Digitaliseringsstyrelsen har udarbejdet nærværende vejledningsskema, der består af en oversigt over konkrete krav til cybersikkerhedsforanstaltninger, som enheder omfattet af NIS 2-loven skal leve op til.
Download excel-verionen af vejledningsskemaet for at benytte selvevalueringsmodulet, der har til formål at understøtte enhederne i deres vurdering af i hvilken grad, de efterlever lovgivningens krav.

OBS. Vær opmærksom på, at der i vejledningsskemaet henvises til **gennemførselsforordning nr. 2024/2690's bilag, artikel 1-13** .

Vejledningsskema for cybersikkerhedsforanstaltninger

Foranstaltninger				Relaterede standarder			
Henvising til gennemførselsforordning nr. 2024/2690's bilag	**Kontrolmål**	**Kontroller**	**Gennemgangsbetingelser**	**ISO-standard**	**NIST-standard**	**ETSI-standard**	**CEN/TS-standard**
1. Politik for sikkerheden i net- og informationssystemer							
1.1. Politik for sikkerheden i net- og informationssystemer	Relevante enheder etablerer og opretholder en sikkerhedspolitik for net- og informationssystemer, der fastlægger den overordnede tilgang til sikkerheden. (2022/2555, artikel 21, stk. 2, litra a).	Med henblik på artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555 skal politikken for sikkerhed i net- og informationssystemer: (a) fastsætte de relevante enheders tilgang til styring af sikkerheden i deres net- og informationssystemer (b) være passende i forhold til og supplere de relevante enheders forretningsstrategi og -mål (c) fastsætte net- og informationssikkerhedsmål (d) omfatte en forpligtelse til løbende at forbedre sikkerheden i net- og informationssystemer (e) omfatte en forpligtelse til at stille de nødvendige ressourcer til rådighed til dens gennemførelse, herunder det nødvendige personale, de nødvendige finansielle ressourcer, samt de nødvendige processer, værktøjer og teknologier (f) meddeles til og anerkendes af relevante medarbejdere og relevante interesserede eksterne parter (g) fastsætte roller og ansvarsområder i henhold til Gennemførselsforordningen pkt. 1.2 (h) omfatte en liste over den dokumentation, der skal opbevares, og en angivelse af, hvor længe denne dokumentation skal opbevares (i) omfatte en liste over emnespecifikke politikker (j) fastsætte indikatorer og foranstaltninger til overvågning af politikkens gennemførelse og den aktuelle status for modenheden af de relevante enheders net- og informationssikkerhed (k) omfatte en angivelse af datoen for ledelsesorganernes formelle godkendelse af de relevante enheder ("ledelsesorganerne") (2024/2690, pkt. 1.1.1.).	Ledelsesorganerne gennemgår og, hvis det er relevant, ajourfører politikken for sikkerheden i net- og informationssystemer mindst én gang om året, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici. Resultatet af hver gennemgang skal dokumenteres (2024/2690, pkt. 1.1.2.).	**ISO 27001:2022** 5.2, A.5.1, A.5.36, A.5.4, 9.3	**NIST CSF v2.0** PR.AT-02, GV.PO-01, GV.PO-02, GV.OC-03, GV.RM-03, GV.OC-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ 6.1-02, REQ 6.1-06, REQ 6.1-07, REQ 6.1-08, Clause 6.3	**CEN/TS 18026:2024** ISP-01, ISP-02, OPS-01, OPS-02, OPS-03
1.2. Roller, ansvarsområder og bemyndigelser	De relevante enheder fastlægger som led i deres sikkerhedspolitik for net- og informationssystemer, jf. Gennemførselsforordningen pkt. 1.1, ansvarsområder og bemyndigelser i forbindelse med sikkerheden i net- og informationssystemer, indordner dem pr. rolle, fordeler dem i overensstemmelse med de relevante enheders behov og meddeler dem til ledelsesorganerne (2024/2690, pkt. 1.2.1.).	De relevante enheder skal kræve, at alt personale og alle tredjeparter anvender et sikkerhedsniveau i deres net- og informationssystemer i overensstemmelse med de relevante enheders etablerede politik for net- og informationssikkerhed, emnespecifikke politikker og procedurer. Mindst én person skal rapportere direkte til ledelsesorganerne om spørgsmål vedrørende sikkerheden i net- og informationssystemer. Afhængigt af de relevante enheders størrelse skal sikkerheden i net- og informationssystemer være omfattet af særlige roller eller opgaver, der udføres, ud over de eksisterende roller. Modstridende forpligtelser og modstridende ansvarsområder adskilles, hvor det er relevant (2024/2690, pkt. 1.2.2., 1.2.3., 1.2.4. & 1.2.5.).	Ledelsesorganerne gennemgår og, hvis det er relevant, ajourfører rollerne, ansvarsområderne og bemyndigelserne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 1.2.6.).	**ISO 27001:2022** 5.3, A.5.2, A.5.3, A.5.4	**NIST CSF v2.0** GV.RR-02, GV.SC-02, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.1.2-01, REQ-7.2-01X, REQ-7.2-03X, REQ 7.2-07X, REQ 7.2-08X, REQ 7.2-09X, REQ 7.2-10X, REQ 7.2-11X,	**CEN/TS 18026:2024** ISP-02, OIS-02

2. Politik for risikostyring							
2.1. Ramme for risikostyring	Med henblik på artikel 21, stk. 2, litra a), i direktiv (EU) 2022/2555 etablerer og opretholder de relevante enheder en passende ramme for risikostyring for at afdække og håndtere de risici, der er forbundet med sikkerheden i net- og informationssystemer. De relevante enheder skal udføre og dokumentere risikovurderinger og på grundlag af resultaterne udarbejde, gennemføre og overvåge en risikobehandlingsplan. Resultaterne af risikovurderingen og de resterende risici accepteres af ledelsesorganerne eller, hvor det er relevant, af personer, der er ansvarlige og bemyndigede til at styre risici, forudsat at de relevante enheder sikrer passende rapportering til ledelsesorganerne (2024/2690, pkt. 2.1.1.).	Med henblik på Gennemførselsforordningen pkt. 2.1.1 fastlægger de relevante enheder procedurer for afdækning, analyse, vurdering og behandling af risici ("risikostyringsprocessen for cybersikkerhed"). Risikostyringsprocessen for cybersikkerhed skal være en integreret del af de relevante enheders overordnede proces for risikostyring, hvor det er relevant. Som led i risikostyringsprocessen for cybersikkerhed skal de relevante enheder: (a) følge en risikostyringsmetode (b) fastsætte risikotolerancetærsklen i overensstemmelse med de relevante enheders risikovillighed (c) fastlægge og opretholde relevante risikokriterier (d) i overensstemmelse med en tilgang, der omfatter alle farer, afdække og dokumentere risici, der påvirker sikkerheden i net- og informationssystemer, navnlig i forbindelse med tredjeparter, og risici, der kan føre til forstyrrelser i net- og informationssystemernes tilgængelighed, integritet, autenticitet og fortrolighed, herunder afdækning af enkelte fejlpunkter (e) analysere de risici, der påvirker sikkerheden i net- og informationssystemer, herunder trussels-, sandsynligheds-, indvirknings- og risikoniveauet, under hensyntagen til efterretninger om cybertrusler og sårbarheder (f) evaluere de afdækkede risici på grundlag af risikokriterierne (g) udpege og prioritere egnede risikobehandlingsmuligheder og -foranstaltninger (h) løbende overvåge gennemførelsen af risikobehandlingsforanstaltningerne (i) identificere, hvem der er ansvarlig for at gennemføre risikobehandlingsforanstaltningerne, og hvornår de bør gennemføres (j) dokumentere de valgte risikobehandlingsforanstaltninger i en risikobehandlingsplan og begrunde accepten af de resterende risici på en forståelig måde. Når de relevante enheder udpeger og prioriterer passende risikobehandlingsmuligheder og -foranstaltninger, tager de hensyn til risikovurderingsresultaterne, resultaterne af proceduren til vurdering af effektiviteten af foranstaltningerne til styring af cybersikkerhedsrisici, gennemførelsesomkostningerne i forhold til den forventede fordel, den klassifikation af aktiver, der er omhandlet i gennemførselsforordning pkt. 12.1, og den forretningskonsekvensanalyse, der er omhandlet i pkt. 4.1.3 (2024/2690, pkt. 2.1.2. & 2.1.3.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører både resultaterne af risikovurderingen og risikostyringsplanen med planlagte mellemrum og mindst én gang om året, samt når der sker væsentlige ændringer med hensyn til drift eller risici eller væsentlige hændelser (2024/2690, pkt. 2.1.4.).	**ISO 27001:2022** 6.1, 6.1.2, 6.1.3, 6.2, 8.2, 8.3, A5.7, A.5.19, A.5.20, A.5.21	**NIST CSF v2.0** ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-03, ID.RM-01, GV.RM-06, GV.RR-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 5, Clause 6.3	**CEN/TS 18026:2024** OIS-01, RM-01, RM-02, RM-03
2.2. Overvågning af overholdelse	De relevante enheder gennemgår regelmæssigt overholdelsen af deres politikker for sikkerheden i net- og informationssystemer, emnespecifikke politikker, regler og standarder. Ledelsesorganerne underrettes gennem regelmæssig rapportering på grundlag af evalueringer af overholdelsen om status for net- og informationssikkerheden (2024/2690, pkt. 2.2.1.).	De relevante enheder indfører et effektivt system til rapportering om overholdelse, som skal være passende for deres strukturer, driftsmiljøer og trusselsbilleder. Systemet til rapportering om overholdelse skal kunne give ledelsesorganerne et informeret overblik over den aktuelle situation med hensyn til de relevante enheders risikostyring (2024/2690, pkt. 2.2.2.).	De relevante enheder udfører overvågningen af overholdelsen med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 2.2.3.).	**ISO 27001:2022** 9.2, A.5.31, A.5.35, A.5.36	**NIST CSF v2.0** GV.OV-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 7.13, REQ-6.3-06X , REQ-6.3-07X, REQ-6.1-08	**CEN/TS 18026:2024** CO-01, DOC-03, INQ-01, INQ-02, INQ-03
2.3. Uafhængig gennemgang af informations- og netsikkerhed	De relevante enheder gennemgår uafhængigt deres tilgang til styring af sikkerheden i deres net- og informationssystemer og gennemførelsen heraf, herunder mennesker, processer og teknologier (2024/2690, pkt. 2.3.1.).	De relevante enheder udvikler og opretholder processer til gennemførelse af uafhængige gennemgange, som skal udføres af personer med passende auditkompetence. Hvis den uafhængige gennemgang foretages af medarbejdere i den relevante enhed, må de personer, der foretager gennemgangen, ikke være underordnet eller overordnet personalet på det område, der er genstand for gennemgangen. Hvis enhedernes størrelse ikke tillader en sådan adskillelse af autoritetsmæssige forhold, træffer de relevante enheder alternative foranstaltninger for at sikre, at gennemgangen er upartisk. Resultaterne af de uafhængige gennemgange, herunder resultaterne af overvågningen af overholdelsen i henhold til Gennmførselsforordningen pkt. 2.2 samt overvågningen og målingen i henhold til Gennmførselsforordningen pkt. 7, rapporteres til ledelsesorganerne. Der træffes korrigerende foranstaltninger, eller den resterende risiko accepteres i henhold til de relevante enheders kriterier for risikoaccept (2024/2690, pkt. 2.3.2. & 2.3.3.).	De uafhængige gennemgange skal foretages med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 2.3.4.).	**ISO 27001:2022** 9.2, 10.1, A.5.35, A.8.34	**NIST CSF v2.0** GV.OV-02, ID.IM-01	**ETSI EN 319 401** Clause 7.13	**CEN/TS 18026:2024** CO-01, CO-02, CO-03, CO-04

3. Håndtering af hændelser							
3.1. Politik for håndtering af hændelser	Med henblik på artikel 21, stk. 2, litra b), i direktiv (EU) 2022/2555 fastlægger og gennemfører de relevante enheder en politik for håndtering af hændelser, hvori der fastsættes roller, ansvarsområder og procedurer for rettidigt at opdage, analysere, inddæmme eller reagere på, afhjælpe virkningerne af, dokumentere og rapportere hændelser (2024/2690, pkt. 3.1.1.).	Den politik, der er omhandlet i Gennemførselsforordningen pkt. 3.1.1, skal være i overensstemmelse med den driftskontinuitets- og katastrofeberedskabsplan, der er omhandlet i Gennemførselsforordningen pkt. 4.1. Politikken skal omfatte: (a) et kategoriseringssystem for hændelser, der er i overensstemmelse med den vurdering og klassifikation af begivenheder, der foretages i henhold til Gennemførselsforordningen pkt. 3.4.1 (b) planer for effektiv kommunikation, herunder med hensyn til eskalering og rapportering (c) tildeling af roller til kompetente medarbejdere med henblik på at opdage og reagere hensigtsmæssigt på hændelser (d) dokumenter, der skal anvendes i forbindelse med opdagelse af og reaktion på hændelser, såsom håndbøger om håndtering af hændelser, eskaleringsdiagrammer, kontaktlister og skabeloner (2024/2690, pkt. 3.1.2.).	De roller, ansvarsområder og procedurer, der fastlægges i politikken, skal testes og gennemgås og, hvis det er relevant, ajourføres med planlagte mellemrum, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 3.1.3.).	**ISO 27001:2022** A.5 .24	**NIST CSF v2.0** GV.SC-08, RS.MA-01, RS.MA-05, RS.MI-01, RS.MI-02, ID.IM-01, ID.IM-04	**ETSI EN 319 401** REQ-7.9.2-12X, REQ-7.9.2-01X, REQ-7.9.2-04X, REQ-7.9.2-05X, REQ-7.9.2-12X, REQ-7.9.2-06X, REQ-7.9.2-08X , REQ-7.9.3-01X through 04X,	**CEN/TS 18026:2024** ISP-02, IM-01, IM-07
3.2. Overvågning og logning	De relevante enheder fastlægger procedurer og anvender værktøjer til at overvåge og logge aktiviteter på deres net- og informationssystemer for at opdage begivenheder, der kan betragtes som hændelser, og reagere i overensstemmelse hermed for at afbøde virkningerne (2024/2690, pkt. 3.2.1.).	I det omfang, det er muligt, skal overvågningen automatiseres og udføres enten kontinuerligt eller med regelmæssige mellemrum, afhængigt af driftskapaciteten. De relevante enheder gennemfører deres overvågningsaktiviteter på en måde, der minimerer falske positive og falske negative resultater. På grundlag af de procedurer, der er omhandlet i Gennemførselsforordningen pkt. 3.2.1, opbevares, dokumenteres og gennemgås logfiler af de relevante enheder. De relevante enheder opstiller en liste over aktiver, der skal være omfattet af logning, på grundlag af resultaterne af den risikovurdering, der foretages i henhold til punkt 2.1. Hvor det er relevant, skal logfilerne omfatte: (a) relevant udgående og indgående nettrafik (b) oprettelse, ændring eller sletning af brugere af de relevante enheders net- og informationssystemer og udvidelse af tilladelserne (c) adgang til systemer og applikationer (d) begivenheder i forbindelse med autentificering (e) al privilegeret adgang til systemer og applikationer og aktiviteter, der udføres af administrative konti (f) adgang til eller ændringer af kritiske konfigurations- og backupfiler (g) logfiler over begivenheder og logfiler fra sikkerhedsværktøjer såsom antivirus, systemer til opdagelse af indtrængen eller firewalls (h) anvendelse af systemressourcer samt deres ydeevne (i) fysisk adgang til faciliteter (j) adgang til og anvendelse af deres netudstyr og -anordninger (k) aktivering, standsning og pause af de forskellige logningsprocesser (l) miljøbegivenheder (2024/2690, pkt. 3.2.1. & 3.2.3.).	Logfilerne gennemgås regelmæssigt for usædvanlige eller uønskede tendenser. Hvor det er relevant, fastsætter de relevante enheder passende værdier for alarmtærskler. Hvis de fastsatte værdier for alarmtærsklerne overskrides, udløses der, hvor det er relevant, automatisk en alarm. De relevante enheder sikrer, at der i tilfælde af en alarm rettidigt iværksættes en kvalificeret og passende reaktion. De relevante enheder opbevarer logfiler og backups heraf i en på forhånd fastsat periode og beskytter dem mod uautoriseret adgang eller ændringer. I det omfang, det er muligt, sikrer de relevante enheder, at alle systemer har synkroniserede tidskilder for at kunne sammenholde logfiler mellem systemer til vurdering af begivenheder. De relevante enheder udarbejder og fører en liste over alle aktiver, der logges, og sikrer, at der er reservesystemer til overvågning og logning. Tilgængeligheden af overvågnings- og logningssystemerne skal overvåges uafhængigt af de systemer, de overvåger. [nedenstående del skal blive ovenstående del skal i D11] Procedurerne og listen over aktiver, der logges, skal gennemgås og, hvis det er relevant, ajourføres regelmæssigt samt efter væsentlige hændelser (2024/2690, pkt. 3.2.4., 3.2.5., 3.2.6. & 3.2.7.).	**ISO 27001:2022** A.5.28, A.8.15, A.8.16, A.8.17	**NIST CSF v2.0** RS.AN-06, RS.AN-07, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.9.1-01X, REQ-7.9.1-02X, REQ-7.9.1-03X, REQ-7.9.1-04X, REQ-7.9.1-05X, REQ-7.9.2-11X, REQ-7.10-05, REQ-7.10- 06, REQ-7.10-07, REQ-7.10- 08, REQ-7.10-02	**CEN/TS 18026:2024** OPS-10, OPS-11, OPS-12, OPS-13, OPS-14, OPS-15, OPS-16, OPS-23, CS-01, IM-07, PSS-01
3.3. Indberetning af begivenheder	De relevante enheder indfører en enkel mekanisme, der gør det muligt for deres ansatte, leverandører og kunder at indberette mistænkelige begivenheder (2024/2690, pkt. 3.3.1.).	De relevante enheder skal, hvor det er relevant, underrette deres leverandører og kunder om mekanismen til indberetning af begivenheder og regelmæssigt uddanne deres ansatte i, hvordan de anvender mekanismen (2024/2690, pkt. 3.3.2.).	Mekanismen for indberetning af mistænkelige hændelser skal gennemgås og, hvis det er relevant, ajourføres regelmæssigt samt efter væsentlige hændelser (2024/2690, pkt. 3.3.).	**ISO 27001:2022** A.6.8	**NIST CSF v2.0** RS.MI-01, RS.CO-02	**ETSI EN 319 401** REQ-7.9.2-12X, REQ-7.9.3-01X, REQ-7.9.3-02X	**CEN/TS 18026:2024** IM-03, IM-04
3.4. Vurdering og klassifikation af begivenheder	De relevante enheder vurderer mistænkelige begivenheder for at fastslå, om de udgør hændelser, og i bekræftende fald fastslå deres art og alvor (2024/2690, pkt. 3.4.1.).	De relevante enheder handler på følgende måde: (a) Vurderingen foretages på grundlag af foruddefinerede kriterier og med prioritering af hændelser med henblik på inddæmning og afhjælpning (b) Hvert kvartal vurderes forekomsten af tilbagevendende hændelser som omhandlet i denne forordnings artikel 4 (c) De relevante logfiler gennemgås med henblik på vurdering og klassifikation af begivenheder (d) Der indføres en procedure for korrelation og analyse af logfiler (e) Begivenheder revurderes og omklassificeres, hvis nye oplysninger bliver tilgængelige, eller efter analyser af tidligere tilgængelige oplysninger (2024/2690, pkt. 3.4.2.).	Proceduren til vurdering af mistænkelige begivenheder skal gennemgås og, hvis det er relevant, ajourføres regelmæssigt samt efter væsentlige hændelser (2024/2690, pkt. 3.4.).	**ISO 27001:2022** A.5.25	**NIST CSF v2.0** DE.AE-04, RS.MA-02, RS.MA-03, RS.MA-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.9.3-01X, REQ-7.9.2-11X, REQ-7.9.4-01X, REQ-7.9.4-02X, REQ-7.9.1-05X	**CEN/TS 18026:2024** IM-02
3.5. Reaktion på hændelser	De relevante enheder skal reagere rettidigt på hændelser i overensstemmelse med dokumenterede procedurer (2024/2690, pkt. 3.5.1.).	Procedurerne for reaktion på hændelser skal omfatte følgende faser: (a) inddæmning af hændelser for at forhindre, at konsekvenserne af hændelsen spredes (b) afhjælpning for at forhindre, at hændelsen fortsætter eller dukker op igen (c) genopretning efter hændelsen, hvor det er nødvendigt. De relevante enheder udarbejder kommunikationsplaner og -procedurer: (a) med enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er) eller, hvor det er relevant, de kompetente myndigheder i forbindelse med underretning om hændelser (b) til kommunikation mellem medarbejdere i den relevante enhed og til kommunikation med relevante interessenter uden for den relevante enhed. De relevante enheder opfører i loggen aktiviteter vedrørende reaktion på hændelser i overensstemmelse med de procedurer, der er omhandlet i punkt 3.2.1, og dokumenterer forløbet (2024/2690, pkt. 3.5.2., 3.5.3. & 3.5.4.).	De relevante enheder tester med planlagte mellemrum deres procedurer for reaktion på hændelser (2024/2690, pkt. 3.5.5.).	**ISO 27001:2022** A.5.26	**NIST CSF v2.0** RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, ID.IM-02, ID.IM-03, ID.IM-04, RS.CO-02, RS.CO-03, RS.AN-03, RS.MI-01, RS.MI-02, RC.CO-03, RC.CO-04	**ETSI EN 319 401** REQ-7.9.2-01X, REQ-7.9-09, REQ-7.9-12, Clause 7.9.2, REQ-7.9.1-05X, REQ-7.9.2-11X, REQ-7.10-01 through 08	**CEN/TS 18026:2024** OIS-03, IM-01, IM-05, IM-07, INQ-02, INQ-03
3.6. Gennemgang efter hændelsen	Hvor det er relevant, foretager de relevante enheder gennemgange efter hændelser, efter en given hændelse er blevet afhjulpet. Disse gennemgange efter hændelser skal, hvor det er muligt, afdække den grundlæggende årsag til hændelsen og resultere i dokumenterede erfaringer for at reducere forekomsten og konsekvenserne af fremtidige hændelser (2024/2690, pkt. 3.6.1.).	De relevante enheder sikrer, at gennemgange efter hændelser bidrager til at forbedre deres tilgang til net- og informationssikkerhed, til risikobehandlingsforanstaltninger og til procedurer for håndtering, opdagelse og reaktion på hændelser (2024/2690, pkt. 3.5.2.).	De relevante enheder gennemgår med planlagte mellemrum, hvorvidt hændelser afstedkom gennemgange efter hændelsen (2024/2690, pkt. 3.5.3.).	**ISO 27001:2022** A.5.27	**NIST CSF v2.0** ID.IM-01, ID.IM-04, RS.AN-08	**ETSI EN 319 401** REQ-7.9.5-01X, REQ-7.9.5-03X, REQ-7.9.5-04X	**CEN/TS 18026:2024** IM-06

4. Driftskontinuitet og krisestyring							
4.1. Driftskontinuitets- og katastrofeberedskabsplan	Med henblik på artikel 21, stk. 2, litra c), i direktiv (EU) 2022/2555 fastlægger og opretholder de relevante enheder en driftskontinuitets- og katastrofeberedskabsplan, der finder anvendelse i tilfælde af hændelser (2024/2690, pkt. 4.1.1.).	De relevante enheders drift genoprettes i overensstemmelse med driftskontinuitets- og katastrofeberedskabsplanen. Planen skal bygge på resultaterne af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, og skal, hvis det er relevant, omfatte følgende: (a) formål, omfang og målgruppe (b) roller og ansvarsområder (c) vigtige kontakter og (interne og eksterne) kommunikationskanaler (d) betingelser for aktivering og deaktivering af planen (e) rækkefølge for genopretning af driften (f) genopretningsplaner for specifikke aktiviteter, herunder genopretningsmål (g) nødvendige ressourcer, herunder backup og reserver (h) genopretning og genoptagelse af aktiviteter efter afslutningen af midlertidige foranstaltninger. De relevante enheder foretager en forretningskonsekvensanalyse for at vurdere de potentielle konsekvenser af alvorlige forstyrrelser af deres forretningsaktiviteter og fastsætter på grundlag af forretningskonsekvensanalysens resultater kontinuitetskrav for net- og informationssystemerne (2024/2690, pkt. 4.1.2. & 4.1.3.).	Driftskontinuitetsplanen og katastrofeberedskabsplanen skal testes, gennemgås og, hvis det er relevant, ajourføres med planlagte mellemrum, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici. De relevante enheder sikrer, at erfaringerne fra sådanne test indarbejdes i planerne (2024/2690, pkt. 4.1.4.).	**ISO 27001:2022** A5.29, A. 5.30	**NIST CSF v2.0** ID.IM-02, ID.IM-03, ID.IM-04, GV.OC-04, GV.SC-08, RC.RP-01, RC.RP-02	**ETSI EN 319 401** Clause 7.11	**CEN/TS 18026:2024** BC-01, BC-02, BC-03, BC-04
4.2. Styring af backups og reserver	De relevante enheder opretholder backupkopier af data og stiller tilstrækkelige ressourcer til rådighed, herunder faciliteter, net- og informationssystemer og personale, for at sikre et passende niveau af reservekapacitet (2024/2690, pkt. 4.2.1.).	På grundlag af resultaterne af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, og driftskontinuitetsplanen fastlægger de relevante enheder backupplaner, der skal omfatte følgende: (a) genopretningstider (b) sikring af, at backupkopier er fuldstændige og nøjagtige, herunder med hensyn til konfigurationsdata og data, der er lagret i cloudcomputing-tjenestemiljøet (c) lagring af backupkopier (online eller offline) på et eller flere sikre steder, som ikke befinder sig i samme netværk som systemet, og som befinder sig i tilstrækkelig afstand til at undgå enhver skade fra en katastrofe på hovedstedet (d) passende fysisk og logisk kontrol med adgang til backupkopier i overensstemmelse med aktivets klassifikationsgrad (e) gendannelse af data fra sikkerhedskopier (f) opbevaringsperioder baseret på forretningsmæssige og lovgivningsmæssige krav. De relevante enheder foretager regelmæssig integritetskontrol af backupkopierne. På grundlag af resultaterne af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, og driftskontinuitetsplanen sikrer de relevante enheder, at der er tilstrækkelige ressourcer til rådighed ved at indføre i det mindste delvis reservekapacitet for følgende: (a) net- og informationssystemer (b) aktiver, herunder faciliteter, udstyr og forsyninger (c) personale med det påkrævede ansvar, de nødvendige bemyndigelser og den nødvendige kompetence (d) passende kommunikationskanaler. Hvor det er relevant, sikrer de relevante enheder, at der tages hensyn til kravene om backup og reservekapacitet i forbindelse med overvågningen og tilpasningen af ressourcer, herunder faciliteter, systemer og personale (2024/2690, pkt. 4.2.2., 4.2.3. & 4.2.4.).	De relevante enheder foretager regelmæssige test af forløbet med genopretning ud fra backupkopier og af reservekapaciteten for at sikre, at de både kan anvendes i en reel genopretningssituation og omfatter kopier, processer og viden til at foretage en effektiv genopretning. De relevante enheder dokumenterer testresultaterne og træffer om nødvendigt korrigerende foranstaltninger (2024/2690, pkt. 4.2.6.).	**ISO 27001:2022** A.8.13, A.8.14	**NIST CSF v2.0** PR.DS-11, RC.RP-01, RC.RP-02, ID.IM-03	**ETSI EN 319 401** Clause 7.11.2	**CEN/TS 18026:2024** OPS-06, OPS-07, OPS-08, OPS-09
4.3. Krisestyring	De relevante enheder indfører en proces til krisestyring (2024/2690, pkt. 4.3.1.).	De relevante enheder sikrer, at krisestyringsprocessen som minimum omfatter følgende elementer: (a) roller og ansvarsområder for personale og, hvor det er relevant, leverandører og tjenesteudbydere med angivelse af rollefordelingen i krisesituationer, herunder specifikke skridt, der skal følges (b) passende kommunikationsmidler mellem de relevante enheder og relevante kompetente myndigheder (c) anvendelse af passende foranstaltninger til at sikre vedligeholdelsen af sikkerheden i net- og informationssystemer i krisesituationer. Med henblik på litra b) skal informationsstrømmen mellem de relevante enheder og de relevante kompetente myndigheder omfatte både obligatorisk kommunikation såsom hændelsesrapporter og dertil knyttede tidsfrister samt ikkeobligatorisk kommunikation. De relevante enheder gennemfører en proces for forvaltning og anvendelse af oplysninger, der modtages fra CSIRT'erne eller de kompetente myndigheder, hvor det er relevant, vedrørende hændelser, sårbarheder, trusler eller mulige afbødende foranstaltninger (2024/2690, pkt. 4.3.2. & 4.3.3.).	De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører krisestyringsplanen regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 4.3.4.).	**ISO 27001:2022** A.5.26, A.5.29, A.5.30	**NIST CSF v2.0** RS.CO-02, RS.CO-03. PR.IR-03, DE.CM-01, ID.AM-03, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08	**ETSI EN 319 401** Clause 7.11.3	**CEN/TS 18026:2024** BC-03, OIS-03

5. Forsyningskædesikkerhed							
5.1. Politik for forsyningskædesikkerhed	Med henblik på artikel 21, stk. 2, litra d), i direktiv (EU) 2022/2555 udarbejder, gennemfører og anvender de relevante enheder en politik for forsyningskædesikkerhed, som indeholder bestemmelser om forbindelserne med deres direkte leverandører og tjenesteudbydere med henblik på at afbøde de afdækkede risici for sikkerheden i net- og informationssystemer. I politikken for forsyningskædesikkerhed udpeger de relevante enheder deres rolle i forsyningskæden og kommunikerer den til deres direkte leverandører og tjenesteudbydere (2024/2690, pkt. 5.1.1.).	Som led i den i Gennemførselsforordningen pkt. 5.1.1 omhandlede sikkerhedspolitik for forsyningskæden fastsætter de relevante enheder kriterier for udvælgelse af og indgåelse af kontrakter med leverandører og tjenesteudbydere. Disse kriterier omfatter følgende: **(a)** leverandørernes og tjenesteudbydernes cybersikkerhedspraksis, herunder deres procedurer for sikker udvikling, **(b)** leverandørernes og tjenesteudbydernes evne til at opfylde de cybersikkerhedsspecifikationer, der er fastsat af de relevante enheder, **(c)** IKT-produkternes og IKT-tjenesternes generelle kvalitet og modstandsdygtighed samt de indbyggede foranstaltninger til styring af cybersikkerhedsrisici, herunder IKTprodukternes og IKT-tjenesternes risici og klassifikationsgrad, **(d)** de relevante enheders evne til at diversificere forsyningskilderne og begrænse leverandørfastlåsning, hvor det er relevant. Ved fastsættelsen af deres politik for forsyningskædesikkerhed tager de relevante enheder hensyn til resultaterne af de koordinerede sikkerhedsrisiko-vurderinger af kritiske forsyningskæder, der foretages i henhold til artikel 22, stk. 1, i direktiv (EU) 2022/2555, hvor det er relevant. På grundlag af politikken for forsyningskædesikkerhed og under hensyntagen til resultaterne af den risikovurdering, der foretages i overensstemmelse med Gennemførselsforordningens bilags punkt 2.1, sikrer de relevante enheder, at der i deres kontrakter med leverandører og tjenesteudbydere, hvor det er relevant gennem serviceleverance-aftaler, angives følgende, hvor det er relevant: **(a)** cybersikkerhedskrav til leverandører eller tjenesteudbydere, herunder krav vedrørende sikkerhed i forbindelse med erhvervelse af IKT-tjenester eller -produkter, jf. punkt 6.1, **(b)** krav til oplysning, færdigheder og uddannelse samt, hvor det er relevant, påkrævede certificeringer af leverandørernes eller tjenesteudbydernes ansatte, **(c)** krav til baggrundskontrol af leverandørers og tjenesteudbyderes ansatte, **(d)** en forpligtelse for leverandører og tjenesteudbydere til uden unødig forsinkelse at underrette de relevante enheder om hændelser, der udgør en risiko for sikkerheden i disse enheders net- og informationssystemer, **(e)** retten til audit eller retten til at modtage auditrapporter, **(f)** en forpligtelse for leverandører og tjenesteudbydere til at håndtere sårbarheder, der udgør en risiko for sikkerheden i de relevante enheders net- og informationssystemer, **(g)** krav vedrørende underentreprise og, såfremt de relevante enheder tillader underentreprise, cybersikkerhedskrav til underleverandører i overensstemmelse med de cybersikkerhedskrav, der er omhandlet i litra a), **(h)** leverandørernes og tjenesteudbydernes forpligtelser ved kontraktens ophør, såsom indhentning og sletning af oplysninger, som leverandørerne og tjenesteyderne har erhvervet i forbindelse med udførelsen af deres opgaver. De relevante enheder tager hensyn til de elementer, der er omhandlet i Gennemførselsforordningen pkt. 5.1.2 og 5.1.3, som led i udvælgelsesprocessen for nye leverandører og tjenesteudbydere samt som led i den udbudsproces, der er omhandlet i pkt. 6.1. (2024/2690, pkt. 5.1.2.. 5.1.3., 5.1.4. & 5.1.5.).	De relevante enheder gennemgår politikken for forsyningskædesikkerhed og overvåger, evaluerer og, hvor det er nødvendigt, reagerer på ændringer i leverandørernes og tjenesteudbydernes cybersikkerhedspraksis med planlagte mellemrum, samt når der sker væsentlige ændringer med hensyn til drift eller risici eller opstår væsentlige hændelser i forbindelse med leveringen af IKT-tjenester, eller når disse har indvirkning på sikkerheden i IKT-produkter fra leverandørerne og tjenesteudbyderne. Med henblik på Gennemførselsforordningen pkt. 5.1.6 skal de relevante enheder: (a) regelmæssigt overvåge rapporter om gennemførelsen af serviceleveranceaftalerne, hvor det er relevant (b) gennemgå hændelser i forbindelse med IKT-produkter og IKT-tjenester fra leverandører og tjenesteudbydere (c) vurdere behovet for spontane gennemgange og dokumentere resultaterne på en forståelig måde (d) analysere de risici, der følger af ændringer i forbindelse med IKT-produkter og IKTtjenester fra leverandører og tjenesteudbydere, og, hvis det er relevant, træffe afbødende foranstaltninger rettidigt (2024/2690, pkt. 5.1.6. & 5.1.7.).	**ISO 27001:2022** A.5.19, A.5.20, A.5.21, A.8.30	**NIST CSF v2.0** GV.OC-03, GV.OC-05, GV.SC-01, GV.SC-04, GV.SC-06, GV.SC-05, GV.SC-07, GV.SC-09, GV.SC-10, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 7.14.1	**CEN/TS 18026:2024** ISP-02, DEV-08, PM-01, PM-02, PM-04, PM-05
5.2. Fortegnelse over leverandører og tjenesteydere	De relevante enheder fører og ajourfører et register over deres direkte leverandører og tjenesteudbydere (2024/2690, pkt. 5.2.).	Registeret over leverandører og tjenesteudbydere skal minimum indeholde: (a) kontaktpunkter for hver direkte leverandør og tjenesteudbyder, (b) en liste over IKT-produkter, IKT-tjenester og IKT-processer, som den direkte leverandør eller tjenesteudbyder leverer til de relevante enheder (2024/2690, pkt. 5.2.).	Registeret over leverandører og tjenesteudbydere gennemgås regelmæssigt med henblik på at sikre kvaliteten af informationerne om leverandører og tjenesteudbydere og de produkter, de leverer, og registeret ajourføres om nødvendigt. (2024/2690, pkt. 5.2.)	**ISO 27001:2022** A.5.22	**NIST CSF v2.0** GV.OC-05, GV.SC-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.14.3-11X, REQ-7.14.3-12X, Clause 7.14.3	**CEN/TS 18026:2024** DEV-02, PM-03
6. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- oginformationssystemer							
6.1. Sikkerhed i forbindelse med erhvervelse af IKT-tjenester eller IKT-produkter	Med henblik på artikel 21, stk. 2, litra e), i direktiv (EU) 2022/2555 fastsætter og gennemfører de relevante enheder på grundlag af den risikovurdering, der foretages i henhold til Gennemførselsordningen pkt. 2.1, processer til styring af risici, der følger af erhvervelsen af IKTtjenester eller IKT-produkter til komponenter, der er kritiske for de relevante enheders sikkerhed i net- og informationssystemer, fra leverandører eller tjenesteudbydere i hele deres livscyklus (2024/2690, pkt. 6.1.1.).	Med henblik på Gennemførselsordningen pkt. 6.1.1 skal de i pkt. 6.1.1 omhandlede processer omfatte: (a) sikkerhedskrav til de IKT-tjenester eller IKT-produkter, der skal erhverves (b) krav vedrørende sikkerhedsopdateringer i hele IKT-tjenesternes eller IKTprodukternes levetid eller udskiftning, når de pågældende tjenester eller produkter ikke længere understøttes (c) oplysninger, der beskriver de hardware- og softwarekomponenter, der anvendes i IKTtjenesterne eller IKT-produkterne (d) oplysninger, der beskriver IKT-tjenesternes eller IKT-produkternes aktuelle cybersikkerhedsfunktioner og den konfiguration, der er nødvendig for en sikker drift heraf (e) sikkerhed for, at IKT-tjenesterne eller IKT-produkterne opfylder sikkerhedskravene i henhold til litra a) (f) metoder til validering af, at de leverede IKT-tjenester eller IKT-produkter opfylder de anførte sikkerhedskrav, samt dokumentation for resultaterne af validering (2024/2690, pkt. 6.1.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører processerne med planlagte mellemrum, samt når der opstår væsentlige hændelser (2024/2690, pkt. 6.1.3.).	**ISO 27001:2022** A.5.21, A.5.23	**NIST CSF v2.0** GV.PO-02, GV.SC-06, ID.RA-09, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.7-01, Clause 7.14.2	**CEN/TS 18026:2024** OIS-04, AM-03, DEV-02, DEV-07, PM-01
6.2. Sikker udviklingsproces	Inden der udvikles et net- og informationssystem, herunder software, fastsætter de relevante enheder regler for sikker udvikling af net- og informationssystemer og anvender dem, når de udvikler net- og informationssystemer internt eller outsourcer udviklingen af net- og informationssystemer. Reglerne skal dække alle udviklingsfaser, herunder specifikation, udformning, udvikling, indførelse og test (2024/2690, pkt. 6.2.1.).	Med henblik på Gennemførselsforordningen pkt. 6.2.1 skal de relevante enheder: (a) foretage en analyse af sikkerhedskravene i specifikations- og udformningsfasen af ethvert udviklings- eller erhvervelsesprojekt, der igangsættes af de relevante enheder eller på vegne af disse enheder (b) anvende principper for udformning af sikre systemer og principper for sikker kodning på alle aktiviteter i forbindelse med udvikling af informationssystemer såsom fremme af indbygget cybersikkerhed og zero trust-arkitektur (c) fastsætte sikkerhedskrav vedrørende udviklingsmiljøer (d) etablere og gennemføre processer til sikkerhedstest i hele udviklingsprocessen (e) på en passende måde udvælge, beskytte og forvalte data i forbindelse med sikkerhedstest (f) rense og anonymisere testdata i henhold til den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1. I forbindelse med outsourcet udvikling af net- og informationssystemer anvender de relevante enheder også de politikker og procedurer, der er omhandlet i Gennemførselsforordningen pkt. 5 og 6.1. (2024/2690, pkt. 6.2.2. & 6.2.3.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører med planlagte mellemrum deres regler for sikker udvikling (2024/2690, pkt. 6.2.4.).	**ISO 27001:2022** A.8.25, A.8.31	**NIST CSF v2.0** ID.AM-08, PR.PS-06, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.7-01, REQ-7.7-02, REQ-7.7-03, REQ-7.7-04, REQ-7.8-10	**CEN/TS 18026:2024** OIS-04, CCM-04, CCM-06, DEV-01, DEV-03, DEV-04, DEV-05, DEV-06
6.3. Konfigurationsstyring	De relevante enheder træffer passende foranstaltninger til at etablere, dokumentere, gennemføre og overvåge konfigurationer, herunder sikkerhedskonfigurationer af hardware, software, tjenester og net (2024/2690, pkt. 6.3.1.).	Med henblik på Gennemførselsforordningen pkt. 6.3.1 skal de relevante enheder: (a) fastlægge og sikre sikkerheden i konfigurationerne af deres hardware, software, tjenester og net (b) fastlægge og gennemføre processer og værktøjer til håndhævelse af de fastlagte sikre konfigurationer af hardware, software, tjenester og net for både nyinstallerede systemer og systemer, der er i drift i hele deres levetid (2024/2690, pkt. 6.2.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører konfigurationerne med planlagte mellemrum, eller når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 6.2.3.).	**ISO 27001:2022** A.8.9	**NIST CSF v2.0** PR.PS-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-6.3-08X, REQ-7.7-03, REQ-6.3-09X, REQ-7.7-08X,	**CEN/TS 18026:2024** OPS-21, PSS-03, PSS-04

6.4. Ændringsstyring, reparation og vedligeholdelse	De relevante enheder anvender ændringsstyringsprocedurer til at kontrollere ændringer af net- og informationssystemer. Hvor det er relevant, skal procedurerne være i overensstemmelse med de relevante enheders generelle politikker vedrørende ændringsstyring (2024/2690, pkt. 6.4.1.).	De procedurer, der er omhandlet i Gennemførselsforordningen pkt. 6.4.1, finder anvendelse på udgivelser, ændringer og nødændringer af enhver software og hardware, der er i drift, og på ændringer af konfigurationen. Procedurerne skal sikre, at disse ændringer dokumenteres og på grundlag af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, testes og vurderes i betragtning af de potentielle virkninger, inden de gennemføres. I tilfælde, hvor de regelmæssige ændringsstyringsprocedurer ikke kunne følges på grund af en nødsituation, skal de relevante enheder dokumentere resultatet af ændringen og begrundelsen for, hvorfor procedurerne ikke kunne følges (2024/2690, pkt. 6.4.2. & 6.4.3.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører procedurerne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer i forbindelse med drift eller risici (2024/2690, pkt. 6.4.4.).	**ISO 27001:2022** 6.3, 8.1, A.7.13, A.8.32	**NIST CSF v2.0** ID.RA-07, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.7-03, REQ-7.7-04, REQ-7.7-07X	**CEN/TS 18026:2024** ISP-03, CCM-01, CCM-02, CCM-03, CCM-04, CCM-05, CCM-06
6.5. Sikkerhedstest	De relevante enheder fastlægger, gennemfører og anvender en politik og procedurer for sikkerhedstest (2024/2690, pkt. 6.5.1.).	De relevante enheder: (a) fastlægger på grundlag af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, behovet for, omfanget af, hyppigheden af og typen af sikkerhedstest (b) udfører sikkerhedstest i henhold til en dokumenteret testmetode, der omfatter de komponenter, der i en risikoanalyse er udpeget som relevante for sikker drift (c) dokumenterer testenes type, omfang, tid og resultater, herunder med en vurdering af den kritiske betydning og en vurdering af afbødende foranstaltninger for hver konstatering (d) anvender afbødende foranstaltninger i tilfælde af alvorlige konstateringer (2024/2690, pkt. 6.5.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører deres sikkerhedstestningspolitikker med planlagte mellemrum (2024/2690, pkt. 6.5.3.).	**ISO 27001:2022** A.8.29, A.8.33, A.8.34	**NIST CSF v2.0** ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.8-10, REQ-7.8-13, REQ-7.8-14X, REQ-7.8-17X, REQ-7.8-18X, REQ-7.8-19X	**CEN/TS 18026:2024** ISP-02, OPS-19, DEV-01, DEV-04, DEV-06
6.6. Sikkerhedspatchstyring	De relevante enheder specificerer og anvender procedurer, der er i overensstemmelse med de procedurer for ændringsstyring, der er omhandlet i Gennemførselsforordningen pkt. 6.4.1, samt med sårbarhedsstyrings-, risikostyrings- og andre relevante styringsprocedurer (2024/2690, pkt. 6.6.1.).	Procedurerne skal sikre, at: (a) sikkerhedspatches anvendes inden for en rimelig periode, efter at de er blevet tilgængelige (b) sikkerhedspatches testes, inden de anvendes i systemer i produktionsmiljøet (c) sikkerhedspatches stammer fra pålidelige kilder, og deres integritet kontrolleres (d) der gennemføres yderligere foranstaltninger, og resterende risici accepteres i tilfælde, hvor en patch ikke er tilgængelig eller i henhold til Gennemførselsforordningen pkt. 6.6.2 ikke anvendes. Uanset punkt 6.6.1, litra a), kan de relevante enheder vælge ikke at anvende en given sikkerhedspatch, hvis ulemperne ved at anvende sikkerhedspatchen er større end cybersikkerhedsfordelene. De relevante enheder skal behørigt dokumentere og begrunde en sådan afgørelse (2024/2690, pkt. 6.6.1. & 6.6.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører procedurerne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer i forbindelse med drift eller risici. Punkterne i afsnit "6.6. Sikkerhedspatchstyring" skal være i overensstemmelse med punkt 6.4.1. Ved gennemgang skal punkterne 6.6.1., 6.6.2. samt 6.4.1. gennemgås i samme ombæring. (2024/2690, pkt. 6.6.)	**ISO 27001:2022** A.8.31, A.8.32	**NIST CSF v2.0** PR.PS-02, DE.CM-09, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.7-09	**CEN/TS 18026:2024** CCM-03, CCM-04, CCM-05, OPS-18
6.7. Netsikkerhed	De relevante enheder træffer passende foranstaltninger til at beskytte deres net- og informationssystemer mod cybertrusler (2024/2690, pkt. 6.7.1.).	Med henblik på Gennemførselsforordningen pkt. 6.7.1 skal de relevante enheder: (a) dokumentere nettets arkitektur på en forståelig og ajourført måde (b) fastlægge og anvende kontrolforanstaltninger til at beskytte de relevante enheders interne netdomæner mod uautoriseret adgang (c) konfigurere kontrolforanstaltninger til at forhindre adgang og netværkskommunikation, der ikke er nødvendig for driften af de relevante enheder (d) fastlægge og anvende kontrolforanstaltninger for fjernadgang til net- og informationssystemer, herunder tjenesteudbyderes adgang (e) undlade at anvende systemer, der anvendes til administration af gennemførelsen af sikkerhedspolitikken, til andre formål (f) udtrykkeligt forbyde eller deaktivere unødvendige forbindelser og tjenester (g) hvis det er relevant, udelukkende tillade adgang til de relevante enheders net- og informationssystemer fra udstyr, der er godkendt af disse enheder (h) kun tillade forbindelser mellem tjenesteudbydere og de relevante enheders systemer efter en anmodning om autorisering og i en bestemt periode, f.eks. varigheden af en vedligeholdelsesaktivitet (i) kun etablere kommunikation mellem særskilte systemer gennem pålidelige kanaler, der isoleres ved hjælp af logisk, kryptografisk eller fysisk adskillelse fra andre kommunikationskanaler og på sikker vis kan identificere deres slutpunkter og beskytte data i kanalen mod ændring eller videregivelse (j) vedtage en gennemførelsesplan for den fulde overgang til den seneste generation af kommunikationsprotokoller i netværkslaget på en sikker, hensigtsmæssig og gradvis måde og fastlægge foranstaltninger til at fremskynde en sådan overgang (k) vedtage en gennemførelsesplan for indførelse af internationalt aftalte og interoperable moderne e-mailkommunikationsstandarder for at sikre e-mailkommunikation og derved afbøde sårbarheder i forbindelse med e-mailrelaterede trusler og fastlægge foranstaltninger til at fremskynde en sådan indførelse (l) anvende bedste praksis for DNS-sikkerhed, internetroutingsikkerhed og routinghygiejne i forbindelse med trafik fra og til nettet (2024/2690, pkt. 6.7.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører disse foranstaltninger med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 6.7.3.).	**ISO 27001:2022** A.8.16, A.8.20	**NIST CSF v2.0** DE.CM-01, PR.IR-01, PR.PS-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.8	**CEN/TS 18026:2024** PS-04, CS-01, CS-02, CS-03, CS-06, CS-07, CS-08, PSS-02
6.8. Netsegmentering	De relevante enheder segmenterer systemer i net eller zoner i overensstemmelse med resultaterne af den risikovurdering, der er omhandlet i Gennemførselsforordningen pkt. 2.1. De opdeler deres systemer og net, så de er adskilt fra tredjeparters systemer og net (2024/2690, pkt. 6.8.1.).	De relevante enheder skal: (a) overveje de funktionelle, logiske og fysiske forhold, herunder placering, mellem pålidelige systemer og tjenester (b) give adgang til et net eller en zone på grundlag af en vurdering af nettets eller zonens sikkerhedskrav (c) placere systemer, der er kritiske for de relevante enheders drift eller for sikkerheden, i sikrede zoner (d) etablere en demilitariseret zone i deres kommunikationsnet for at sikre, at kommunikationen fra eller til deres netværk er sikker (e) begrænse adgangen og kommunikationen mellem og inden for zoner til det, der er nødvendigt for de relevante enheders drift eller for sikkerheden (f) adskille det dedikerede net til administration af net- og informationssystemerne fra de relevante enheders driftsnet (g) adskille netadministrationskanalerne fra anden nettrafik (h) adskille systemerne i produktionsmiljøet for de relevante enheders tjenester fra systemer, der anvendes til udvikling og test, herunder sikkerhedskopier (2024/2690, pkt. 6.8.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører netopdelingen med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer i forbindelse med drift eller risici (2024/2690, pkt. 6.8.3.).	**ISO 27001:2022** A.8.22	**NIST CSF v2.0** PR.IR-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.8-02	**CEN/TS 18026:2024** IAM-09, CS-02, CS-04, CS-05

6.9. Beskyttelse mod skadelig og uautoriseret software	De relevante enheder beskytter deres net- og informationssystemer mod skadelig og uautoriseret software (2024/2690, pkt. 6.9.1.).	Med henblik herpå gennemfører de relevante enheder navnlig foranstaltninger, der detekterer eller forhindrer brugen af skadelig eller uautoriseret software. De relevante enheder sikrer, hvis det er relevant, at deres net- og informationssystemer er udstyret med software til detektion og afhjælpning, og at det ajourføres regelmæssigt i overensstemmelse med den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, og de kontraktlige aftaler med udbyderne (2024/2690, pkt. 6.9.2.).	De relevante enheder gennemgår foranstaltningerne og evaluerer om de har været hensigtsmæssige i forhold til at beskytte net- og informationssystemer mod skadelig og uautoriseret software. (2024/2690, pkt. 6.9.)	**ISO 27001:2022** A.5.32, A.8.7	**NIST CSF v2.0** DE.CM-01, DE.CM-09, PR.PS-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.7-05	**CEN/TS 18026:2024** OPS-04, OPS-05, CS-03
6.10. Håndtering og offentliggørelse af sårbarheder	De relevante enheder indhenter oplysninger om tekniske sårbarheder i deres net- og informationssystemer, evaluerer deres eksponering for sådanne sårbarheder og træffer passende foranstaltninger til at håndtere sårbarhederne (2024/2690, pkt. 6.10.1.).	Med henblik på Gennemførselsforordningen pkt. 6.10.1 skal de relevante enheder: (a) overvåge oplysninger om sårbarheder gennem passende kanaler såsom meddelelser fra CSIRT'er, kompetente myndigheder eller oplysninger fra leverandører eller tjenesteudbydere (b) med planlagte intervaller foretage sårbarhedsscanninger, hvor det er relevant, og dokumentere resultaterne af scanningerne (c) uden unødig forsinkelse afhjælpe sårbarheder, som de relevante enheder har konstateret som værende af kritisk betydning for deres drift (d) sikre, at deres sårbarhedshåndtering er forenelig med deres procedurer for ændringsstyring, sikkerhedspatchstyring, risikostyring og hændelsesstyring (e) fastlægge en procedure for offentliggørelse af sårbarheder i overensstemmelse med den gældende nationale koordinerede politik for offentliggørelse af sårbarheder. De relevante enheder udarbejder og gennemfører en plan for at afhjælpe sårbarheden i tilfælde, hvor sårbarhedens potentielle indvirkning berettiger dette. I andre tilfælde dokumenterer og begrunder de relevante enheder årsagen til, at sårbarheden ikke kræver afhjælpning (2024/2690, pkt. 6.10.2. & 6.10.3.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører med planlagte mellemrum de kanaler, de anvender til overvågning af sårbarhedsoplysninger (2024/2690, pkt. 6.10.4.).	**ISO 27001:2022** A.8.8	**NIST CSF v2.0** ID.RA-01, ID.RA-02, ID.RA-04, ID.RA-05, ID.RA-06, PR.PS-02, PR.PS-03, ID.RA-08, ID.RA-06, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM- 04	**ETSI EN 319 401** REQ-7.8-13, REQ-7.8-14X, REQ-7.9.2-09X, REQ-7.9.2-10X, REQ-7.9.5-01X , REQ-7.9.5-02X	**CEN/TS 18026:2024** OIS-03, OPS-17, OPS-18, OPS-19, OPS-20, OPS-21, DEV-06
7. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici							
7. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici	Med henblik på artikel 21, stk. 2, litra f), i direktiv (EU) 2022/2555 fastlægger, gennemfører og anvender de relevante enheder en politik og procedurer til vurdering af, om de foranstaltninger til styring af cybersikkerhedsrisici, som den relevante enhed har truffet, gennemføres og opretholdes effektivt (2024/2690, pkt. 7.1.1.).	Der skal i den politik og de procedurer, der er omhandlet i Gennemførselsforordningen pkt. 7.1, tages hensyn til resultaterne af risikovurderingen i henhold til pkt. 2.1 og tidligere væsentlige hændelser. De relevante enheder fastlægger: (a) hvilke foranstaltninger til styring af cybersikkerhedsrisici der skal overvåges og måles, herunder processer og kontrolforanstaltninger (b) hvilke metoder der skal anvendes til passende overvågning, måling, analyse og evaluering for at sikre gyldige resultater (c) hvornår overvågningen og målingen skal udføres (d) hvem der er ansvarlig for at overvåge og måle effektiviteten af foranstaltningerne til styring af cybersikkerhedsrisici (e) hvornår resultaterne fra overvågningen og målingen skal analyseres og evalueres (f) hvem der skal analysere og evaluere disse resultater (2024/2690, pkt. 7.1.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken og procedurerne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer i forbindelse med drift eller risici (2024/2690, pkt. 7.1.3.).	**ISO 27001:2022** 6.2, 9.1, 9.3	**NIST CSF v2.0** ID.IM-03, GV.RM-06, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 5, ref. to ISO/IEC 27005:2022, REQ-7.9.5-03X, REQ-7.9.5-04X	**CEN/TS 18026:2024** ISP-02, OPS-20, C0-04
8. Grundlæggende cyberhygiejnepraksisser og sikkerhedsuddannelse							
8.1. Bevidstgørelse og grundlæggende cyberhygiejnepraksisser	Med henblik på artikel 21, stk. 2, litra g), i direktiv (EU) 2022/2555 sikrer de relevante enheder, at deres ansatte, herunder medlemmer af ledelsesorganer, samt direkte leverandører og tjenesteudbydere er opmærksomme på risici, underrettes om betydningen af cybersikkerhed og anvender cyberhygiejnepraksisser (2024/2690, pkt. 8.1.1.).	Med henblik på Gennemførselsforordningen pkt. 8.1.1 skal de relevante enheder tilbyde deres ansatte, herunder medlemmer af ledelsesorganer samt direkte leverandører og tjenesteydere, hvis det er relevant i overensstemmelse med pkt. 5.1.4, et bevidstgørelsesprogram, som: (a) planlægges over en periode, således at aktiviteterne gentages, og nye medarbejdere inddrages i dem (b) fastlægges i overensstemmelse med politikken for net- og informationssikkerhed, emnespecifikke politikker og relevante procedurer for net- og informationssikkerhed (c) omfatter relevante cybertrusler, de eksisterende foranstaltninger til styring af cybersikkerhedsrisici, kontaktpunkter og ressourcer til yderligere oplysning og rådgivning af brugere om cybersikkerhedsspørgsmål samt cyberhygiejnepraksis (2024/2690, pkt. 8.1.2.).	Bevidstgørelsesprogrammet testes med hensyn til effektivitet, hvor det er relevant. Bevidstgørelsesprogrammet ajourføres og tilbydes med planlagte mellemrum under hensyntagen til ændringer i cyberhygiejnepraksis, det nuværende trusselsbillede og risici for de relevante enheder (2024/2690, pkt. 8.1.3.).	**ISO 27001:2022** 7.3, A.6.3, A.8.7	**NIST CSF v2.0** PR.AT-01, PR.AT-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.2-01X, REQ-7.2-02, REQ-7.2-03X, REQ-7.2-04X, REQ-7.2-05X	**CEN/TS 18026:2024** HR-04, DOC-01
8.2. Sikkerhedsuddannelse	De relevante enheder udpeger medarbejdere, hvis roller kræver sikkerhedsrelevante færdigheder og ekspertise, og sikrer, at de modtager regelmæssig uddannelse i net- og informationssystemers sikkerhed. De relevante enheder udarbejder, gennemfører og anvender et uddannelsesprogram i overensstemmelse med politikken for net- og informationssikkerhed, de emnespecifikke politikker og andre relevante procedurer for net- og informationssikkerhed, hvori uddannelsesbehovene for visse roller og stillinger fastlægges på grundlag af kriterier (2024/2690, pkt. 8.2.1. & 8.2.2.).	Den uddannelse, der er omhandlet i Gennemførselsforordningen pkt. 8.2.1, skal være relevant for medarbejderens jobfunktion, og dens effektivitet skal vurderes. Uddannelsen skal tage hensyn til eksisterende sikkerhedsforanstaltninger og omfatte følgende: (a) instruktioner vedrørende sikker konfiguration og drift af net- og informationssystemer, herunder mobile enheder (b) orientering om kendte cybertrusler (c) uddannelse i hvad, der skal gøres, når der indtræffer sikkerhedsrelevante begivenheder. De relevante enheder skal uddanne medarbejdere, der overgår til nye stillinger eller roller, som kræver sikkerhedsrelevante færdigheder og ekspertise (2024/2690, pkt. 8.2.3. & 8.2.4.).	Programmet ajourføres og gennemføres regelmæssigt under hensyntagen til gældende politikker og regler, tildelte roller, ansvarsområder, kendte cybertrusler og den teknologiske udvikling (2024/2690, pkt. 8.2.5.).	**ISO 27001:2022** 7.2, A.6.3	**NIST CSF v2.0** PR.AT-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.2-04X, REQ-7.2-02, REQ-7.2-05X, REQ-7.2-07X, REQ-7.2-09X, REQ-7.2-12X	**CEN/TS 18026:2024** HR-04, PM-01

9. Kryptografi							
9. Kryptografi	Med henblik på artikel 21, stk. 2, litra h), i direktiv (EU) 2022/2555 fastlægger, gennemfører og anvender de relevante enheder en politik og procedurer vedrørende kryptografi for at sikre en passende og effektiv anvendelse af kryptografi til at beskytte fortroligheden, autenticiteten og integriteten af data i overensstemmelse med de relevante enheders klassifikation af aktiver og resultaterne af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1. (2024/2690, pkt. 9.1.).	Det er fastlagt. at: (a) typen, styrken og kvaliteten af de kryptografiske foranstaltninger, der er nødvendige for at beskytte de relevante enheders aktiver, herunder data i hvile og data under overførsel, i overensstemmelse med de relevante enheders klassifikation af aktiver (b) de protokoller eller typer af protokoller med udgangspunkt i litra a), der skal vedtages, samt de kryptografiske algoritmer, krypteringens styrke, de kryptografiske løsninger og den brugspraksis, der skal godkendes og kræves anvendt i enhederne efter en kryptografisk fleksibel tilgang, hvor dette er relevant (c) de relevante enheders tilgang til nøgleforvaltning, herunder, hvor det er relevant, metoder til følgende: i) generering af forskellige nøgler til kryptografiske systemer og applikationer ii) udstedelse og erhvervelse af offentlige nøglecertifikater iii) distribution af nøgler til de tilsigtede enheder, herunder hvordan nøgler aktiveres, når de modtages iv) opbevaring af nøgler, herunder hvordan autoriserede brugere får adgang til nøgler v) ændring eller ajourføring af nøgler, herunder regler om, hvornår og hvordan nøgler skal ændres vi) håndtering af kompromitterede nøgler vii)tilbagekaldelse af nøgler, herunder hvordan nøgler kaldes tilbage eller deaktiveres viii)genoprettelse af tabte eller beskadigede nøgler ix) backup eller arkivering af nøgler x) destruktion af nøgler xi) logning og revision af centrale ledelsesrelaterede aktiviteter xii) fastsættelse af aktiverings- og deaktiveringsdatoer for nøgler for at sikre, at nøglerne kun kan anvendes i den angivne periode i henhold til organisationens regler om nøgleforvaltning (2024/2690, pkt. 9.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører deres politik og procedurer med planlagte mellemrum under hensyntagen til det aktuelle tekniske niveau inden for kryptografi (2024/2690, pkt. 9.3.).	**ISO 27001:2022** A.5.31, A.8.24	**NIST CSF v2.0** PR.DS-01, PR.DS-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 7.5, ref. to clause 8.24 of ISO/IEC 27002:2022	**CEN/TS 18026:2024** ISP-02, CKM-01, CKM-02, CKM-03, CKM-04
10. Personalesikkerhed							
10.1. Personalesikkerhed	Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 sikrer de relevante enheder, at deres ansatte og direkte leverandører og tjenesteydere, hvor det er relevant, forstår og forpligter sig til deres sikkerhedsansvar, alt efter hvad der er relevant for de udbudte tjenester og jobbet, og i overensstemmelse med de relevante enheders politik for sikkerhed i net- og informationssystemer (2024/2690, pkt. 10.1.1.).	De omhandlede krav skal omfatte følgende: (a) mekanismer til at sikre, at alle ansatte, direkte leverandører og tjenesteudbydere, hvor det er relevant, forstår og følger den standardpraksis for cyberhygiejne, som enhederne anvender i henhold til Gennemførselsforordningen pkt. 8.1. (b) mekanismer til at sikre, at alle brugere med administrativ eller privilegeret adgang er bekendt med og handler i overensstemmelse med deres roller, ansvarsområder og bemyndigelser (c) mekanismer til at sikre, at medlemmer af ledelsesorganer forstår og handler i overensstemmelse med deres rolle, ansvarsområder og bemyndigelser med hensyn til sikkerheden i net- og informationssystemer (d) mekanismer til ansættelse af personale, der er kvalificeret til de respektive roller, såsom kontrol af jobreferencer, undersøgelsesprocedurer, validering af certificeringer eller skriftlige prøver (2024/2690, pkt. 10.1.2.).	De relevante enheder gennemgår med planlagte mellemrum og mindst én gang om året tildelingen af personale til specifikke roller som omhandlet i Gennemførselsforordningen pkt. 1.2 samt deres dertil afsatte menneskelige ressourcer. De ajourfører om nødvendigt tildelingen (2024/2690, pkt. 10.1.3.).	**ISO 27001:2022** 7.1, 7.2, A.6.2, A.6.3	**NIST CSF v2.0** PR.AT-02, GV.RR-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 7.2	**CEN/TS 18026:2024** HR-01, HR-02, HR-03
10.2. Baggrundskontrol	De relevante enheder sikrer i det omfang, det er muligt, at der foretages baggrundskontrol af deres ansatte og, hvor det er relevant, af direkte leverandører og tjenesteydere i overensstemmelse med Gennemførselsforordningen pkt. 5.1.4, hvis det er nødvendigt i forbindelse med deres rolle, ansvarsområder og autoriseringer (2024/2690, pkt. 10.2.1.).	De relevante enheder skal følgende: (a) indføre kriterier for de roller, ansvarsområder og bemyndigelser, der kun må udøves eller indehaves af personer, hvis baggrund er blevet kontrolleret (b) sikre, at der foretages den i Gennemførselsforordningen pkt. 10.2.1 omhandlede baggrundskontrol af disse personer, inden de begynder at udøve disse roller og myndigheder eller tildeles disse ansvarsområder, under hensyntagen til gældende love, forskrifter og etiske regler i forhold til de forretningsmæssige krav, klassifikationen af aktiver, jf. Gennemførselsforordningen pkt. 12.1, og de net- og informationssystemer, der skal tilgås, samt de opfattede risici (2024/2690, pkt. 10.2.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken med planlagte mellemrum og ajourfører den, hvor det er nødvendigt (2024/2690, pkt. 10.2.3.).	**ISO 27001:2022** A.6.1	**NIST VSF v2.0** GV.RR-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.2-09X, REQ-7.2-17	**CEN/TS 18026:2024** HR-02
10.3. Procedurer ved ophør eller ændring af ansættelsesforhold	De relevante enheder sikrer, at ansvarsområder og opgaver i forbindelse med sikkerheden i net- og informationssystemer, der forbliver gyldige efter ophør eller ændring af deres ansattes ansættelsesforhold, defineres og håndhæves kontraktligt (2024/2690, pkt. 10.3.1.).	De relevante enheder medtager i den enkeltes arbejds- og ansættelsesvilkår, kontrakt eller aftale de ansvarsområder og forpligtelser, der stadig er gældende efter ansættelsesforholdets eller kontraktens ophør, såsom fortrolighedsklausuler (2024/2690, pkt. 10.3.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører arbejds- og ansættelsesvilkår, kontrakt eller aftale de ansvarsområder og forpligtelser, der stadig er gældende efter ansættelsesforholdets eller kontraktens ophør, såsom fortrolighedsklausuler (2024/2690, pkt. 10.3.).	**ISO 27001:2022** A.6.5	**NIST CSF v2.0** GV.RR-04	**ETSI EN 319 401** REQ-7.3.2-07X, REQ-7.4-08X	**CEN/TS 18026:2024** HR-05, HR-06
10.4. Disciplinærprocedure	De relevante enheder etablerer, formidler og opretholder en disciplinærprocedure til håndtering af overtrædelser af politikker for sikkerheden i net- og informationssystemer (2024/2690, pkt. 10.4.1.).	Der skal i proceduren tages hensyn til relevante retlige, vedtægtsmæssige, kontraktmæssige og forretningsmæssige krav (2024/2690, pkt. 10.4.1.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører disciplinærproceduren med planlagte mellemrum, samt når det er nødvendigt på grund af juridiske ændringer eller væsentlige ændringer i forbindelse med drift eller risici (2024/2690, pkt. 10.4.2.).	**ISO 27001:2022** 5.28, A.6.4	**NIST CSF v2.0** ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.2-06X	**CEN/TS 18026:2024** HR-01

11. Adgangskontrol							
11.1. Politik for adgangskontrol	Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 fastlægger, dokumenterer og gennemfører de relevante enheder politikker for logisk og fysisk kontrol af adgangen til deres net- og informationssystemer på grundlag af forretningsmæssige krav samt krav til sikkerheden i net- og informationssystemer (2024/2690, pkt. 11.1.1.).	Politikkerne skal: (a) omhandle adgang for personer, herunder personale, besøgende og eksterne enheder såsom leverandører og tjenesteydere (b) omhandle for net- og informationssystemer (c) sikre, at der kun gives adgang til brugere, der er blevet behørigt autentificeret (2024/2690, pkt. 11.1.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikkerne med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 11.1.3.).	**ISO 27001:2022** A.5.15, A.7.2, A.8.3, A.8.21, A9	**NIST CSF v2.0** PR.AA-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.4-02X, REQ-7.4-09X, REQ-7.4-13X, REQ-7.4-01, REQ-7.4-06X, REQ-7.4-11X, REQ-7.4-20X	**CEN/TS 18026:2024** OIS-02, ISP-02, IAM-01
11.2. Forvaltning af adgangsrettigheder	De relevante enheder skal give, ændre, fjerne og dokumentere adgangsrettigheder til net og informationssystemer i overensstemmelse med den politik for adgangskontrol, der er omhandlet i Gennemførselsforordningen pkt. 11.1. (2024/2690, pkt. 11.2.1.).	De relevante enheder: (a) tildeler og tilbagekalder adgangsrettigheder på grundlag af "need to know"- princippet, "least privilege"-princippet og princippet om adskillelse af opgaver (b) sikrer, at adgangsrettighederne ændres derefter ved ophør eller ændring af ansættelsesforhold (c) sikrer, at adgangen til net- og informationssystemer autoriseres af de relevante personer (d) sikre, at adgangsrettighederne på passende vis tager højde for tredjeparters adgang, såsom besøgende, leverandører og tjenesteudbydere, navnlig ved at begrænse adgangsrettigheder i omfang og varighed (e) føre et register over tildelte adgangsrettigheder (f) logge forvaltningen af adgangsrettigheder (2024/2690, pkt. 11.2.2.).	De relevante enheder gennemgår adgangsrettighederne med planlagte mellemrum og ændrer dem på grundlag af organisatoriske ændringer. De relevante enheder dokumenterer resultaterne af deres gennemgang, herunder de nødvendige ændringer af adgangsrettighederne (2024/2690, pkt. 11.2.3.).	**ISO 27001:2022** A.5.3, A.5.18, A.9	**NIST CSF v2.0** PR.AA-05, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 7.4, REQ-7.9.1-04X	**CEN/TS 18026:2024** OIS-02, IAM-04, IAM-05, PSS-03, HR-05
11.3. Privilegerede konti og systemadministrationskonti	De relevante enheder fører politikker for forvaltning af privilegerede konti og systemadministrationskonti som led i den politik for adgangskontrol, der er omhandlet i Gennemførselsforordningen pkt. 11.1. (2024/2690, pkt. 11.3.1.).	Politikkerne skal: (a) indføres stærke identifikations-, autentificerings- (såsom multifaktor-autentificering) og autoriseringsprocedurer for privilegerede konti og systemadministrationskonti (b) oprettes særlige konti, der udelukkende skal anvendes til systemadministrationsaktiviteter, såsom installation, konfiguration, forvaltning eller vedligeholdelse (c) individualisere og begrænse systemadministrationsbeføjelserne i videst muligt omfang (d) fastsætte, at systemadministrationskonti kun anvendes til ved forbindelse til systemadministrationssystemer (2024/2690, pkt. 11.3.2.).	De relevante enheder gennemgår adgangsrettighederne til privilegerede konti og systemadministrationskonti med planlagte mellemrum, ændrer dem efter organisatoriske ændringer og dokumenterer resultaterne af gennemgangen, herunder nødvendige ændringer af adgangsrettighederne (2024/2690, pkt. 11.3.3.).	**ISO 27001:2022** A.8.2, A.8.18, A.9	**NIST CSF v2.0** ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.4-10X	**CEN/TS 18026:2024** ISP-02, IAM-05, IAM-06
11.4. Administrationssystemer	De relevante enheder skal begrænse (og kontrollere) anvendelsen af systemadministrationssystemer i overensstemmelse med den politik for adgangskontrol, der er omhandlet i Gennemførselsforordningen pkt. 11.1. (2024/2690, pkt. 11.4.1.).	De relevante enheder skal: (a) kun anvende systemadministrationssystemer til systemadministrationsformål og ikke til andre aktiviteter (b) logisk adskille disse systemer fra applikationssoftware, der ikke anvendes til systemadministrationsformål (c) beskytte adgangen til systemadministrationssystemer gennem autentificering og kryptering (2024/2690, pkt. 11.4.2.).	De relevante enheder kontrollerer om anvendelsen af systemadministrationssystemer sker i overensstemmelse med den politik for adgangskontrol, der er omhandlet i Gennemførselsforordningen pkt. 11.1. (2024/2690, pkt. 11.4.1.).	**ISO 27001:2022** A.8.2, A.8.18	**NIST CSF v2.0**	**ETSI EN 319 401** REQ-7.4-10X, REQ-7.4-02X, REQ-7.4-03X, REQ-7.4-04X, REQ-7.4-05X, REQ-7.8-08,	**CEN/TS 18026:2024** OIS-02, IAM-06, IAM-09
11.5. Identifikation	De relevante enheder forvalter hele livscyklussen for net- og informationssystemer og deres brugere (2024/2690, pkt. 11.5.1.).	Med henblik herpå skal de relevante enheder: (a) oprette unikke identiteter for net- og informationssystemer og deres brugere (b) forbinde en given brugeridentitet med en enkelt person (c) sikre tilsyn med identiteter i net- og informationssystemer (d) logge forvaltningen af identiteter. De relevante enheder må kun tillade identiteter, der er tildelt flere personer, såsom fælles identiteter, hvis dette er nødvendigt af forretningsmæssige eller driftsmæssige årsager og er underlagt en udtrykkelig godkendelsesproces og dokumenteres. De relevante enheder tager hensyn til identiteter, der er tildelt flere personer, i den ramme for styring af cybersikkerhedsrisici, der er omhandlet i Gennemførselsforordningens pkt. 2.1. (2024/2690, pkt. 11.5.2. & 11.5.3.).	De relevante enheder gennemgår regelmæssigt identiteterne for net- og informationssystemer og deres brugere og deaktiverer dem straks, hvis der ikke længere er behov for dem (2024/2690, pkt. 11.5.4.).	**ISO 27001:2022** A.5.16	**NIST CSF v2.0** PR.AA-01, PR.AA-05, PR.AC-02	**ETSI EN 319 401** REQ-7.4-11X, REQ-7.4-08X, REQ-7.4-12X, REQ-7.7-06X, REQ-7.9.1-04X	**CEN/TS 18026:2024** IAM-02, IAM-03, IAM-06
11.6. Autentificering	De relevante enheder indfører sikre autentificeringsprocedurer og -teknologier baseret på adgangsbegrænsninger og politikken for adgangskontrol (2024/2690, pkt. 11.6.1.).	De relevante enheder skal: (a) sikre, at autentificeringsstyrken er hensigtsmæssig i forhold til klassifikationen af det aktiv, der tilgås (b) kontrollere tildelingen til brugerne og forvaltningen af hemmelige autentificeringsoplysninger ved hjælp af en proces, der sikrer oplysningernes fortrolighed, herunder via rådgivning af personalet om passende håndtering af autentificeringsoplysninger (c) kræve ændring af autentificeringsoplysninger ved den indledende tildeling, med planlagte mellemrum og ved mistanke om, at oplysningerne er blevet kompromitteret (d) kræve nulstilling af autentificeringsoplysninger og blokering af brugere efter et på forhånd fastsat antal mislykkede loginforsøg (e) afslutte inaktive sessioner efter en på forhånd fastsat periode med inaktivitet og (f) kræve særskilte autentificeringsoplysninger for adgang til privilegerede konti eller administrationskonti. De relevante enheder anvender i det omfang, det er muligt, de nyeste autentificeringsmetoder i overensstemmelse med den tilknyttede vurderede risiko og klassifikationen af det aktiv, der tilgås, samt unikke autentificeringsoplysninger (2024/2690, pkt. 11.6.2. & 11.6.3.).	De relevante enheder gennemgår autentificeringsprocedurerne og -teknologierne med planlagte mellemrum (2024/2690, pkt. 11.6.4.).	**ISO 27001:2022** A.5.17	**NISTCSF v2.0** PR.AA-05, PR.AA-03, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.4-02X, REQ-7.4-05X, REQ-7.7-06X, REQ-7.4-11X	**CEN/TS 18026:2024** IAM-07, IAM-08
11.7. Multifaktor-autentificering	Med henblik på artikel 21, stk. 2, litra j), i direktiv (EU) 2022/2555 implementerer de relevante enheder løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video-, og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant (L 333/80, artikel 21, stk. 2, litra j).	De relevante enheder sikrer, at brugerne autentificeres ved hjælp af flere autentificeringsfaktorer eller mekanismer til kontinuerlig autentificering, når de forsøger at tilgå enhedernes net- og informationssystemer, hvor det er relevant, i overensstemmelse med klassifikationen af det aktiv, der tilgås (2024/2690, pkt. 11.7.1.) .	De relevante enheder sikrer, at autentificeringsstyrken er hensigtsmæssig i forhold til klassifikationen af det aktiv, der tilgås (2024/2690, pkt. 11.7.2.).	**ISO 27001:2022** A.8.5	**NIST CSF v2.0** PR.AA-03	**ETSI EN 319 401** REQ-7.4-05X, REQ-7.4-06X, ref. to clause 2 of CA/Browser Forum network security guide	**CEN/TS 18026:2024** OPS-23, IAM-06, IAM-07

12. Forvaltning af aktiver							
12.1. Klassifikation af aktiver	Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 fastsætter de relevante enheder klassifikationsgrader med henblik på det krævede beskyttelsesniveau for alle aktiver, herunder oplysninger, der er omfattet af deres net- og informationssystemer (2024/2690, pkt. 12.1.1.).	De relevante enheder skal: (a) fastlægge et system med klassifikationsgrader for aktiver (b) knytte alle oplysninger og aktiver til en klassifikationsgrad på grundlag af krav om fortrolighed, integritet, autenticitet og tilgængelighed for at angive det påkrævede beskyttelsesniveau i forhold til deres følsomhed, kritiske betydning, risiko og forretningsværdi (c) tilpasse tilgængelighedskravene til aktiverne til de leverings- og genopretningsmål, der er fastsat i deres driftskontinuitets- og katastrofeberedskabsplaner (2024/2690, pkt. 12.1.2.).	De relevante enheder foretager regelmæssige gennemgange af klassifikationsniveauerne for aktiver og ajourfører dem, hvor det er relevant (2024/2690, pkt. 12.1.3.).	**ISO 27001:2022** A.5.9, A.5.12, A.5.13	**NIST CSF v2.0** ID.AM-05	**ETSI EN 319 401** REQE-7.3.2-01X, REQ-7.3.2-02X, REQ-7.3.2-03X, REQ-7.3.2-04X, REQ-7.3.2-05X, REQ-7.3.2-06X, REQ-7.3.2-07X	**CEN/TS 18026:2024** AM-05
12.2. Håndtering af aktiver	De relevante enheder fastlægger, gennemfører og anvender en politik for korrekt håndtering af aktiver, herunder oplysninger, i overensstemmelse med deres politik for net- og informationssikkerhed og formidler politikken for korrekt håndtering af aktiver til enhver, der anvender eller håndterer aktiver (2024/2690, pkt. 12.2.1.).	Politikken skal: (a) dække aktivernes fuldstændige livscyklus, herunder erhvervelse, anvendelse, opbevaring, transport og bortskaffelse (b) indeholde regler om sikker anvendelse, sikker opbevaring, sikker transport og uigenkaldelig sletning og destruktion af aktiverne (c) indeholde bestemmelser om, at overførsler skal finde sted på en sikker måde i overensstemmelse med den type aktiv, der overføres (2024/2690, pkt. 12.2.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 12.2.3.).	**ISO 27001:2022** A.5.9, A.5.10, A.5.14, A.7.10	**NIST CSF v2.0** ID.IM-01	**ETSI EN 319 401** REQ-7.3.2-06X, REQ-7.3.3-01X, REQ-7.3.3-02X, REQ-7.3.3-03X	**CEN/TS 18026:2024** ISP-02, AM-02, AM-03
12.3. Politik om mobile medier	De relevante enheder fastlægger, gennemfører og anvender en politik for forvaltning af mobile lagringsmedier og formidler den til deres ansatte og de tredjeparter, der håndterer mobile lagringsmedier i de relevante enheders lokaler eller andre steder, hvor de mobile medier tilsluttes de relevante enheders net- og informationssystemer (2024/2690, pkt. 12.3.1.).	Politikken skal: (a) fastsætte et teknisk forbud mod tilslutning af mobile medier, medmindre der er en organisatorisk begrundelse for deres anvendelse (b) indeholde bestemmelser om deaktivering af autoeksekvering fra sådanne medier og scanning af medierne for skadelig kode, inden de anvendes i enhedernes systemer (c) indeholde foranstaltninger til kontrol og beskyttelse af bærbare lagringsenheder, der indeholder data, mens de er i transit eller under opbevaring (d) hvor det er relevant, indeholde foranstaltninger om anvendelse af kryptografiske teknikker for at beskytte oplysninger på mobile lagringsmedier (2024/2690, pkt. 12.3.2.).	De relevante enheder gennemgår og, hvis det er relevant, ajourfører politikken med planlagte mellemrum, samt når der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 12.3.3.).	**ISO 27001:2022** A.7.7, A.7.10	**NIST CSF v2.0** PR.DS-01, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.3.3-01X, REQ-7.3.3-02X, REQ-7.3.3-03X	**CEN/TS 18026:2024** ISP-02, AM-02, PS-04
12.4. Fortegnelse over aktiver	De relevante enheder udarbejder og vedligeholder en fuldstændig, nøjagtig, ajourført og konsekvent fortegnelse over deres aktiver. De registrerer ændringer i fortegnelsen på en sporbar måde (2024/2690, pkt. 12.4.1.).	Detaljeringsgraden af fortegnelsen over aktiver skal modsvare de relevante enheders behov. Fortegnelsen skal omfatte følgende: (a) en liste over aktiviteter og tjenesteydelser og beskrivelser heraf (b) en liste over net- og informationssystemer og andre tilknyttede aktiver, der understøtter enhedernes drift og tjenester (2024/2690, pkt. 12.4.2.).	De relevante enheder reviderer og ajourfører regelmæssigt fortegnelsen og deres aktiver og dokumenterer ændringernes historik (2024/2690, pkt. 12.4.3.).	**ISO 27001:2022** A.5.9	**NIST CSF v2.0** ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-07, ID.AM-08, ID.IM-01, ID.IM-	**ETSI EN 319 401** Clause 7.3	**CEN/TS 18026:2024** AM-04
12.5. Deponering, tilbagelevering eller sletning af aktiver ved ophør af ansættelsesforhold	De relevante enheder etablerer procedurer, der beskriver håndteringen af de af aktiver, som er i personalets varetægt (2024/2690, pkt. 12.5.).	De relevante enheder indfører, gennemfører og anvender procedurer, der sikrer, at de af deres aktiver, som er i personalets varetægt, deponeres, tilbageleveres eller slettes ved ansættelsesforholdets ophør, og dokumenterer deponering, tilbagelevering og sletning af disse aktiver. I tilfælde, hvor deponering, tilbagelevering eller sletning af aktiver ikke er mulig, sikrer de relevante enheder, at aktiverne ikke længere kan anvendes til at tilgå de relevante enheders net- og informationssystemer i overensstemmelse med Gennemførselsforordningen pkt. 12.2.2. (2024/2690, pkt. 12.5.).	De relevante enheder gennemgår med planlagte mellemrum og, hvis det er relevant, ajourfører deres procedurer for håndtering af aktiver, som er i personalets varetægt. (2024/2690, pkt. 12.5.)	**ISO 27001:2022** A.5.11, A.5.18, A.8.24	**NIST CSF v2.0**	**ETSI EN 319 401** REQ-7.3.2-07X, REQ-7.3.3-01X, REQ-7.3.3-02X, REQ-7.3.3-03X, REQ-7.4-08X	**CEN/TS 18026:2024** AM-01
13. Miljømæssig og fysisk sikkerhed							
13.1. Understøttende forsyningstjenester	Med henblik på artikel 21, stk. 2, litra c), i direktiv (EU) 2022/2555 forebygger de relevante enheder tab, beskadigelse eller kompromittering af net- og informationssystemer samt afbrydelse af deres drift som følge af svigt eller forstyrrelse af de understøttende forsyningstjenester (2024/2690, pkt. 13.1.1.).	Med henblik herpå skal de relevante enheder, hvor det er relevant: (a) beskytte anlæg mod strømsvigt og andre forstyrrelser som følge af mangler i de understøttende forsyningstjenester såsom elektricitet, telekommunikation, vandforsyning, gas, spildevand, ventilation og klimaanlæg (b) overveje anvendelsen af reservekapacitet i forbindelse med forsyningstjenester (c) beskytte forsyningstjenesterne for elektricitet og telekommunikation, som transporterer data eller forsyner net- og informationssystemerne, mod aflytning og beskadigelse. (d) overvåge de forsyningstjenester, der er omhandlet i litra c), og rapportere begivenheder uden for de minimums- og maksimumskontroltærskler, der er omhandlet i Gennemførselsforordningen pkt. 13.2.2, litra b), og som påvirker forsyningstjenesterne, til det kompetente interne eller eksterne personale. (e) indgå kontrakter om nødforsyning med tilsvarende tjenester, f.eks. brændstof til nødstrømforsyning (f) overvåge, vedligeholde og teste forsyningen til de net- og informationssystemer, der er nødvendige for driften af den tjeneste, der tilbydes, navnlig el-, temperatur- og fugtighedskontrol, telekommunikation og internetforbindelse, samt sikre, at de nævnte systemer fungerer kontinuerligt (2024/2690, pkt. 13.1.2.).	De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører beskyttelsesforanstaltningerne regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 13.1.3.).	**ISO 27001:2022** A. 7.11	**NIST CSF v2.0** DE.CM-02, DE.CM-06, GV.OC-03, GV.OC-05, GV.OC-07, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** REQ-7.6-03, REQ-7.6-05, REQ-7.11.2-01X, REQ-7.11.2-02X, For network connections REQ-7.8-12	**CEN/TS 18026:2024** PS-05
13.2. Beskyttelse mod fysiske og miljømæssige trusler	Med henblik på artikel 21, stk. 2, litra e), i direktiv (EU) 2022/2555 skal de relevante enheder på grundlag af resultaterne af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, forebygge eller mindske konsekvenserne af begivenheder, der skyldes fysiske og miljømæssige trusler, såsom naturkatastrofer og andre forsætlige eller uforsætlige trusler (2024/2690, pkt. 13.2.1.).	De relevante enheder skal, hvor det er relevant: (a) udforme og gennemføre foranstaltninger til beskyttelse mod fysiske og miljømæssige trusler (b) fastsætte minimums- og maksimumskontroltærskler for fysiske og miljømæssige trusler (c) overvåge miljømæssige parametre og rapportere begivenheder uden for de i litra b) omhandlede minimums- og maksimumskontroltærskler til det kompetente interne eller eksterne personale (2024/2690, pkt. 13.2.2.).	De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører foranstaltningerne til beskyttelse mod fysiske og miljømæssige trusler regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 13.2.3.).	**ISO 27001:2022** A. 7.3, A.7.5	**NIST CSF v2.0** PR.IR-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**ETSI EN 319 401** Clause 7.6	**CEN/TS 18026:2024** PS-05

13.3. Perimeterkontrol og fysisk adgangskontrol	Med henblik på artikel 21, stk. 2, litra i), i direktiv (EU) 2022/2555 skal de relevante enheder forebygge og overvåge uautoriseret fysisk adgang til, beskadigelse af og indgreb i deres net- og informationssystemer (2024/2690, pkt. 13.3.1.).	De relevante enheder skal: (a) på grundlag af den risikovurdering, der foretages i henhold til Gennemførselsforordningen pkt. 2.1, fastlægge og anvende sikkerhedsperimetre til at beskytte områder, hvor net- og informationssystemer og andre tilknyttede aktiver befinder sig (b) beskytte de områder, der er omhandlet i litra a), ved hjælp af passende adgangskontrol og adgangspunkter (c) udforme og gennemføre foranstaltninger til fysisk sikkerhed i kontorer, lokaler og faciliteter (d) løbende overvåge deres lokaler for uautoriseret fysisk adgang (2024/2690, pkt. 13.3.2.).	De relevante enheder tester, gennemgår og, hvis det er relevant, ajourfører foranstaltningerne til fysisk adgangskontrol regelmæssigt, samt efter der opstår væsentlige hændelser eller sker væsentlige ændringer med hensyn til drift eller risici (2024/2690, pkt. 13.3.3.).	**ISO 27001:2022** A. 7.1, A.7.2, A.7.4	**NIST CSF v2.0** PR.AA-06, DE.CM-02	**ETSI EN 319 401** Clause 7.6	**CEN/TS 18026:2024** PS-01, PS-02, PS-03, PS-04