktum fx ”1.1”.
* Kategori: Angiver kategoriseringen fra SANS CIS af en given kontrol. SANS CIS 1 – SANS CIS 5 er essentielle for implementering af it-sikkerhed og er derfor kategoriseret ”Foundational Cyber Hygiene”. Sub-kontrollerne er kategoriseret i Foundational eller Advanced. Foundational-krav er essentielle krav til processer, it-arkitektur og tekniske foranstaltninger. Advanced-krav omhandler nye teknologier og procedurer for maksimal sikkerhed, men er vanskeligere at implementere.
* ISO27001 ref.: Reference til eventuelle kontroller i ISO27001 inden for SANS CIS-emnet samt reference til krav i Kravkataloget baseret på pågældende ISO27001-kontroller.

Række **(3)** indeholder et eksempel på, hvorledes kolonnerne er udfyldt i Kravkataloget.

|  |
| --- |
|  |
| Bilag 1: Kravkatalog baseret på ISO27001 |
|  |

# Generelle krav

|  |  |
| --- | --- |
| **Krav-ID** | **Kravtekst med henblik på at understøtte efterlevelse af ISO27001 eller tilsvarende risikobaseret tilgang til informationssikkerhed** |
|  | Leverandøren skal med henblik på løbende sikring af informationssikkerhed i tilknytning til levering af Ydelserne opretholde et ledelsessystem for informationssikkerhedsstyring (ISMS) efter den til enhver tid gældende version af ISO27001 eller tilsvarende (national eller international) anerkendt standard baseret på en risikostyringsproces, jf. K2, og i overensstemmelse med de i K3 angivne specifikke krav til Leverandørens ISMS. Leverandøren skal herunder løbende tilpasse sit ISMS, såfremt Leverandørens opdatering af sin risikovurdering, jf. K2, medfører et behov herfor. |
|  | Leverandørens risikostyring af informationssikkerheden i forhold til Leverandørens opfyldelse af Kontrakten skal baseres på en dokumenteret og regelmæssigt opdateret risikovurdering. I relation til Leverandørens risikovurdering gælder det, at:   * Risikovurderingen skal omfatte de Ydelser og de dele af Leverandørens virksomhed, som kan have konsekvenser for informationssikkerheden i Systemet, * Leverandøren som minimum skal opdatere sin risikovurdering én (1) gang årligt, samt i forbindelse med forestående ændringer af Leverandørens egne organisatoriske forhold, forestående ændringer af en eventuel underleverandørs forhold eller forestående ændringer af Systemet, der erfaringsmæssigt kan have konsekvenser for informationssikkerheden for de med Kontrakten forbundne Ydelser, * Leverandøren skal opdatere sin risikovurdering efter påbud fra Kunden om at inkludere en specifik trussel i risikovurderingen, herunder men ikke begrænset til som følge af ændringer i Kundens egen til enhver tid gældende risikovurdering og/eller konsekvensanalyse vedrørende databeskyttelse (DPIA). En sådan af Kunden påbudt opdatering af Leverandørens risikovurdering skal ske inden for en passende frist henset til truslens karakter, samt at * Leverandøren uden ugrundet ophold skal fremsende Leverandørens gældende risikovurdering med henblik på Kundens godkendelse, og således at Kunden til enhver tid har Leverandørens seneste risikovurdering. |
|  | Leverandøren skal sikre, at Leverandørens ISMS som minimum opfylder nedenstående specifikke krav, jf. afsnit 2 baseret på kontroller fra ISO27001, Anneks A, og afsnit 1 baseret på kontroller fra SANS CIS. Nedenstående specifikke krav skal opfyldes uanset implikationerne ved Leverandørens opfyldelse af K1 og K2. |

# Specifikke krav baseret på ISO27001, Anneks A

| Informationssikkerhedspolitikker – ISO27001, Anneks A, punkt 5 | | | |
| --- | --- | --- | --- |
| Retningslinjer for styring af informationssikkerhed – ISO27001, punkt 5.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal fastlægge et sæt politikker for informationssikkerhed i relation til Kontraktens opfyldelse, som skal godkendes af Leverandørens ledelse, offentliggøres og kommunikeres til Leverandørens medarbejdere, eventuelle underleverandører, samt til Kunden, og som skal indgå i Leverandørens ISMS, jf. K1, og understøtte den gældende risikovurdering, jf. K2. | 5.1.1 | N/A |
|  | Leverandørens politikker for informationssikkerhed i relation til Kontraktens opfyldelse skal gennemgås med planlagte mellemrum, og minimum én (1) gang årligt, samt i tilfælde af væsentlige ændringer, herunder i den gældende risikovurdering, jf. K2, for at sikre politikkernes fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet. | 5.1.2 | N/A |
| Organisering af informationssikkerhed – ISO27001, Anneks A, punkt 6 | | | |
| Intern organisering – ISO27001, punkt 6.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal definere og fordele alle ansvarsområder for informationssikkerhed i forbindelse med Kontraktens opfyldelse blandt Leverandørens medarbejdere. | 6.1.1 | N/A |
|  | Leverandøren skal sikre, at modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for informationssikkerhedsbrud i Systemet og i forbindelse med Kontraktens opfyldelse. | 6.1.2 | N/A |
|  | Leverandøren skal opretholde passende kontakt med relevante myndigheder i forbindelse med Kontraktens opfyldelse. | 6.1.3 | SANS CIS 19.  Kravkatalogets afsnit 1.19 |
|  | Leverandøren skal opretholde passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer i forbindelse med Kontraktens opfyldelse. | 6.1.4 | N/A |
|  | Leverandøren skal anvende informationssikkerhed ved projektstyring i forbindelse med Kontraktens opfyldelse uanset projekttype. | 6.1.5 | N/A |
| Mobilt udstyr og fjernarbejdspladser – ISO27001, punkt 6.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal implementere en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr i forbindelse med opfyldelse af Kontrakten. | 6.2.1 | N/A |
|  | Leverandøren skal implementere en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser i forbindelse med Kontraktens opfyldelse. | 6.2.2 | N/A |
| Personalesikkerhed – ISO27001, Anneks A, punkt 7 | | | |
| Før ansættelsen - ISO27001, Anneks A, punkt 7.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal efterprøve baggrunden for alle medarbejdere, der medvirker til Kontraktens opfyldelse, i overensstemmelse med relevante love, forskrifter og etiske regler og under hensyntagen til risikovurderingen, jf. K2. | 7.1.1 | N/A |
|  | Leverandøren skal sikre, at kontrakter med medarbejdere og kontrahenter, der medvirker til Kontraktens opfyldelse, beskriver de pågældendes og Leverandørens ansvar for informationssikkerhed. | 7.1.2 | N/A |
| Under ansættelsen - ISO27001, Anneks A, punkt 7.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001 Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer i relation til Kontraktens opfyldelse. | 7.2.1 | SANS CIS 17.  Kravkatalogets afsnit 1.17 |
|  | Leverandøren skal sikre, at Leverandørens medarbejdere og, hvor det er relevant, underleverandører ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer i det omfang, det er relevant for deres jobfunktion og Kontraktens opfyldelse. | 7.2.2 | SANS CIS 17.  Kravkatalogets afsnit 1.17 |
|  | Leverandøren skal etablere en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud i relation til Kontraktens opfyldelse. | 7.2.3 | N/A |
| Ansættelsesforholdets ophør eller ændring - ISO27001, Anneks A, punkt 7.3 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001 Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at informationssikkerhedsansvar og ‑forpligtelser i relation til Kontraktens opfyldelse, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikeres til medarbejdere eller kontrahenter og håndhæves. | 7.3.1 | N/A |
| Styring af aktiver - ISO27001, Anneks A, punkt 8 | | | |
| Ansvar for aktiver - ISO27001, Anneks A, punkt 8.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal identificere de Informationsaktiver, der anvendes til Kontraktens opfyldelse, og udarbejde og vedligeholde en fortegnelse over disse Informationsaktiver. Leverandøren skal herunder dokumentere Systemet i overensstemmelse med [Bilag [X] - Dokumentation]. | 8.1.1 | SANS CIS 1.  Kravkatalogets afsnit 1.1 |
|  | Leverandøren skal udpege personer og/eller entiteter hos Leverandøren som ejere af hvert Informationsaktiv, der anvendes til Kontraktens opfyldelse. Ejerskabet skal fremgå af fortegnelsen, jf. K19 | 8.1.2 | N/A |
|  | Leverandøren skal identificere, dokumentere og implementere regler for accepteret brug af Informationsaktiver, der anvendes til Kontraktens opfyldelse. | 8.1.3 | N/A |
|  | Leverandøren skal sikre, at alle Leverandørens medarbejdere afleverer alle Informationsaktiver, som har været anvendt til Kontraktens opfyldelse, og som er i deres besiddelse, når deres ansættelse eller aftale ophører. | 8.1.4 | N/A |
| Klassifikation af information - ISO27001, Anneks A, punkt 8.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal foretage en klassifikation af information efter lovmæssige krav, værdi og efter hvor følsom og kritisk informationen er for Kunden i forhold til uautoriseret offentliggørelse eller ændring. | 8.2.1 | N/A |
|  | Leverandøren skal udarbejde og implementere et passende sæt af procedurer til mærkning af information med tilknytning til Kontraktens opfyldelse i overensstemmelse med klassifikationen af information. | 8.2.2 | N/A |
|  | Leverandøren skal udarbejde og implementere procedurer til håndtering af Informationsaktiver, der anvendes til Kontraktens opfyldelse, i overensstemmelse med klassifikationen af information. | 8.2.3 | N/A |
| Mediehåndtering - ISO27001, Anneks A, punkt 8.3 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001 Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal implementere procedurer til styring af bærbare medier i relation til Kontraktens opfyldelse i overensstemmelse med klassifikationen af information (se endvidere afsnit 2.8.2 om malwarebeskyttelse). | 8.3.1 | SANS CIS 8, 13 og 14. Kravkatalogets afsnit 1.8, 1.13 og 1.14 |
|  | Leverandøren skal bortskaffe medier, der har været anvendt til Kontraktens opfyldelse, når der ikke længere er brug for dem, på forsvarlig vis og i overensstemmelse med formelle procedurer. | 8.3.2 | N/A |
|  | Leverandøren skal beskytte medier, der indeholder information relateret til Kontraktens opfyldelse, mod uautoriseret adgang, misbrug eller ødelæggelse under transport i overensstemmelse med klassifikationen af information. | 8.3.3 | N/A |
| Adgangsstyring - ISO27001, Anneks A, punkt 9 | | | |
| Forretningsmæssige krav til adgangsstyring - ISO27001, Anneks A, punkt 9.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal fastlægge, dokumentere og vedligeholde en politik for adgangsstyring i relation til Kontraktens opfyldelse i overensstemmelse med den til enhver tid gældende risikovurdering, jf. K2. | 9.1.1 | SANS CIS 5, 14 og 16. Kravkatalogets afsnit 1.5, 1.14 og 1.16 |
|  | Leverandøren skal sikre, at Brugere og Leverandørens medarbejdere kun har adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte i relation til Kontraktens opfyldelse, jf. også K29 | 9.1.2 | SANS CIS 1, 9, 11 og 12. Kravkatalogets afsnit 1.1, 1.9, 1.11 og 1.12 |
| Administration af brugeradgang - ISO27001, Anneks A, punkt 9.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal implementere en formel procedure for registrering og afmelding af Brugere med henblik på tildeling af adgangsrettigheder i forbindelse med Kontraktens opfyldelse. | 9.2.1 | SANS CIS 16. Kravkatalogets afsnit 1.16 |
|  | Leverandøren skal implementere en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester, der anvendes til Kontraktens opfyldelse. | 9.2.2 | SANS CIS 5. Kravkatalogets afsnit 1.5 |
|  | Leverandøren skal begrænse og styre tildeling og anvendelse af privilegerede adgangsrettigheder i relation til Kontraktens opfyldelse. | 9.2.3 | N/A |
|  | Leverandøren skal styre tildelingen af hemmelige autentifikationsinformationer i relation til Kontraktens opfyldelse ved hjælp af en formel administrationsproces. | 9.2.4 | N/A |
|  | Leverandøren skal sikre, at aktivejere med jævne mellemrum gennemgår Leverandørens medarbejderes adgangsrettigheder og autorisationer i relation til Kontraktens opfyldelse. | 9.2.5 | N/A |
|  | Leverandøren skal inddrage alle medarbejderes og eksterne brugeres adgangsrettigheder og autorisationer til information og informationsbehandlingsfaciliteter i relation til Kontraktens opfyldelse, når deres ansættelsesforhold, kontrakt eller aftale ophører eller skal tilpasses efter en ændring. | 9.2.6 | SANS CIS 5 og 16. Kravkatalogets afsnit 1.5 og 1.16 |
| Brugerens ansvar - ISO27001, Anneks A, punkt 9.3 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at Leverandørens brugere, herunder medarbejdere og eksterne brugere, følger Leverandørens praksis ved anvendelse af hemmelig autentifikationsinformation i forbindelse med Kontraktens opfyldelse. | 9.3.1 | SANS CIS 5 og 16. Kravkatalogets afsnit 1.5 og 1.16 |
| Brugerens ansvar - ISO27001, Anneks A, punkt 9.4 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal begrænse adgangen til information og applikationssystemers funktioner i relation til Kontraktens opfyldelse i overensstemmelse med politikken for adgangsstyring, jf. K29. | 9.4.1 | SANS CIS 5 og 16. Kravkatalogets afsnit 1.5 og 1.16 |
|  | Adgang til systemer og applikationer, der anvendes til Kontraktens opfyldelse, skal styres af en procedure for sikker log-on i overensstemmelse med politikken for adgangsstyring, jf. K29. | 9.4.2 | N/A |
|  | Leverandøren skal sikre, at systemer til administration af adgangskoder i relation til Kontraktens opfyldelse er interaktive og sikrer adgangskoder af høj kvalitet. | 9.4.3 | SANS CIS 16. Kravkatalogets afsnit 1.16 |
|  | Leverandøren skal effektivt begrænse og styre brugen af systemprogrammer, der kan omgå system- og applikationskontroller i relation til Kontraktens opfyldelse. | 9.4.4 | SANS CIS 5. Kravkatalogets afsnit 1.5 |
|  | Leverandøren skal begrænse adgangen til kildekoder til Programmel, der anvendes til Kontraktens opfyldelse. | 9.4.5 | SANS CIS 18. Kravkatalogets afsnit 1.18 |
| Kryptografi - ISO27001, Anneks A, punkt 10 | | | |
| Kryptografiske kontroller - ISO27001, Anneks A, punkt 10.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal udarbejde og implementere en politik for anvendelse af kryptografi til beskyttelse af information i forbindelse med Kontraktens opfyldelse.  Leverandøren skal herunder sikre, at:   * politikken for anvendelse af kryptografi understøtter den gældende risikovurdering, jf. K2, samt at * politikken for anvendelse af kryptografi understøtter K79. | 10.1.1 | SANS CIS 10, 13, 14 og 15. Kravkatalogets afsnit 1.10, 1.13, 1.14 og 1.15 |
|  | Leverandøren skal sikre, at der udarbejdes og implementeres en politik for anvendelse, beskyttelse og levetid for krypteringsnøgler i relation til Kontraktens opfyldelse gennem hele livscyklussen for en krypteringsnøgle. Politikken skal være i overensstemmelse med den gældende risikovurdering, jf. K2. | 10.1.2 | SANS CIS 13. Kravkatalogets afsnit 1.13 |
| Fysisk sikring og miljøsikring - ISO27001, Anneks A, punkt 11 | | | |
| Sikre områder - ISO27001, Anneks A, punkt 11.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal definere og anvende perimetersikring til at beskytte fysiske områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter, der anvendes til Kontraktens opfyldelse. Den anvendte perimetersikring skal afspejle den gældende risikovurdering, jf. K2. | 11.1.1 | N/A |
|  | Leverandøren skal beskytte sikre områder i relation til Kontraktens opfyldelse med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang. | 11.1.2 | N/A |
|  | Leverandøren skal tilrettelægge og etablere fysisk sikring af kontorer, lokaler og faciliteter, der anvendes til Kontraktens opfyldelse. | 11.1.3 | N/A |
|  | Leverandøren skal tilrettelægge og etablere fysisk beskyttelse af faciliteter, der anvendes til Kontraktens opfyldelse, mod naturkatastrofer, ondsindede angreb eller ulykker, herunder brand, oversvømmelse, jordskælv, eksplosion, borgerlige uroligheder og andre former for natur- eller menneskeskabte katastrofer. | 11.1.4 | N/A |
|  | Leverandøren skal tilrettelægge og etablere procedurer for arbejde i sikre fysiske områder i relation til Kontraktens opfyldelse, jf. K54. | 11.1.5 | N/A |
|  | Leverandøren skal sikre, at fysiske adgangssteder, hvor uautoriserede personer kan komme ind på Leverandørens område (fx områder til af- og pålæsning), styres og så vidt muligt adskilles fra informationsbehandlingsfaciliteter, der anvendes til Kontraktens opfyldelse, for at undgå uautoriseret adgang. | 11.1.6 | N/A |
| Udstyr - ISO27001, Anneks A, punkt 11.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at udstyr, der anvendes til Kontraktens opfyldelse, placeres og beskyttes, således at risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes. Placering og beskyttelse af udstyr skal afspejle den gældende risikovurdering, jf. K2. | 11.2.1 | N/A |
|  | Leverandøren skal sikre, at udstyr, der anvendes til Kontraktens opfyldelse, beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger. | 11.2.2 | N/A |
|  | Leverandøren skal sikre, at kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, der anvendes til Kontraktens opfyldelse, beskyttes mod indgreb, interferens og skader. | 11.2.3 | N/A |
|  | Leverandøren skal sikre, at udstyr, der anvendes til Kontraktens opfyldelse, vedligeholdes korrekt og i overensstemmelse med [Bilag [X] Drift] for at sikre dets fortsatte tilgængelighed og integritet. | 11.2.4 | N/A |
|  | Leverandørens udstyr, information og Programmel, der anvendes til Kontraktens opfyldelse, må ikke fjernes fra Leverandørens lokation(er) uden forudgående tilladelse fra Leverandørens ledelse. | 11.2.5 | N/A |
|  | Leverandøren skal sikre, at der etableres sikring af Informationsaktiver, der anvendes til Kontraktens opfyldelse uden for Leverandørens organisation, under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationen, herunder i henhold til den gældende risikovurdering, jf. K2. | 11.2.6 | N/A |
|  | Leverandøren skal sikre, at alt udstyr med lagringsmedier, der anvendes til Kontraktens opfyldelse, verificeres for at sikre, at følsomme data og licensbeskyttet Programmel er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug af udstyret. | 11.2.7 | N/A |
|  | Leverandøren skal sikre, at Leverandørens medarbejderes udstyr, som anvendes til Kontraktens opfyldelse, er passende beskyttet, når dette udstyr er uden opsyn. | 11.2.8 | SANS CIS 16. Kravkatalogets afsnit 1.16 |
|  | Leverandøren skal udarbejde en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter, i det omfang førnævnte udstyr anvendes til Kontraktens opfyldelse. | 11.2.9 | N/A |
| Driftssikkerhed - ISO27001, Anneks A, punkt 12 | | | |
| Driftsprocedurer og ansvarsområder - ISO27001, Anneks A, punkt 12.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal dokumentere driftsprocedurer, der anvendes i forbindelse med Kontraktens opfyldelse, og gøre disse tilgængelige for alle brugere, der har brug for dem. | 12.1.1 | N/A |
|  | Leverandøren skal styre ændringer af Leverandørens organisation, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden i relation til Kontraktens opfyldelse. | 12.1.2 | N/A |
|  | Leverandøren skal overvåge og tilpasse anvendelsen af ressourcer og skal foretage fremskrivninger af fremtidige kapacitetskrav for at sikre, at Systemet fungerer som krævet. [Kapacitetsstyringen skal ske i overensstemmelse med Kontraktens Bilag [X] Drift]. | 12.1.3 | N/A |
|  | Leverandøren skal adskille Udviklings-, Test- og Driftsmiljøer i relation til Kontraktens opfyldelse for at nedsætte risikoen for uautoriseret adgang til eller ændringer af Driftsmiljøet. | 12.1.4 | SANS CIS 18. Kravkatalogets afsnit 1.18 |
| Malwarebeskyttelse - ISO27001, Anneks A, punkt 12.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse implementere kontroller til detektering, forhindring og gendannelse for at beskytte mod malware i kombination med passende brugerbevidsthed. De pågældende procedurer og værktøjer skal afspejle den gældende risikovurdering, jf. K2. | 12.2.1 | SANS CIS 8. Kravkatalogets afsnit 1.8 |
| Backup - ISO27001, Anneks A, punkt 12.3 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at der tages backupkopier af information, Programmel og system-images, der anvendes til Kontraktens opfyldelse, og disse skal testes regelmæssigt i overensstemmelse med den aftalte backuppolitik. | 12.3.1 | SANS CIS 10. Kravkatalogets afsnit 1.10 |
| Logning og overvågning - ISO27001, Anneks A, punkt 12.4 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser i relation til Kontraktens opfyldelse udføres, opbevares og gennemgås regelmæssigt. | 12.4.1 | SANS CIS 6, 12 og 15. Kravkatalogets afsnit 1.6, 1.12 og 1.15 |
|  | Leverandøren skal beskytte logningsfaciliteter og logoplysninger i relation til Kontraktens opfyldelse mod manipulation og uautoriseret adgang. | 12.4.2 | N/A |
|  | Leverandøren skal sikre, at aktiviteter udført af systemadministratorer og systemoperatører i relation til Kontraktens opfyldelse logges, og Leverandøren skal beskytte disse logge og gennemgå disse regelmæssigt. | 12.4.3 | N/A |
|  | Leverandøren skal sikre, at urene i alle relevante informationsbehandlingssystemer, der anvendes til Kontraktens opfyldelse, er synkroniseret til en enkelt referencetidskilde. | 12.4.4 | SANS CIS 6. Kravkatalogets afsnit 1.6 |
| Styring af driftssoftware - ISO27001, Anneks A, punkt 12.5 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal implementere procedurer til styring af Programmel på driftssystemer, der anvendes til Kontraktens opfyldelse. | 12.5.1 | SANS CIS 2. Kravkatalogets afsnit 1.2 |
| Sårbarhedsstyring - ISO27001, Anneks A, punkt 12.6 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal som led i sin risikovurdering, jf. K2, have en dokumenteret proces for løbende indhentning af informationer om aktuelle tekniske sårbarheder i Systemet. Leverandøren skal herunder evaluere Systemets eksponering for sådanne sårbarheder, og den hermed forbundne risiko for informationssikkerheden i Systemet, og iværksætte passende foranstaltninger for at håndtere den tilhørende risiko, jf. K1. | 12.6.1 | SANS CIS 4. Kravkatalogets afsnit 1.4 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse fastlægge og implementere regler om Programmel, som foretages af Leverandørens medarbejdere. | 12.6.2 | SANS CIS 2. Kravkatalogets afsnit 1.2 |
| Overvejelser i forbindelse med audit af informationssystemer - ISO27001, Anneks A, punkt 12.7 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at auditkrav og -aktiviteter i relation til Kontraktens opfyldelse, der indebærer verificering af driftssystemer, planlægges og aftales omhyggeligt for at minimere afbrydelser af Kundens forretningsprocesser. | 12.7.1 | SANS CIS 6, 12 og 15. Kravkatalogets afsnit 1.6, 1.12 og 1.15 |
| Kommunikationssikkerhed - ISO27001, Anneks A, punkt 13 | | | |
| Styring af netværkssikkerhed - ISO27001, Anneks A, punkt 13.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at netværk styres og kontrolleres, således at informationerne i Systemet beskyttes. Leverandøren skal herunder sikre, at styring og kontrol af netværk afspejler den gældende risikovurdering, jf. K2. | 13.1.1 | SANS CIS 1, 9, 11 og 12. Kravkatalogets afsnit 1.1, 1.9, 1.11 og 1.12 |
|  | Leverandøren skal identificere og indgå aftaler om sikkerhedsmekanismer, serviceniveauer og styringskrav til de netværkstjenester, der anvendes til Kontraktens opfyldelse, uanset om disse netværkstjenester leveres internt hos Leverandøren eller er outsourcede. | 13.1.2 | SANS CIS 9. Kravkatalogets afsnit 1.9 |
|  | Leverandøren skal opdele grupper af informationstjenester, brugere og informationssystemer, der anvendes til Kontraktens opfyldelse, i netværk. | 13.1.3 | SANS CIS 11 og 12. Kravkatalogets afsnit 1.11 og 1.12 |
| Informationsoverførsel - Baseret på ISO27001, Anneks A, punkt 13.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at der foreligger formelle overførselspolitikker, -procedurer og -kontroller for at beskytte informationsoverførsel ved brug af alle former for kommunikationsmidler, der anvendes i forbindelse med Kontraktens opfyldelse. | 13.2.1 | N/A |
|  | Leverandøren skal indgå aftaler, der understøtter sikker overførsel af forretningsinformation mellem Leverandøren og eksterne parter i forbindelse med Kontraktens opfyldelse. Leverandøren skal sikre, at aftalerne understøtter den gældende risikovurdering, jf. K2. | 13.2.2 | N/A |
|  | Leverandøren skal træffe særlige sikkerhedsforanstaltninger til beskyttelse af informationer i elektroniske meddelelser, som udveksles i forbindelse med Kontraktens opfyldelse. Leverandøren skal herunder sikre, at de særlige sikkerhedsforanstaltninger understøtter den gældende risikovurdering, jf. K2. | 13.2.3 | SANS CIS 8, 12 og 13. Kravkatalogets afsnit 1.8, 1.12 og 1.13 |
|  | Leverandøren skal identificere, regelmæssigt gennemgå og dokumentere krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler behovet for at beskytte information relateret til Kontraktens opfyldelse, herunder under hensyntagen til den gældende risikovurdering, jf. K2. | 13.2.4 | N/A |
| Anskaffelse, udvikling og vedligeholdelse af systemer - ISO27001, Anneks A, punkt 14 | | | |
| Sikkerhedskrav til informationssystemer - ISO27001, Anneks A, punkt 14.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at informationssikkerhedsrelaterede krav indgår i kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer, som Leverandøren anvender i relation til Kontraktens opfyldelse. | 14.1.1 | N/A |
|  | Leverandøren skal beskytte informationer i forbindelse med applikationstjenester over offentlige netværk, der anvendes i relation til Kontraktens opfyldelse, mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring. | 14.1.2 | SANS CIS 9. Kravkatalogets afsnit 1.9 |
|  | Leverandøren skal beskytte informationer i forbindelse med handelsapplikationer og -tjenester, der anvendes til Kontraktens opfyldelse, for at forhindre ufuldstændig transmission, fejlforsendelser, uautoriseret ændring af meddelelser, uautoriseret offentliggørelse, uautoriseret kopiering eller retransmission af meddelelser. | 14.1.3 | N/A |
| Sikkerhed i udviklings- og hjælpeprocesser - ISO27001, Anneks A, punkt 14.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal fastlægge og anvende regler for udvikling af Programmel, som Leverandøren anvender til Kontraktens opfyldelse. | 14.2.1 | SANS CIS 18. Kravkatalogets afsnit 1.18 |
|  | Leverandøren skal styre ændringer af Programmel inden for udviklingslivscyklussen, som Leverandøren anvender til Kontraktens opfyldelse, ved hjælp af formelle procedurer for ændringsstyring, jf. K61. | 14.2.2 | N/A |
|  | Leverandøren skal gennemgå og teste Applikationer, der er forretningskritiske for Kontraktens opfyldelse, ved ændring af Infrastrukturen for at sikre, at ændringen ikke indvirker negativt på drift og sikkerhed. | 14.2.3 | N/A |
|  | Leverandøren skal sikre, at ændringer i Programmel, som Leverandøren anvender til Kontraktens opfyldelse, begrænses til nødvendige ændringer, og at alle ændringer styres effektivt. | 14.2.4 | SANS CIS 3 og 7. Kravkatalogets afsnit 1.3 og 1.7 |
|  | Leverandøren skal sikre, at principper for udvikling af sikre systemer fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med de implementeringer af informationssystemer, som Leverandøren anvender i relation til Kontraktens opfyldelse. | 14.2.5 | N/A |
|  | Leverandøren skal etablere sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus for så vidt angår Programmel, som Leverandøren anvender til Kontraktens opfyldelse. | 14.2.6 | SANS CIS 18. Kravkatalogets afsnit 1.18 |
|  | Leverandøren skal føre tilsyn med og overvåge systemudviklingsaktiviteter, relateret til Kontraktens opfyldelse, der er outsourcet. | 14.2.7 | N/A |
|  | Leverandøren skal udføre test af sikkerhedsfunktionalitet ved systemudvikling relateret til Kontraktens opfyldelse. | 14.2.8 | SANS CIS 3, 4, 7, 18 og 20. Kravkatalogets afsnit 1.3, 1.4, 1.7, 1.18 og 1.20 |
|  | Leverandøren skal etablere godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner af Programmel, som Leverandøren anvender i relation til Kontraktens opfyldelse. | 14.2.9 | N/A |
| Testdata - ISO27001, Anneks A, punkt 14.3 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal omhyggeligt udvælge testdata og skal sikre, at testdata beskyttes og styres. | 14.3.1 | N/A |
| Leverandørforhold - ISO27001:2013, Anneks A, punkt 15 | | | |
| Informationssikkerhed i leverandørforhold - ISO27001:2013, Anneks A, punkt 15.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001 Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at informationssikkerhedskrav til at minimere risici forbundet med underleverandørers adgang til Informationsaktiver, der anvendes til Kontraktens opfyldelse, aftales med underleverandører og dokumenteres. Leverandøren skal herunder sikre, at informationssikkerhedskravene til underleverandøren er passende henset til den gældende risikovurdering, jf. K2. | 15.1.1 | N/A |
|  | Leverandøren skal fastlægge og aftale alle relevante informationssikkerhedskrav med hver enkelt underleverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere it-infrastrukturkomponenter til information omfattet af Kontrakten. | 15.1.2 | N/A |
|  | Leverandøren skal sikre, at aftaler med underleverandører indeholder krav til håndtering af informationssikkerhedsrisici forbundet med forsyningskæden for IKT-tjenester og ‑produkter, der anvendes til Kontraktens opfyldelse. | 15.1.3 | N/A |
| Styring af leverandørydelser - ISO27001, Anneks A, punkt 15.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal regelmæssigt overvåge, gennemgå og auditere underleverandørydelser, der anvendes til Kontraktens opfyldelse. | 15.2.1 | N/A |
|  | Leverandøren skal styre ændringer af underleverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, -procedurer og ‑kontroller, under hensyntagen til hvor kritiske de involverede forretningsinformationer, -systemer og ‑processer er for Kontraktens opfyldelse, og til en revurdering af risiciene, samt i overensstemmelse med den gældende risikovurdering, jf. K2. | 15.2.2 | N/A |
| Styring af informationssikkerhedsbrud - ISO27001, Anneks A, punkt 16 | | | |
| Styring af informationssikkerhedsbrud og forbedringer - ISO27001, Anneks A, punkt 16.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal fastlægge ledelsesansvar og procedurer for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud relateret til Kontraktens opfyldelse. | 16.1.1 | N/A |
|  | Leverandøren skal sikre, at informationssikkerhedshændelser relateret til Kontraktens opfyldelse rapporteres ad passende ledelseskanaler så hurtigt som muligt. | 16.1.2 | SANS CIS 19. Kravkatalogets afsnit 1.19 |
|  | Leverandøren skal sikre, at medarbejdere og kontrahenter, som bruger informationssystemer og ‑tjenester, der anvendes til Kontraktens opfyldelse, har pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i disse informationssystemer og ‑tjenester. | 16.1.3 | N/A |
|  | Leverandøren skal sikre, at informationssikkerhedshændelser i relation til Kontraktens opfyldelse vurderes, og at det besluttes, om informationssikkerhedshændelser skal klassificeres som informationssikkerhedsbrud. | 16.1.4 | SANS CIS 8. Kravkatalogets afsnit 1.8 |
|  | Leverandøren skal sikre, at informationssikkerhedsbrud i relation til Kontraktens opfyldelse håndteres i overensstemmelse med de dokumenterede procedurer. | 16.1.5 | N/A |
|  | Leverandøren skal sikre, at den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud i forbindelse med Kontraktens opfyldelse. | 16.1.6 | N/A |
|  | Leverandøren skal sikre, at der i forbindelse med Kontraktens opfyldelse defineres og anvendes procedurer til identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som bevis. | 16.1.7 | SANS CIS 6. Kravkatalogets afsnit 1.6 |
| Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring - ISO27001, Anneks A, punkt 17 | | | |
| Informationssikkerhedskontinuitet - ISO27001, Anneks A, punkt 17.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe. | 17.1.1 | N/A |
|  | Leverandøren skal i relation til Kontraktens opfyldelse fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation. | 17.1.2 | N/A |
|  | Leverandøren skal verificere de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten i relation til Kontraktens opfyldelse med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer. | 17.1.3 | N/A |
| Redundans - ISO27001, Anneks A, punkt 17.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at informationsbehandlingsfaciliteter implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskravene for Systemet. | 17.2.1 | N/A |
| Overensstemmelse - ISO27001, Anneks A, punkt 18 | | | |
| Overensstemmelse med lov- og kontraktkrav - ISO27001, Anneks A, punkt 18.1 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal sikre, at alle relevante lov-, myndigheds- og kontraktkrav, samt Leverandørens metode til overholdelse af disse krav, er klart identificeret, dokumenteret og opdateret for hvert informationssystem og for Leverandørens organisation. | 18.1.1 | N/A |
|  | Leverandøren skal implementere passende procedurer til at sikre, at der er overensstemmelse med lov-, myndigheds- og kontraktkrav i relation til immaterielle rettigheder og Leverandørens anvendelse af beskyttet Programmel til Kontraktens opfyldelse. | 18.1.2 | N/A |
|  | Leverandøren skal i relation til Kontraktens opfyldelse beskytte registreringer omfattet af Kontrakten mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overensstemmelse med lov-, myndigheds- og kontraktkrav samt forretningsmæssige krav. | 18.1.3 | N/A |
|  | Leverandøren skal sikre, at privatlivets fred og personoplysninger i relation til Kontraktens opfyldelse beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter. | 18.1.4 | N/A |
|  | Leverandøren skal sikre, at anvendelsen af kryptografi i forbindelse med Kontraktens opfyldelse er i overensstemmelse med alle relevante aftaler, love og forskrifter. | 18.1.5 | SANS CIS 13. Kravkatalogets afsnit 1.13 |
| Gennemgang af informationssikkerhed - ISO27001, Anneks A, punkt 18.2 | | | |
| **Krav-ID** | **Kravtekst baseret på ISO27001, Anneks A** | **ISO27001 Inputkilde** | **SANS CIS ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at Leverandørens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer. | 18.2.1 | SANS CIS 20. Kravkatalogets afsnit 1.20 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at Leverandørens ledere regelmæssigt undersøger, om informationsbehandlingen og ‑procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav. | 18.2.2 | N/A |
|  | Leverandøren skal regelmæssigt undersøge informationssystemer, der anvendes til Kontraktens opfyldelse, for, om de er i overensstemmelse med de relevante informationssikkerhedspolitikker og -standarder. | 18.2.3 | SANS CIS 3, 7 og 20. Kravkatalogets afsnit 1.3, 1.7 og 1.20 |

# Bilag 2: Kravkatalog baseret på SANS CIS

|  |
| --- |
|  |
| Specifikke krav baseret på SANS CIS Critical Security Controls |
|  |

| SANS CIS 1: Inventory of Authorized and Unauthorized Devices | | | | |
| --- | --- | --- | --- | --- |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal aktivt kontrollere (opgøre, spore og korrigere opgørelser) alle hardwareenheder på det netværk, der anvendes til Kontraktens opfyldelse, således at kun autoriserede enheder får adgang, og uautoriserede og ukontrollerede enheder bliver fundet og forhindret i at få adgang. | 1 | Foundational Cyber Hygiene | ISO 8.1.1, 9.1.2 og 13.1.1. Kravkatalogets afsnit 2.4.1, 2.5.1 og 2.9.1 |
|  | Leverandøren skal implementere et identifikationsværktøj til automatiseret opgørelse over hardwareenheder, der anvendes til Kontraktens opfyldelse, og bruge dette identifikationsværktøj til at skabe en oversigt over de hardwareenheder, der er tilsluttet Leverandørens offentlige og private netværk. | 1.1 | Foundational |  |
|  | Hvis Leverandøren i relation til Kontraktens opfyldelse tildeler adresser ved hjælp af Dynamic Host Configuration Protocol (DHCP) eller tilsvarende, skal Leverandøren installere DHCP-serverlogning og anvende disse oplysninger til at forbedre oversigten over hardwareenheder og til at opdage ukendte hardwareenheder. | 1.2 | Foundational |  |
|  | Leverandøren skal sikre, at oversigten over hardwareenheder i relation til Kontraktens opfyldelse automatisk opdateres, når nye godkendte hardwareenheder tilsluttes netværket. | 1.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse føre en oversigt over hardwareenheder, der er tilsluttet Leverandørens netværk, og over selve netværksenhederne, og Leverandøren skal på Kundens anmodning som minimum oplyse netværksadressen, maskinens navn(e), formålet med hver enkelt enhed, hver enheds ansvarlige ejer og afdelingen forbundet med hver enkelt enhed. | 1.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse implementere netværksniveauautentifikation via 802.1x-standarden eller tilsvarende for at begrænse og kontrollere, hvilke hardware-enheder der kan tilsluttes netværket. Netværksniveauautentifikationen skal være sammenkoblet med oversigten over godkendte hardwareenheder, jf. K118, således at det kan konstateres, om der er tale om autoriserede eller uautoriserede hardwareenheder. | 1.5 | Foundational |  |
|  | Leverandøren skal benytte sig af klientcertifikater i relation til Kontraktens opfyldelse til at validere og verificere hardware-enheder, før de tilsluttes det private netværk. | 1.6 | Advanced |  |
| SANS CIS 2: Inventory of Authorized and Unauthorized Software | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal aktivt kontrollere (opgøre, spore og korrigere opgørelser) al Programmel på det netværk, der anvendes til Kontraktens opfyldelse, således at kun autoriseret Programmel er installeret og kan afvikles, og således at uautoriseret og ukontrolleret Programmel opdages og forhindres i at blive installeret og afviklet. | 2 | Foundational Cyber Hygiene | ISO 12.5.1 og 12.6.2. Kravkatalogets afsnit 2.8.5 og 2.8.6 |
|  | Leverandøren skal opstille en liste over godkendt Programmel og de godkendte versioner, der er brug for i relation til Kontraktens opfyldelse for servere, arbejdsstationer og bærbare computere i alle varianter og brugssituationer. Denne liste skal overvåges af et filintegritetskontrolværktøj for at bekræfte, at listen over godkendt Programmel ikke ændres uden gyldig autorisation. | 2.1 | Foundational |  |
|  | Leverandøren skal implementere hvidlistning af Programmel i relation til Kontraktens opfyldelse, så der kun afvikles Programmel, hvis det findes på hvidlisten, og afvikling af al andet Programmel forhindres.  Hvidlisten kan gøres meget omfattende (som de tilgængelige hvidlister fra kommercielle hvidliste-leverandører), så brugere ikke unødigt begrænses ved brug af almindeligt anvendt Programmel. Omvendt kan en hvidliste gøres ganske snæver i forbindelse med systemer til særlige formål, der kun kræver et lille antal af programmer for at opfylde de krævede og nødvendige formål. | 2.2 | Foundational |  |
|  | Leverandøren skal implementere værktøjer til opgørelse af Programmel, der anvendes til Kontraktens opfyldelse, som dækker servere, arbejdsstationer og bærbare computere.  Programmelopgørelsessystemet skal kunne spore versionen på både det underliggende operativsystem og de installerede Applikationer.  Programmelopgørelsessystemet skal endvidere være bundet op på opgørelsen over hardware, jf. K118, således at alle hardwareenheder og tilhørende Programmel kan spores fra et enkelt sted. | 2.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at virtuelle maskiner og/eller systemer, der er isoleret fra det almindelige driftsnetværk, anvendes til at isolere og køre Applikationer, som, baseret på en højere risiko, jf. K2, ikke må installeres på det almindelige driftsnetværk. | 2.4 | Advanced |  |
| SANS CIS 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal etablere, implementere og aktivt kontrollere (spore, indberette, korrigere) sikkerhedskonfigurationer for it-miljøer (bærbare computere, servere og arbejdsstationer), der anvendes til Kontraktens opfyldelse, ved stringent konfigurations- og ændringsstyring med henblik på at forhindre angribere i at udnytte sårbare services og indstillinger. | 3 | Foundational Cyber Hygiene | ISO 14.2.4, 14.2.8 og 18.2.3. Kravkatalogets afsnit 2.10.2 og 2.14.2 |
|  | Leverandøren skal etablere standard sikkerhedskonfigurationer for operativsystemer og Applikationer i relation til Kontraktens opfyldelse. Standardiserede images skal udgøre hærdede versioner af operativsystemer og Applikationer. Disse images skal godkendes og opdateres regelmæssigt for at opdatere deres sikkerhedskonfiguration i lyset af de seneste sårbarheder og angrebsvektorer. | 3.1 | Foundational |  |
|  | Leverandøren skal følge en stram konfigurationsstyring og opbygge et sikkerheds-image, der skal anvendes til alle nye installationer af Programmel, der tages i brug i forbindelse med Kontraktens opfyldelse.  Enhver eksisterende installation, der bliver kompromitteret, skal genkonfigurereres med det relevante sikkerheds-image.  Regelmæssige opdateringer af eller undtagelser fra det relevante image skal integreres i Leverandørens ændringsstyringsprocesser, jf. K61.  Leverandøren skal udarbejde sikkerheds-images til arbejdsstationer, servere og andre systemtyper, der anvendes til Kontraktens opfyldelse. | 3.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse opbevare master-images på forsvarligt konfigurerede servere, valideret med integritetskontrolværktøjer, der kan foretage kontinuerlig inspektion, og ændringsstyringsværktøjer for at sikre, at det kun er muligt at foretage autoriserede ændringer i images.  Alternativt kan disse master-images lagres i offline maskiner, fysisk isoleret fra driftsnetværket, således at images kopieres til sikre medier for at kunne flytte dem mellem image-lagerservere og driftsnetværket. | 3.3 | Foundational |  |
|  | Leverandøren skal udføre al fjernadministration af udstyr, der anvendes til Kontraktens opfyldelse, via sikre forbindelser. Protokoller, der ikke aktivt understøtter stærk kryptering, må udelukkende anvendes, såfremt de anvendes via en sekundær krypteringsforbindelse. | 3.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende værktøjer til kontrol af filintegritet for at sikre, at kritiske systemfiler (herunder følsomme system- og applikationsfiler, biblioteker og konfigurationer) ikke er blevet ændret.  Leverandøren skal sikre, at sådanne værktøjer kan:   1. redegøre for rutinemæssige og forventede ændringer; 2. fremhæve og underrette om usædvanlige eller uventede ændringer; 3. vise historik over konfigurationsændringer; og 4. identificere brugeren, der foretog ændringen (herunder den oprindeligt benyttede konto i tilfælde af en bruger-id-ændring).   Disse integritetskontroller skal identificere mistænkelige systemændringer såsom:   1. ejer- og tilladelsesændringer i filer eller mapper; 2. anvendelsen af alternative datastrømme, som kunne anvendes til at skjule ondsindede handlinger; og 3. indførelsen af ekstra filer i centrale systemområder (som kunne indikere angriberes ondsindede efterladen af data eller uhensigtsmæssigt tilføjelse af yderligere filer under batch distributionsprocesser). | 3.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse implementere og teste et automatiseret konfigurationsovervågningssystem, der kontrollerer alle fjerntestbare sikkerhedskonfigurationselementer og udsender en alarm, hvis der foretages uautoriserede ændringer. Dette omfatter detektering af nye *listening ports*, nye administratorprofiler, ændringer i gruppe- og lokalpolitikker (hvis relevant) og nye tjenester, der kører på et system.  Leverandøren skal sikre, at der, så vidt muligt, altid bruges værktøjer i relation til Kontraktens opfyldelse, som er i overensstemmelse med Security Content Automation Protocol (SCAP) eller tilsvarende, for at strømline rapporteringen og integrationen. | 3.6 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse implementere systemkonfigurationsstyringsværktøjer, der automatisk vil håndhæve og omstille konfigurationsindstillinger inden for planlagte regelmæssige intervaller.  Værktøjerne skal være i stand til at udløse en omstilling af konfigurationsindstillingerne på et planlagt, manuelt eller hændelsesbaseret grundlag. | 3.7 | Foundational |  |
| SANS CIS 4: Continuous Vulnerability Assessment and Remediation | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse løbende tilvejebringe, vurdere og handle på nye oplysninger for at afdække sårbarheder, afhjælpe disse og dermed minimere risikoen for informationssikkerhedsbrud. | 4 | Foundational Cyber Hygiene | ISO 12.6.1 og 14.2.8. Kravkatalogets afsnit 2.8.6 og 2.10.2 |
|  | Leverandøren skal som minimum ugentligt køre en automatiseret sårbarhedsscanning på alle systemer på netværket, der anvendes til Kontraktens opfyldelse, og levere lister over de mest kritiske sårbarheder i prioriteret rækkefølge til alle ansvarlige systemadministratorer sammen med en risiko score, der sammenligner de forskellige systemadministratorers og afdelingers effektivitet i at reducere risikoen.  Leverandøren skal herunder anvende en sårbarhedsscanner, der scanner for både kodebaserede sårbarheder (som angivet i Common Vulnerabilities and Exposures entries eller tilsvarende) og konfigurationsbaserede sårbarheder (som angivet i the Common Configuration Enumeration Project eller tilsvarende). | 4.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sammenholde hændelseslogs med oplysningerne fra sårbarhedsscanningerne med henblik på at:   1. kontrollere og verificere, at resultaterne af de regelmæssige sårbarhedsscanninger bliver logget korrekt. 2. sammenholde sikkerhedshændelser med forudgående sårbarhedsscanningsresultater for at kunne afgøre, om det givne angreb blev rettet mod et mål, der var registreret som værende sårbart. | 4.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udføre sårbarhedsscanning i autentificeret tilstand enten med agenter, der kører lokalt på hvert slutsystem for at analysere sikkerhedskonfigurationen, eller med eksterne scannere, der er tildelt administrative rettigheder til det system, der afprøves.  Leverandøren skal bruge dedikerede konti til autentificerede sårbarhedsscanninger, der ikke må anvendes til andre administrative aktiviteter, og som bør være forbundet til bestemte maskiner med specifikke IP-adresser.  Endelig skal Leverandøren sikre, at kun autoriserede medarbejdere har adgang til brugergrænsefladen for sårbarhedsmanagement-systemet, og at rettigheder er kontrolleret for hver enkelt bruger. | 4.3 | Foundational |  |
|  | Leverandøren skal tilmelde sig en sårbarhedsunderretningstjeneste for hele tiden at være opmærksom på nye sårbarheder og bruge denne tjenestes oplysninger til at opdatere organisationens sårbarhedsscanningsaktiviteter i relation til Kontraktens opfyldelse mindst én gang om måneden.  Alternativt skal det sikres, at de sårbarhedsscanningsværktøjer, der anvendes, jævnligt opdateres med alle relevante vigtige sikkerhedshuller. | 4.4 | Foundational |  |
|  | Leverandøren skal implementere automatiske patch management- og opdateringsværktøjer til Programmel, der anvendes til Kontraktens opfyldelse, hvor sådanne værktøjer er tilgængelige og sikre.  Leverandøren skal sikre, at patches installeres på alt Programmel, der anvendes til Kontraktens opfyldelse, medmindre andet aftales med Kunden. | 4.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse overvåge hændelseslogs, der er forbundet med enhver scanningsaktivitet og tilhørende administratorkonti, for at sikre, at disse scanningsaktiviteter sker inden for begrænsede tidsrammer, hvor sådanne scanninger medfører mindst mulig gene. | 4.6 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sammenligne resultaterne fra back-to-back sårbarhedsscanninger for at kontrollere, at sårbarhederne blev håndteret, enten ved patching, ved gennemførelse af en kompenserende kontrol eller ved dokumentation og accept af en rimelig forretningsmæssig risiko.  Leverandøren skal herunder sikre, at en sådan accept af forretningsmæssige risici i forbindelse med eksisterende sårbarheder evalueres regelmæssigt for at afgøre, om nyere kompenserende kontroller eller efterfølgende patches kan håndtere sårbarheder, der tidligere er accepteret, eller hvis forholdene har ændret sig, kan øge risikoen. | 4.7 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse etablere en proces dedikeret til at risikovurdere sårbarheder baseret på sårbarhedens udnyttelsesmuligheder og potentielle konsekvenser, og segmenteret i passende grupper af Informationsaktiver (fx DMZ-servere, interne netværk, servere, computere mv.). Denne dedikerede proces skal indgå i den samlede risikovurdering, jf. K2.  Leverandøren skal patche de farligste sårbarheder i relation til Kontraktens opfyldelse først. En trinvis udrulning anvendes herefter til at minimere effekten på Systemets tilgængelighed. Leverandøren skal desuden etablere en forventet patching-tidsplan baseret på risikovurderingsniveauet. | 4.8 | Foundational |  |
| SANS CIS 5: Controlled Use of Administrative Privileges | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal anvende processer og værktøjer til at kontrollere (spore, forhindre og korrigere) brug, tildeling og konfiguration af administratorrettigheder på computere, netværk og Applikationer, der anvendes til Kontraktens opfyldelse. | 5 | Foundational Cyber Hygiene | ISO 9.1.1, 9.2.2 – 9.2.6, 9.3.1 og 9.4.1 – 9.4.4. Kravkatalogets afsnit 2.5.1, 2.5.2, 2.5.3 og 2.5.4 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse minimere brugen af administratorkonti og kun anvende administratorkonti, når det er nødvendigt. Leverandøren skal endvidere implementere specifik audit af brugen af administratorkonti samt monitorere for unormal adfærd med administratorkonti. | 5.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende automatiserede værktøjer til opgørelse af alle administratorkonti samt validere, at alle personer med administrative rettigheder på computere og servere er blevet godkendt af en leder. | 5.2 | Foundational |  |
|  | Leverandøren skal sikre, at alle standardadgangskoder til Programmel, Applikationer, operativsystemer, routere, firewalls, trådløse netværksadgangspunkter samt andre tilsvarende systemer, der anvendes til Kontraktens opfyldelse, ændres forud for idriftsættelsen for dermed at sikre, at adgangskodekvaliteten svarer til administratorkonto-niveau. | 5.3 | Foundational |  |
|  | Leverandøren skal konfigurere systemer, der anvendes til Kontraktens opfyldelse, til at logge samt udsende en notifikation, når en konto tilføjes eller fjernes fra et domænes administratorgruppe, eller når en ny lokal administratorbrugerkonto tilføjes. | 5.4 | Foundational |  |
|  | Leverandøren skal konfigurere systemer, der anvendes til Kontraktens opfyldelse, til at logge samt udsende en notifikation, hver gang et log-in på en administratorbrugerkonto mislykkes. | 5.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende multifaktor autentifikation, for alle administratorkonti, inkl. domæneadministratorkonti. | 5.6 | Foundational |  |
|  | I tilfælde, hvor multifaktor autentifikation ikke understøttes, skal Leverandøren sikre, at brugerkonti skal anvende lange passwords (dvs. længere end 14 tegn) i relation til Kontraktens opfyldelse. | 5.7 | Foundational |  |
|  | I forbindelse med anvendelsen af administratorrettigheder i relation til Kontraktens opfyldelse, skal Leverandøren sikre, at administratorer først skal logge på ved hjælp af en fuldt logget, ikke-administrativ konto. Efterfølgende skal administratoren, når denne er logget på uden særlige administratorrettigheder, overgå til administratorrettigheder ved hjælp af et værktøj. | 5.8 | Foundational |  |
|  | Administratorer skal i relation til Kontraktens opfyldelse bruge en særlig computer til alle administrative opgaver og opgaver, der kræver særligt privilegeret adgang. Denne computer skal være isoleret fra Leverandørens primære netværk og ikke have adgang til internettet. Maskinen må hverken bruges til at læse e-mails, oprette dokumenter eller surfe på internettet. | 5.9 | Advanced |  |
| SANS CIS 6: Maintenance, Monitoring, and Analysis of Audit Logs | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal indsamle, administrere og analysere hændelseslogninger i relation til Kontraktens opfyldelse med det formål at opdage et angreb og forstå samt genoprette Systemet efter et angreb. | 6 | N/A | ISO 12.4.1 – 12.4.4 og 12.7.1. Kravkatalogets afsnit 2.8.4 og 2.8.7 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse, benytte mindst to tidskilder, der er synkroniseret med referencetidskilden, jf. K69, hvorfra alle servere og netværksudstyr regelmæssigt kan foretage tidssynkronisering, så tidsstempler i logfiler er konsistente. | 6.1 | Foundational |  |
|  | Leverandøren skal verificere indstillingerne for hændelseslogninger for hvert Informationsaktiv, der anvendes til Kontraktens opfyldelse, og det Programmel, som er installeret herpå, for på den måde at sikre, at logfiler indeholder dato, tidsstempel, kildeadresser, destinationsadresser samt andre elementer relevant for hver pakke og/eller transaktion.  Leverandøren skal sikre, at logfilerne registreres i et standardiseret format i relation til Kontraktens opfyldelse, såsom de formater, der er skitseret i Common Event Expressions eller tilsvarende. Hvis logfiler ikke kan genereres i et standardiseret format, kan et log-normaliseringsværktøj anvendes til at konvertere logs til et sådant format. | 6.2 | Foundational |  |
|  | Leverandøren skal sikre, at alle systemer, der lagrer logs i relation til Kontraktens opfyldelse, har tilstrækkelig plads til, at logfilerne genereres regelmæssigt, således at logfilerne ikke fylder pladsen op mellem log-rotationsintervaller. Leverandøren skal desuden sikre, at logfilerne regelmæssigt arkiveres og underskrives digitalt. | 6.3 | Foundational |  |
|  | Leverandøren skal sikre, at sikkerhedspersonale og/eller systemadministratorer regelmæssigt udarbejder rapporter over uregelmæssigheder i logfiler i relation til Kontraktens opfyldelse. Sikkerhedspersonalet og/eller systemadministratorerne skal derefter aktivt gennemgå uregelmæssighederne og registrere deres resultater. | 6.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse konfigurere netværksperimeterenheder, herunder firewalls, netværksbaserede IPS samt indgående og udgående proxyer til effektivt at logge af al trafik (både tilladt og blokeret), som en enhed måtte modtage. | 6.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse implementere SIEM- (Security Information and Event Management) eller logningsanalyseringsværktøjer til sammenlægning og konsolidering af logs fra flere maskiner samt sammenligning og analyse af logs.  Ved hjælp af SIEM-værktøjet skal Leverandøren beskrive profiler for sædvanlige hændelser i givne systemer, så systemadministratorerne og sikkerhedspersonale kan fokusere på at detektere usædvanlige hændelser, undgå falske positiver, hurtigere identificere uregelmæssigheder og forhindre, at uforholdsmæssigt store ressourcer bruges på systemanalyser ved ubetydelige alarmer. | 6.6 | Foundational |  |
| SANS CIS 7: Email and Web Browser Protections | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse minimere angrebsfladen og mulighederne for, at angribere kan manipulere medarbejderes adfærd via interaktion med webbrowsere og e-mailsystemer. | 7 | N/A | ISO 14.2.4, 14.2.8 og 18.2.3. Kravkatalogets afsnit 2.10.2 og 2.14.2 |
|  | Leverandøren skal sikre, at kun fuldt understøttede webbrowsere og e-mailklienter anvendes i relation til Kontraktens opfyldelse, og at der kun bruges den nyeste version af de browsere, som udbyderen har stillet til rådighed, med henblik på at udnytte de nyeste sikkerhedsfunktioner og rettelser. | 7.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse afinstallere eller deaktivere alle unødvendige eller uautoriserede browsere, e-mailklient-plugins og add-on-applikationer og sikre, at alle plugins benytter applikation/URL-hvidlister og kun tillader brug af en sådan applikation i forbindelse med forhåndsgodkendte domæner. | 7.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse begrænse brugen af unødvendige script-sprog i alle web-browsere og e-mail-klienter. | 7.3 | Foundational |  |
|  | Leverandøren skal logge alle URL-anmodninger fra alle Leverandørens systemer, der anvendes til Kontraktens opfyldelse, uanset om det sker onsite eller fra en bærbar enhed, for at identificere potentielt skadelig aktivitet og hjælpe sikkerhedspersonale med at identificere potentielt kompromitterede systemer. | 7.4 | Foundational |  |
|  | Leverandøren skal implementere to separate browserkonfigurationer i alle systemer, der anvendes til Kontraktens opfyldelse. Den ene konfiguration, der skal bruges til almindelig webbrowsing, skal deaktivere alle plugins, unødvendige script-sprog og generelt være konfigureret til begrænset funktionalitet. Den anden konfiguration skal give mulighed for mere browserfunktionalitet, men skal kun bruges til at få adgang til bestemte websteder, der kræver brugen af en sådan funktionalitet. | 7.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse vedligeholde og håndhæve netværksbaserede URL-filtre, der begrænser et systems evne til at oprette forbindelse til hjemmesider, der ikke er godkendt af Leverandøren. Leverandøren skal herunder:   1. abonnere på URL-kategoriseringstjenester for at sikre, at Leverandøren er ajourført med de seneste hjemmesidekategoriseringsdefinitioner, der er til rådighed; 2. blokere ikke-kategoriserede hjemmesider som standard; og 3. håndhæve denne filtrering for alle installationer, der anvendes, uanset om de befinder sig fysisk hos Leverandøren eller ej. | 7.6 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse implementere Sender Policy Framework (SPF) med henblik på at mindske risikoen for spam og hoaxes ved at indsætte SPF-poster i DNS og muliggøre receiver-side-verifikation i mailservere. | 7.7 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse scanne og blokere alle vedhæftede filer i e-mails, der lander i Leverandørens e-mail-gateway, hvis de indeholder skadelig kode eller filtyper, der er unødvendige. Scanningen skal ske, før e-mailen lander i Leverandørens brugeres indbakker. Dette omfatter både e-mailindholdsfiltrering og webindholdsfiltrering. | 7.8 | Foundational |  |
| SANS CIS 8: Malware Defenses | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kontrollere installation, spredning og eksekvering af skadelig kode fra flere steder i Infrastrukturen, samt optimere brugen af automatisering for at muliggøre hurtig opdatering af beskyttelsesværktøjer, dataindsamling og iværksættelse af korrigerende handlinger. | 8 | N/A | ISO 8.3.1, 12.2.1 og 13.2.3. Kravkatalogets afsnit 2.4.3, 2.8.2 og 2.9.2 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende automatiserede værktøjer til løbende at overvåge arbejdsstationer, servere og bærbare enheder ved hjælp af anti-virus-, anti-spyware-, personlige firewalls- og host-baseret IPS-funktionalitet. Leverandørens skal herunder sikre, at samtlige detekteringer af malware rapporteres til Leverandørens anti-malware-administrationsværktøjer og hændelseslog-servere. | 8.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende anti-malware-software med en centraliseret infrastruktur, der indsamler oplysninger omkring filers omdømme, eller lade administratorer manuelt installere opdateringer på alle maskiner.  Leverandøren skal desuden sikre, at der i relation til Kontraktens opfyldelse anvendes et automatiseret system, der kan kontrollere og verificere, at hver enkelt maskine har modtaget sin signaturopdatering, efter en sådan opdatering er blevet sendt ud. | 8.2 | Foundational |  |
|  | Leverandørens skal i relation til Kontraktens opfyldelse begrænse anvendelsen af eksterne medier, til eksterne medier med et godkendt formål. Leverandøren skal herunder:   1. overvåge anvendelse og forsøg på anvendelsen af ikke-ledelsesgodkendt eksternt udstyr; 2. konfigurere computere, arbejdsstationer og servere til ikke automatisk at køre indhold fra bærbare medier; 3. foretage en anti-malware-scanning af bærbare medier før anvendelse af disse. | 8.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende anti-udnyttelsesfunktioner, såsom Data Execution Prevention (DEP), Adresse Space Layout Randomization (ASLR), virtualization/containerization eller tilsvarende. | 8.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse bruge netværksbaserede anti-malware-værktøjer til at identificere eksekverbare filer i al netværkstrafik samt anvende teknikker, udover signaturbaseret registrering, til at identificere og frasortere skadeligt indhold, før dette når frem til sit mål. | 8.5 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udføre logning af Domain Name System (DNS) forespørgsler for at opspore host-navne-opslag af kendte skadelige C2 (Command & Control)-domæner. | 8.6 | Foundational |  |
| SANS CIS 9: Limitation and Control of Network Ports, Protocols, and Services | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kontrollere (spore, begrænse og korrigere) den løbende operative brug af porte, protokoller og tjenester på netværksenheder med det formål at minimere sårbarheder over for angreb. | 9 | N/A | ISO 9.1.2, 13.1.1, 13.1.2 og 14.1.2. Kravkatalogets afsnit 2.5.2, 2.9.1 og 2.10.1 |
|  | Leverandøren skal sikre, at kun porte, protokoller og tjenester med bekræftede forretningsmæssige formål anvendes til Kontraktens opfyldelse. | 9.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende værtbaserede firewalls eller port-filtrerings-værktøjer på slutsystemer med en standardafvisning af al datatrafik med undtagelse af de tjenester og porte, der specifikt er godkendt. | 9.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse regelmæssigt foretage automatiske scanninger af porte i forhold til samtlige nøgleservere og holde dem op imod en effektiv baseline. Hvis en ændring, der ikke fremgår af Leverandørens godkendte baseline, opdages, skal der genereres en advarsel herom, og ændringen skal vurderes. | 9.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kontrollere enhver server, der er synlig fra internettet eller fra et upålideligt netværk, og hvis den ikke er nødvendig for at opfylde forretningsmæssige formål, skal den flyttes til en intern VLAN og have en privat adresse. | 9.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at kritiske tjenester køres på separate fysiske eller logiske host-maskiner, såsom DNS-, fil-, mail-, web- og databaseservere. | 9.5 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende applikationsfirewalls foran alle kritiske servere for at kontrollere og validere den indkomne datatrafik til serveren. Uautoriserede tjenester eller datatrafik skal blokeres og generere en alarm. | 9.6 | Advanced |  |
| SANS CIS 10: Data Recovery Capability | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende processer og værktøjer til behørig backup af kritiske informationer med en velafprøvet metodik for, hvordan information effektivt kan gendannes. | 10 | N/A | ISO 10.1.1 og 12.3.1. Kravkatalogets afsnit 2.6.1 og 2.8.3 |
|  | Leverandørens skal i relation til Kontraktens opfyldelse sikre, at:   1. der automatisk bliver foretaget backup mindst én gang om ugen, og endnu oftere for så vidt angår følsomme oplysninger; 2. der over tid laves flere forskellige backup-filer, således at der i tilfælde af malware-infektion kan ske gendannelse fra en version, der vurderes at ligge forud for infektionshændelsen.   For at sikre evnen til hurtigt at kunne retablere et system fra en backup-fil, skal styresystemet, Programmellet og dataene på en maskine indgå i den samlede backup-procedure. Disse tre komponenter behøver ikke at være inkluderet i samme backup-fil eller bruge det samme backup-software. | 10.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse teste data på backup-medier regelmæssigt ved at udføre en datagendannelse for at sikre, at backup’en fungerer efter hensigten. | 10.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at backups er fuldstændigt beskyttet ved enten fysisk sikkerhed eller kryptering, både ved opbevaring, og når de flyttes på tværs af netværk. Dette omfatter også remote-backup og cloud-tjenester. | 10.3 | Foundational |  |
|  | Leverandøren skal sikre, at nøglesystemer, der anvendes til Kontraktens opfyldelse, har mindst én backup-destination, som ikke er konstant adresserbar via styresystemsopkald. | 10.4 | Foundational |  |
| SANS CIS 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse etablere, implementere og aktivt kontrollere (spore, indberette og korrigere) sikkerhedskonfigurationen på Kundens it-miljøer via en stringent konfigurationsstyring og ændringshåndtering med henblik på at forhindre angribere i at udnytte sårbarheder, herunder sårbare tjenester og indstillinger. | 11 | N/A | ISO 9.1.2, 13.1.1, og 13.1.3. Kravkatalogets afsnit 2.5.1 og 2.9.1 |
|  | Leverandøren skal sammenligne Leverandørens firewall-, router- og switch-sikkerhedskonfiguration, der anvendes af Leverandøren til Kontraktens opfyldelse, med sikkerhedskonfigurationsstandarder for hver enkelt type netværksenhed. Sikkerhedskonfiguration af sådanne enheder skal dokumenteres, revideres og godkendes af Leverandørens ændringstilsyn.  Enhver afvigelse fra standardkonfigurationen eller opdateringer hertil skal dokumenteres og godkendes, jf. K61. | 11.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at alle nye konfigureringsregler, som går videre end et almindeligt hærdet basiskonfigurationsniveau, der tillader trafik gennem netværkssikkerhedsenheder, såsom firewalls og netværksbaserede IPS, dokumenteres og registreres i et konfigurationsstyringssystem. Ved registrering af nye konfigurationsregler i relation til Kontraktens opfyldelse angives:   1. en specifik forretningsmæssig begrundelse for hver ændring, 2. navnet på den specifikke person, der har ansvaret for det pågældende forretningsmæssige behov, og 3. den forventede varighed af det givne behov. | 11.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende automatiserede værktøjer til at verificere standardenhedskonfigurationer og registrere ændringer. Alle ændringer til disse filer skal logges og automatisk indberettes til sikkerhedspersonalet. | 11.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kontrollere netværksenheder ved hjælp af to-faktor-autentificering og krypterede sessioner. | 11.4 | Foundational |  |
|  | Leverandøren skal sikre, at den seneste stabile version af enhver sikkerhedsrelateret opdatering er installeret på alle netværksenheder, der anvendes til Kontraktens opfyldelse. | 11.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at netværksteknikere anvender en særskilt maskine til alle administrative opgaver samt opgaver, der kræver særlige administratorrettigheder.  En sådan maskine skal isoleres fra Leverandørens almindelige netværk og ikke være opkoblet til internettet, og Leverandøren skal sikre, at maskinen ikke anvendes til almindelige opgaver, såsom e-mail, tekstbehandling eller internetsurfing. | 11.6 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse administrere netværksinfrastruktur via netværksforbindelser, der er adskilt fra Leverandørens forretningsmæssige brug af netværk, ved hjælp af separate VLAN-tilslutninger eller ved hjælp af separate fysiske netværkstilslutninger for managementsessioner for netværksenheder. | 11.7 | Foundational |  |
| SANS CIS 12: Boundary Defense | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kontrollere (spore, forhindre og korrigere) strømmen af informationsoverførsler mellem netværk med forskellige tillidsniveauer med særligt fokus på sikkerhedsskadeligt data. | 12 | N/A | ISO 9.1.2, 12.4.1, 12.7.1, 13.1.1, 13.1.3 og 13.2.3. Kravkatalogets afsnit 2.5.1, 2.8.4, 2.8.7, 2.9.1 og 2.9.2 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse nægte kommunikation med (eller begrænse datastrømmen til) kendte skadelige IP-adresser (”sortliste”) eller begrænse adgangen til kun at omfatte sider, som Leverandøren har tillid til (”hvidliste”).  Leverandøren skal udføre regelmæssige tests ved at sende data-pakker fra ”bogon IP-adresser” (dvs. falske, non-routable eller ubrugte IP-adresser) ind i netværket for at kontrollere, at datapakkerne ikke transmitteres gennem netværkets perimetre. | 12.1 | Foundational |  |
|  | Ved anvendelsen af DMZ-netværk i relation til Kontraktens opfyldelse skal Leverandøren konfigurere et monitoreringssystem, der som minimum registrerer information om datapakkernes topmargintekst eller den fulde topmargintekst, hvilket vil være at foretrække, for datatrafik, der passerer gennem netværket. Leverandøren skal sikre, at denne trafik transmitteres til et korrekt konfigureret informationssikkerhedshændelsesstyringssystem (”SIEM”) eller andet logningsanalyseringssystem, så information om hændelser kan samkøres (korreleres) fra alle enheder på netværket. | 12.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende netværksbaserede IDS-sensorer på internet- og extranetbaserede DMZ-systemer og ‑netværk, der søger efter usædvanlige angrebsmekanismer og skal opdage kompromittering af disse systemer. Disse netværksbaserede IDS-sensorer kan anvende signaturer, netværksadfærdsanalyse eller andre datatrafikanalysemekanismer til at opfange disse angreb. | 12.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at netværksbaserede IPS-enheder anvendes til at komplementere IDS ved at blokere kendte ondsindede signaturer eller adfærd, der kendetegner et potentielt angreb. I forbindelse med Leverandørens evaluering af netværksbaserede IPS-produkter i relation til Kontraktens opfyldelse skal Leverandøren overveje IPS-produkter, der anvender andre teknikker end den signaturbaserede, såsom virtual machine eller sandkassebaserede tilgange. | 12.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse designe og implementere netværksperimetre, således at al udgående netværkstrafik til internettet går igennem mindst en proxyserver til filtrering i applikationslaget. Proxyserveren skal understøtte dekrypteret netværkstrafik, logge individuelle TCP-sessioner samt blokere specifikke URL'er, domænenavne og IP-adresser med det formål at oprette en sortliste og få indført hvidlister over tilladte websteder, der kan tilgås via proxyserveren samtidig med, at alle andre websteder blokeres. Leverandøren skal sikre, at udgående trafik til internettet tvinges via en godkendt proxyserver på Leverandørens perimetre. | 12.5 | Foundational |  |
|  | Leverandøren skal sikre, at alle fjernadgangstyper (herunder VPN, dial-up og lignende adgangstyper), der anvendes til Kontraktens opfyldelse, kræver brug af to-faktor autentifikation. | 12.6 | Foundational |  |
|  | Leverandøren skal ved fjernstyring administrere konfiguration og installation af Programmel og patch levels på de af Leverandørens eksterne enheder, som opnår fjernadgang til Leverandørens interne netværk, og som anvendes til Kontraktens opfyldelse.  Til brug for tredjepartsenheder (fx underleverandører) skal Leverandøren udsende minimumssikkerhedsstandarder for adgang til Leverandørens netværk og udføre en sikkerhedsscanning, inden der tillades adgang. | 12.7 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse regelmæssigt scanne for bagdørs-forbindelser til internettet, der omgår DMZ-systemer, herunder uautoriserede VPN-adgange og dual-homed hosts, der er tilsluttet Leverandørens netværk samt tilsluttet andre netværk via en trådløs internetforbindelse, opkaldsmodem eller andre mekanismer. | 12.8 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende Netflow-indsamling og ‑analyse eller tilsvarende for DMZ-netværksdatastrømme for at registrere unormal aktivitet. | 12.9 | Foundational |  |
|  | Med henblik på at identificere skjulte dataeksfiltreringskanaler skal Leverandøren konfigurere den indbyggede sessionssporingsfunktion i Leverandørens firewalls, der anvendes til Kontraktens opfyldelse, til at identificere TCP-sessioner, der tager usædvanlig lang tid i forhold til den givne opgave og firewall-enhed, for på baggrund heraf at alarmere de relevante personer om kilde- og destinationsadresser relateret til disse lange sessioner. | 12.10 | Advanced |  |
| SANS CIS 13: Data Protection | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende processer og værktøjer, der forebygger risikoen for og minimerer konsekvenserne ved ekstrahering af data, samt sikre fortrolighed og integritet ved følsomme informationer. | 13 | N/A | ISO 8.3.1, 10.1.1 – 10.1.2, 13.2.3 og 18.1.5. Kravkatalogets afsnit 2.4.3, 2.6.1, 2.9.2 og 2.14.1 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udføre en vurdering af data for at identificere følsomme oplysninger, der kræver anvendelse af krypterings- og integritetskontrol. | 13.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende godkendt krypteringssoftware til bærbare enheder og systemer, der indeholder følsom information. | 13.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse implementere et automatiseret værktøj i Infrastrukturen, der monitorerer følsomme oplysninger, nøgleord og dokumentegenskaber med henblik på at opdage uautoriserede forsøg på ekstrahering af data på tværs af netværk og med henblik på at blokere sådanne forsøg samt underrette sikkerhedspersonalet. | 13.3 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udføre regelmæssige scanninger af Infrastrukturen ved hjælp af automatiske værktøjer for at kontrollere, om følsomme oplysninger findes på systemet i *klar tekst*. Disse værktøjer, der søger efter mønstre, der indikerer tilstedeværelsen af følsomme oplysninger, skal anvendes med henblik på at undersøge, om en forretningsmæssig eller teknisk proces efterlader eller på anden måde lækker følsomme oplysninger. | 13.4 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse konfigurere systemerne til ikke at skrive data på USB-enheder, herunder USB-tokens og USB-harddiske, medmindre der er forretningsmæssige behov for at understøtte sådanne enheder.  Hvis der er behov for sådanne enheder i forbindelse med Kontraktens opfyldelse, skal Leverandøren anvende Programmel, der kan konfigurere systemer til kun at tillade brug af bestemte USB-enheder (baseret på serienummer eller andre unikke karakteristika), og som automatisk kan kryptere alle data, der placeres på sådanne enheder.  Leverandøren skal herunder føre og ajourføre en oversigt over alle godkendte enheder. | 13.5 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende netværksbaserede DLP-løsninger til monitorering og kontrol af dataflow i Leverandørens netværk. Enhver afvigelse, der overstiger almindelig variation i trafikmønstrene, skal registreres, og de rette foranstaltninger skal iværksættes for at håndtere sådanne. | 13.6 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse overvåge al udgående datatrafik og registrere al uautoriseret brug af kryptering. Leverandøren skal desuden sikre, at Leverandøren er i stand til at opdage fjendtlige tilkoblinger, afbryde sådanne forbindelser og genoprette det inficerede system. | 13.7 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse blokere adgang til kendte fildelings- og e-mail-eksfiltreringshjemmesider. | 13.8 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende host-baseret Data Loss Prevention (DLP) til at håndhæve access control lists (ACL), også i situationer hvor data kopieres fra en server. | 13.9 | Advanced |  |
| SANS CIS 14: Controlled Access Based on the Need to Know | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende processer og værktøjer til at spore, kontrollere, hindre og korrigere sikker adgang til kritiske Informationsaktiver på baggrund af hvilke personer, computere, servere og Applikationer, der er blevet formelt godkendt og tildelt ret til at tilgå disse kritiske Informationsaktiver. | 14 | N/A | ISO 8.3.1, 9.1.1 og 10.1.1. Kravkatalogets afsnit 2.4.2, 2.5.1 og 2.6.1 |
|  | Leverandøren skal segmentere netværk, der anvendes til Kontraktens opfyldelse, i henhold til betegnelse eller klassifikationsniveau for den information, der lagres på serverne.  Leverandøren skal herunder placere al følsom information på separate VLAN-netværk med firewall-filtrering for at sikre, at kun autoriserede personer, hvor det er nødvendigt for disse at få adgang for at kunne udføre deres individuelt specifikke pligter, er i stand til at kommunikere med det givne system. | 14.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kryptere al kommunikation indeholdende følsomme oplysninger, der kommunikeres via usikre netværk. Hver gang oplysninger kommunikeres gennem et usikkert netværk, skal oplysningerne således være krypteret. | 14.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at alle netværksswitches muliggør brugen af VLAN for segmenterede arbejdsstationsnetværk for at begrænse netværksenheders mulighed for at kommunikere direkte med andre enheder på sub-netværk og dermed begrænse en angribers mulighed for at kompromittere tilstødende systemer. | 14.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse beskytte al information lagret på systemer med filsystemer, netværksdeling, krav (”claims”), Applikationer eller databasespecifikke adgangskontrollister. Dette skal bl.a. sikre, at kun autoriserede personer med et behov for at tilgå bestemte informationer som led i deres arbejdsbetingede opgaver skal have adgang til at tilgå disse informationer. | 14.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at følsomme oplysninger, som er lagret på systemet, krypteres, når de ikke er i brug (”at rest”). Endvidere skal det kræve sekundære autentifikationsmekanismer, som ikke er integreret i operativsystemet, at få adgang til disse krypterede oplysninger. | 14.5 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udføre og håndhæve en detaljeret logføring over adgang til ikke-offentlige data og særlig autentifikation ved følsomme data. | 14.6 | Foundational |  |
|  | Leverandøren skal sikre, at arkiverede datasæt eller systemer, der ikke regelmæssigt anvendes til Kontraktens opfyldelse, fjernes fra Leverandørens netværk. Disse systemer må kun anvendes som stand-alone systemer (ikke tilkoblet netværket) i tilfælde af, at forretningsenheden skulle få brug for systemet, eller skal være helt virtualiseret og slukket, indtil behovet opstår. | 14.7 | Foundational |  |
| SANS CIS 15: Wireless Access Control | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende processer og værktøjer til at spore/kontrollere/forhindre/korrigere sikkerheden ved brug af trådløse lokale netværk (LAN), access points og trådløse klient-systemer. | 15 | N/A | ISO 10.1.1, 12.4.1 og 12.7.1. Kravkatalogets afsnit 2.6.1, 2.8.4 og 2.8.7 |
|  | Leverandøren skal sikre, at hver eneste trådløse enhed, som er tilsluttet netværket i relation til Kontraktens opfyldelse, matcher en autoriseret konfiguration og sikkerhedsprofil og er tilknyttet en dokumenteret ejer af forbindelsen og et defineret forretningsbehov. Leverandøren skal derudover sikre, at trådløse enheder, der ikke har en sådan autoriseret konfiguration og sikkerhedsprofil i relation til Kontraktens opfyldelse, nægtes adgang. | 15.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse konfigurere netværkssårbarhedsscanningsværktøjer med henblik på at opdage trådløse access points, der er tilsluttet det kablede netværk. Identificerede enheder skal sammenholdes med en liste over autoriserede trådløse access points, og Leverandøren skal herefter deaktivere uautoriserede access points. | 15.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende wireless intrusion detection systems (WIDS) til at identificere skadelige trådløse enheder samt opdage angrebsforsøg og succesfulde angreb. Leverandøren skal derudover sikre, at al trådløs datatrafik overvåges ved WIDS, når datatrafikken passerer ind i kabelnetværket. | 15.3 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at kun såfremt der identificeres et specifikt forretningsmæssigt behov for trådløs adgang, skal klientmaskiner autoriseres til trådløs adgang til trådløse netværk. For enheder, der ikke har et væsentligt forretningsmæssigt behov, skal den trådløs adgang i hardwarekonfigurationen (basic input / output system, Extensible Firmware Interface eller tilsvarende) deaktiveres. | 15.4 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at al trådløs datatrafik som minimum udnytter Advanced Encryption Standard (AES) kryptering, der som minimum anvendes sammen med WiFi Protected Access 2 (WPA2) beskyttelse. | 15.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at der ved trådløse netværk anvendes godkendelsesprotokoller, der leverer beskyttelse af legitimationsoplysninger og gensidig godkendelse. | 15.6 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse deaktivere muligheden for anvendelse af trådløse peer-to-peer datanet for trådløse enheder. | 15.7 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse deaktivere muligheden for forbindelse til trådløse eksterne enheder (fx via Bluetooth) i enheder, medmindre anvendelse af en sådan ekstern enhed kan dokumenteres at være nødvendig for at opfylde et forretningsmæssigt behov. | 15.8 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse oprette separate virtuelle lokalnetværk (VLAN) til BYOD-systemer og andre enheder, der ikke er tillid til. Internetadgang fra dette VLAN skal som minimum gå gennem samme netværksgrænse som Leverandørens almindelige trafik. Adgang fra dette VLAN skal behandles som om, der ikke er tillid hertil, og filtreres og revideres i overensstemmelse hermed. | 15.9 | Foundational |  |
| SANS CIS 16: Account Monitoring and Control | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til Kontraktens opfyldelse aktivt kontrollere livscyklussen for system- og applikationskonti, herunder administrere oprettelsen, brugen af, midlertidig inaktivering og sletning, med det formål at minimere risikoen for, at konti kan udnyttes til cyberangreb. | 16 | N/A | ISO 9.1.1, 9.2.1 – 9.2.6, 9.3.1, 9.4.1 – 9.4.3 og 11.2.8. Kravkatalogets afsnit 2.5.1, 2.5.2, 2.5.3, 2.5.4 og 2.7.2 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse gennemgå alle brugerkonti og deaktivere enhver konto, der ikke kan relateres til en relevant forretningsproces eller aktivejer. | 16.1 | Foundational |  |
|  | Leverandøren skal sikre, at alle brugerkonti, der anvendes til Kontraktens opfyldelse, har en udløbsdato, der overvåges og håndhæves. | 16.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse etablere og føre tilsyn med en proces for tilbagekaldelse af systemadgang, hvor konti deaktiveres straks efter, at en ansat eller underleverandør hos Leverandøren opsiges. Leverandøren skal deaktivere konti i stedet for at slette dem for at bevare auditsporet i relation til Kontraktens opfyldelse. | 16.3 | Foundational |  |
|  | Leverandøren skal regelmæssigt overvåge brugen af alle konti, der anvendes ved Kontraktens opfyldelse, og automatisk logge brugere af efter en standardperiode uden aktivitet. | 16.4 | Foundational |  |
|  | Leverandøren skal konfigurere skærmlåsning af computere for at begrænse adgangen til ubemandede arbejdsstationer, der anvendes til Kontraktens opfyldelse. | 16.5 | Foundational |  |
|  | Leverandøren skal overvåge anvendelsen af brugerkonti, der anvendes til Kontraktens opfyldelse, for at opdage konti, der ikke er i brug, og underrette brugeren eller brugerens overordnede herom. Brugerkonti, der ikke er i brug, skal deaktiveres, hvis der ikke er behov for dem, og Leverandøren skal registrere og dokumentere, hvis der gøres undtagelser herfor (fx leverandørvedligeholdelseskonti, som er nødvendige for systemgendannelse eller andre løbende handlinger).  Leverandøren skal herunder sikre, at:   1. en leder og/eller aktivejer matcher aktive medarbejdere og eksterne brugere med enhver konto, som en leder og/eller aktivejer er ansvarlig for; og 2. sikkerheds- eller systemadministratorer derefter deaktiverer konti, der ikke er tildelt en medarbejder eller ekstern bruger. | 16.6 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende og konfigurere brugerkonto-lockout, sådan at en brugerkonto låses i en fastsat tidsperiode efter et givent antal mislykkede loginforsøg. | 16.7 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse overvåge forsøg på at få adgang til deaktiverede konti ved hjælp af audit-logning. | 16.8 | Foundational |  |
|  | Leverandøren skal konfigurere adgang til alle brugerkonti, der anvendes til Kontraktens opfyldelse, gennem et centraliseret autentifikationssystem. Leverandøren skal desuden konfigurere netværks- og sikkerhedsudstyr til at understøtte centraliserede autentifikationsmetoder. | 16.9 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse dokumentere Leverandørens brugeres typiske kontoforbrug ved at fastslå, hvornår på dagen der normalt logges på, og hvor længe adgangen varer. Leverandøren skal sikre, at der genereres rapporter, der viser brugere, som har logget ind på usædvanlige tidspunkter, eller som har overskredet deres normale login-periode, herunder registrering af tilfælde, hvor brugerens brugerkonti anvendes på andre computere end den sædvanlige. | 16.10 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kræve multifaktor-autentifikation for alle brugerkonti, som har adgang til følsomme informationer eller systemer. | 16.11 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at i tilfælde hvor multifaktor-autentifikation ikke understøttes, skal brugerkonti være forpligtede til at bruge lange passwords (længere end 14 tegn). | 16.12 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at der altid anvendes krypterede kanaler, når kontobrugernavne og autentifikationsinformationer sendes på tværs af netværk. | 16.13 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse kontrollere og verificere, at alle autentifikationsfiler er krypterede eller omdannet via en hashfunktion, og at disse autentifikationsfiler ikke kan tilgås uden root- eller administratorrettigheder. Leverandøren skal desuden registrere og foretage audit af al adgang til passwordfiler i systemet | 16.14 | Foundational |  |
| SANS CIS 17: Security Skills Assessment and Appropriate Training to Fill Gaps | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal i relation til alle funktioner og roller i Leverandørens organisation, der medvirker direkte til Kontraktens opfyldelse, identificere den specifikke viden, samt de specifikke færdigheder og evner, der er nødvendige for at sikre informationssikkerheden i forbindelse hermed. Leverandøren skal herunder udvikle og gennemføre et program med det formål at vurdere og identificere forbedringsbehov og afhjælpe sikkerhedshuller ved hjælp af politikker, organisering, uddannelse samt awareness. | 17 | N/A | ISO 7.2.2. Kravkatalogets afsnit 2.3.2 |
|  | Leverandøren skal udføre gap-analyser for at vurdere, hvilke kompetencer medarbejderne mangler, som de har brug for, for at gennemføre Kontraktens krav til informationssikkerhed, samt identificere uønsket adfærd i relation hertil. Disse oplysninger skal bruges til at tilrettelægge uddannelse og oplysning (awareness) af alle medarbejdere, der medvirker direkte til Kontraktens opfyldelse. | 17.1 | Foundational |  |
|  | Leverandøren skal sikre uddannelse af medarbejdere, så alle nødvendige kompetencer og kvalifikationer er til stede for at gennemføre Kontraktens krav til informationssikkerhed. | 17.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse indføre et sikkerheds-awareness-program, der:   * 1. fokuserer på de metoder, der almindeligvis anvendes til indtrængning, og som kan blokeres af en medarbejder,   2. leveres i korte onlinemoduler,   3. løbende opdateres (mindst én gang årligt) for at vise de nyeste angrebsteknikker,   4. mindst én gang årligt skal gennemføres af samtlige medarbejdere,   5. er overvåget for så vidt angår medarbejderes gennemførelse af programmet, og   6. omfatter ledelsens personlige meddelelser, deltagelse i uddannelse og ansvarlighed gennem effektivitetsmålinger. | 17.3 | Foundational |  |
|  | Leverandøren skal underbygge og øge informationsniveauet gennem regelmæssige tests for at teste, om en medarbejder, der medvirker direkte til Kontraktens opfyldelse, vil klikke på et link i en mistænkelig e-mail eller telefonisk vil udlevere følsomme oplysninger uden at følge passende procedurer til at autentificere et opkald. De medarbejdere, der ikke består testen, skal modtage målrettet uddannelse herom. | 17.4 | Foundational |  |
|  | Leverandøren skal anvende sikkerhedskompetencevurderingsværktøjer i relation til roller, der medvirker direkte til Kontraktens opfyldelse for at identificere kompetencemangler. Leverandøren skal bruge praktiske og autentiske eksempler til at vurdere kompetencerne. Alternativt kan Leverandøren anvende et tilsvarende online-værktøj, som simulerer faktiske og autentiske scenarier for hver af de identificerede opgaver for at vurdere kompetencer. | 17.5 | Advanced |  |
| SANS CIS 18: Application Software Security | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal kontrollere den sikkerhedsmæssige livscyklus for alt in-house-udviklet og anskaffet Programmel, der anvendes til Kontraktens opfyldelse med henblik på at forebygge, opdage og korrigere sikkerhedsmæssige sårbarheder. | 18 | N/A | ISO 9.4.5, 12.1.4, 14.2.1 og 14.2.6 – 14.2.8. Kravkatalogets afsnit 2.5.4, 2.8.1 og 2.10.2 |
|  | Leverandøren skal for så vidt angår tredjepartsprogrammel, der anvendes til Kontraktens opfyldelse, kontrollere, at den version, der bruges, stadig understøttes af producenten. Hvis dette ikke er tilfældet, skal Leverandøren opdatere tredjepartsprogrammellet til den nyeste version, og alle relevante patches og leverandørsikkerhedsmæssige anbefalinger skal installeres. | 18.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse beskytte webapplikationer ved at implementere webapplikationsfirewalls (WAF’s), der kontrollerer al trafik, der strømmer til webapplikationen, for almindelige webapplikationsangreb, herunder men ikke begrænset til cross-site scripting, SQL injektion, kommandoinjektion og mappekrydsningsangreb. For Applikationer, der ikke er web-baserede, skal specifikke applikationsfirewalls anvendes, hvis sådanne værktøjer er tilgængelige for den givne applikationstype. Hvis trafikken er krypteret, skal enheden enten sidde bag krypteringen eller være i stand til at dekryptere trafikken inden analysen. Hvis ingen af disse muligheder er egnet, skal en host-baseret webapplikationsfirewall implementeres. | 18.2 | Foundational |  |
|  | Leverandøren skal sikre, at der i forbindelse med egenudviklet Programmel, der anvendes til Kontraktens opfyldelse, udføres og dokumenteres en eksplicit fejlkontrol på alle input, herunder størrelse, datatype og acceptable områder eller formater. | 18.3 | Foundational |  |
|  | Leverandøren skal teste både egenudviklede og tredjeparts webapplikationer, der anvendes til Kontraktens opfyldelse, for almindelige sikkerhedsmæssige svagheder ved hjælp af automatiserede sikkerhedsscanningsværktøjer til webapplikationer. Leverandøren skal gennemføre disse tests før implementering, samt hver gang webapplikationen opdateres, og på en løbende regelmæssig basis. Især skal input-validering og output-kodningsrutiner af applikationsprogrammel gennemgås og testes. | 18.4 | Foundational |  |
|  | Leverandøren skal sikre, at Systemet ikke viser Systemets fejlmeddelelser til eksterne slutbrugere. | 18.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse opretholde særskilte miljøer for produktions- og ikke-produktionssystemer. Leverandøren skal desuden sikre, at udviklere som udgangspunkt ikke må have uovervåget adgang til Driftsmiljøet. | 18.6 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse, for Applikationer der er afhængige af en database, anvende standardskabeloner for hærdelseskonfigurationer. Alle systemer, der indgår i kritiske forretningsprocesser i relation til Kontraktens opfyldelse, skal ligeledes testes. | 18.7 | Foundational |  |
|  | Leverandøren skal sikre, at alt softwareudviklingspersonale, der medvirker direkte til Kontraktens opfyldelse, uddannes i sikker kodning inden for deres specifikke udviklingsområde. | 18.8 | Foundational |  |
|  | Leverandøren skal sikre, at udviklingsartefakter, der anvendes i relation til Kontraktens opfyldelse, fx prøvedata og -scripts, ubrugte biblioteker, komponenter, fejlkoder og værktøjer, i forbindelse med egenudviklede webapplikationer, ikke er inkluderet i den implementerede Programmel eller er tilgængelige i Driftsmiljøet. | 18.9 | Foundational |  |
| SANS CIS 19: Incident Response and Management | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal med det formål at beskytte information omfattet af Kontrakten udvikle og implementere en hændelsesreaktionsinfrastruktur (fx planer, definerede roller, uddannelse, kommunikation og ledelsesmæssig kontrol) for hurtigt at opdage en informationssikkerhedshændelse og dernæst effektivt begrænse skaden, eliminere informationssikkerhedshændelsen og genoprette netværket og Systemets integritet. | 19 | N/A | ISO 6.1.3, 7.2.1, 16.1.2 og 16.1.4 – 16.1.7. Kravkatalogets afsnit 2.2.1, 2.3.2 og 2.12.1 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse sikre, at der foreligger skriftlige informationssikkerhedshændelsesprocedurer, der bl.a. indeholder en definition af personalets rolle i forbindelse med håndteringen af informationssikkerhedshændelser. Procedurerne skal desuden definere de forskellige faser i hændelseshåndteringen. | 19.1 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse fordele ansvar og roller til specifikke medarbejdere i forbindelse med håndtering af computer- og netværkshændelser. | 19.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udpege, hvilke medarbejdere med ledelsesansvar der i processen for håndtering af informationssikkerhedshændelser har ansvar for at træffe nøglebeslutninger. | 19.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udarbejde retningslinjer vedrørende tidsfrister for systemadministratorers og andet personales rapportering af unormale hændelser til hændelseshåndteringsteamet, fremgangsmåden for en sådan rapportering samt hvilke typer oplysninger, der skal indgå i hændelsesanmeldelsen. Leverandøren skal desuden sikre, at denne rapportering også omfatter underretning af myndigheder i overensstemmelse med gældende love og forskrifter vedrørende inddragelse af disse i informationssikkerhedshændelser. | 19.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse indsamle og opbevare den relevante kontaktinformation, der skal anvendes til tredjepartsrapportering af en informationssikkerhedshændelse. | 19.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse videreformidle information om indrapporterede anormaliteter og informationssikkerhedshændelser til alt personale, herunder medarbejdere og underleverandører, der medvirker direkte til Kontraktens opfyldelse. Leverandøren skal desuden sikre, at sådan information er en del af de oplysninger, som medarbejderne får som led i Leverandørens awareness-aktiviteter. | 19.6 | Foundational |  |
|  | Leverandøren skal regelmæssigt afholde simulationsundervisning for det personale, der er tilknyttet hændelseshåndteringsteamet, for at sikre, at de er bevidste om aktuelle trusler og risici samt om deres pligter i hændelseshåndteringsteamet i relation til Kontraktens opfyldelse. | 19.7 | Foundational |  |
| SANS CIS 20: Penetration Tests and Red Team Exercises | | | | |
| **Krav-ID** | **Kravtekst baseret på SANS CIS** | **SANS**  **Inputkilde** | **Kategori** | **ISO27001 ref.** |
|  | Leverandøren skal teste den overordnede informationssikkerhed (herunder teknologier, processer, og medarbejdere) i relation til Kontraktens opfyldelse ved at simulere angreb på informationssikkerheden. | 20 | N/A | ISO 14.2.8, 18.2.1, 18.2.3. Kravkatalogets afsnit 2.10.2 og 2.14.2 |
|  | Leverandøren skal i relation til Kontraktens opfyldelse foretage regelmæssige eksterne og interne penetrationstest for at identificere sårbarheder og angrebsvektorer, der kan udnyttes. Penetrationstestene skal ske såvel uden for netværksperimetret (dvs. internettet eller trådløse frekvenser rundt om organisationen) som inden for netværksperimetret (dvs. på det interne netværk) for både at simulere eksterne og interne angreb. | 20.1 | Foundational |  |
|  | Leverandøren skal sikre, at samtlige bruger- eller systemkonti, der bruges til at udføre penetrationstests i relation til Kontraktens opfyldelse, kontrolleres og overvåges for at sikre, at de kun bliver brugt til legitime formål, og at de fjernes eller genoprettes til normal tilstand, når tests er gennemført. | 20.2 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udføre regelmæssige *Red-Team-*øvelser for at teste organisatorisk parathed til at identificere og stoppe angreb eller til at reagere hurtigt og effektivt. | 20.3 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse udføre tests med henblik på at undersøge tilstedeværelsen af ubeskyttede systemoplysninger og artefakter, der ville være brugbare for angribere, herunder netværksdiagrammer, konfigurationsfiler, ældre gennemtrængningstestrapporter, e-mails eller dokumenter, der indeholder adgangskoder eller andre oplysninger, der er afgørende for Systemets drift. | 20.4 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse opstille klare mål for penetrationstesten med henblik på at variere typen af angreb og identificere mål i form af specifikke maskiner eller Informationsaktiver med det formål at være forberedt på forskellige typer angreb, bl.a. APT- og multivektor angreb. Leverandøren skal herunder foretage manuelle og automatiserede *Red-Team*-tests, der både inkluderer pivoterede angreb og multifaktor-angreb, for at give en realistisk vurdering af sikkerhedstilstanden og risici for kritiske Informationsaktiver. | 20.5 | Foundational |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse anvende sårbarhedsscanning, herunder i overensstemmelse med K71, og penetrationstestværktøjer i kombination. Resultaterne af sårbarhedsscanningerne skal bruges som udgangspunkt til at vejlede og målrette penetrationstestene. | 20.6 | Foundational |  |
|  | Hvor det er muligt og relevant, skal Leverandøren i relation til Kontraktens opfyldelse sikre, at *Red-Team*-resultater dokumenteres ved anvendelse af åbne, maskinlæsbare standarder (fx SCAP eller tilsvarende). Leverandøren skal desuden udvikle et pointsystem til scoring af resultaterne af *Red-Team*-øvelser, så resultaterne er sammenlignelige over tid. | 20.7 | Advanced |  |
|  | Leverandøren skal i relation til Kontraktens opfyldelse oprette et testmiljø, der efterligner et driftsmiljø, med henblik på at foretage specifikke gennemtrængningstests og *Red-Team*-angreb mod elementer, der typisk ikke testes i produktionen, fx angreb mod administrativ kontrol, dataindsamling og øvrige kontrolsystemer. | 20.8 | Advanced |  |

# Bilag 3: Mapning mellem ISO27001, SANS CIS og Kravkataloget

|  |
| --- |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| **ISO 27001:2013,**  **Anneks A** | **SANS CIS** | **Kravkatalogets Krav-ID** |
| 8.1.1, 9.1.2, 13.1.1 | SANS CIS #1: Inventory of Authorized and Unauthorized Devices | **ISO**: K19, K30, K74  **SANS**: K118, K119, K 120, K121, K122, K123, K124 |
| 12.5.1, 12.6.2 | SANS CIS #2: Inventory of Authorized and Unauthorized Software | **ISO**: K70, K72  **SANS**: K125, K126, K127, K128, K129 |
| 14.2.4, 14.2.8, 18.2.3 | SANS CIS #3: Secure Configuration for Hardware and Software | **ISO**: K87, K91, K117  **SANS**: K130, K131, K132, K133, K134, K135, K136, K137 |
| 12.6.1, 14.2.8 | SANS CIS #4: Continuous and Vulnerability Assessment and Remediation | **ISO**: K71, K91  **SANS**: K138, K139, K140, K141, K142, K143, K144, K145, K146 |
| 9.1.1, 9.2.2 – 9.2.6, 9.3.1, 9.4.1 – 9.4.4 | SANS CIS #5: Controlled Use of Administrative Privileges | **ISO**: K29, K32-K36, K37, K38-K41  **SANS**: K147, K148, K149, K150, K151, K152, K153, K154, K155, K156 |
| 12.4.1 – 12.4.4, 12.7.1 | SANS CIS #6: Maintenance, Monitoring, and Analysis of Audit Logs | **ISO**: K66-K69, K73  **SANS**: K157, K158, K159, K160, K161, K162, K163 |
| 14.2.4, 14.2.8, 18.2.3 | SANS CIS #7: Email and web browser Protections | **ISO**: K87, K91, K117  **SANS**: K164, K165, K166, K167, K168, K169, K170, K171, K172 |
| 8.3.1, 12.2.1, 13.2.3 | SANS CIS #8: Malware Defenses | **ISO**: K26, K64, K79  **SANS**: K173, K174, K175, K176, K177, K178, K179 |
| 9.1.2, 13.1.1, 13.1.2, 14.1.2 | SANS CIS #9: Limitation and Control of Network Ports | **ISO**: K30, K74, K75, K82  **SANS**: K180, K181, K182, K183, K184, K185, K186 |
| 10.1.1, 12.3.1 | SANS CIS #10: Data Recovery Capability | **ISO**: K43, K65  **SANS**: K187, K188, K189, K190, K191 |
| 9.1.2, 13.1.1, 13.1.3 | SANS CIS #11: Secure Configurations for Network Devices | **ISO**: K30, K74, K76  **SANS**: K192, K193, K194, K195, K196, K197, K198, K199 |
| 9.1.2, 12.4.1, 12.7.1, 13.1.1, 13.1.3, 13.2.3 | SANS CIS #12: Boundary Defense | **ISO**: K30, K66, K73, K74, K76, K79  **SANS**: K200, K201, K202, K203, K204, K205, K206, K207, K208, K209, K210 |
| 8.3.1, 10.1.1 – 10.1.2, 13.2.3, 18.1.5 | SANS CIS #13: Data Protection | **ISO**: K26, K43-K44, K79, K114  **SANS**: K211, K212, K213, K214, K215, K216, K217, K218, K219, K220 |
| 8.3.1, 9.1.1, 10.1.1 | SANS CIS #14: Controlled Access Based on the Need to Know | **ISO**: K26, K29, K43  **SANS**: K221, K222, K223, K224, K225, K226, K227, K228 |

|  |  |  |
| --- | --- | --- |
| 10.1.1, 12.4.1, 12.7.1 | SANS CIS #15: Wireless Access Control | **ISO**: K43, K66, K73  **SANS**: K229, K230, K231, K232, K233, K234, K235, K236, K237, K238 |
| 9.1.1, 9.2.1 – 9.2.6, 9.3.1, 9.4.1 – 9.4.3, 11.2.8 | SANS CIS #16: Account Monitoring and Control | **ISO**: K29, K31-K36, K37, K38-K40, K58  **SANS**: K239, K240, K241, K242, K243, K244, K245, K246, K247, K248, K249, K250, K251, K252, K253 |
| 7.2.2 | SANS CIS #17: Security Skills Assessment and Appropriate Training to Fill Gaps | **ISO**: K16  **SANS**: K254, K255, K256, K257, K258, K259 |
| 9.4.5, 12.1.4, 14.2.1, 14.2.6 – 14.2.8 | SANS CIS #18: Application Software Security | **ISO**: K42, K63, K84, K89-K91  **SANS**: K260, K261, K262, K263, K264, K265, K266, K267, K268, K269 |
| 6.1.3, 7.2.1, 16.1.2, 16.1.4 – 16.1.7 | SANS CIS #19: Incident Response and Management | **ISO**: K8, K15, K100, K102-K105  **SANS**: K270, K271, K272, K273, K274, K275, K276, K277 |
| 14.2.8, 18.2.1, 18.2.3 | SANS CIS #20: Penetration Tests and Red Team Exercises | **ISO**: K91, K115, K117  **SANS**: K278, K279, K280, K281, K282, K283, K284, K285, K286 |

|  |
| --- |
|  |
| digst.dk |