18.11.2025

CRA valmistajan velvoitteet ja ENISAN kartoitusdokumenttiin perustuvat suuntaa antavat vaatimukset

Tässä dokumentissa kuvataan CRA:n velvoitteet valmistajille, CRA:n vaatimuskohdat ja suuntaa antavat ulkoiset vaatimukset, jotka on koostettu ENISA Cyber Resilience Act Requirements Standards Mapping pohjalta: Cyber Resilience Act Requirements Standards Mapping - final_with_identifiers_0.pdf. Liikenne- ja viestintävirasto toteaa selvyyden vuoksi, että tämä kooste ei ole kattava listaus vaatimuksista vaan tarkoitus on neuvoa ylätasolla tämänhetkisestä tilanteesta. Oikeudellisesti sitovat velvoitteet säädetään asetuksessa, komission täytäntöönpanosäädöksissä sekä yhdenmukaistetuissa standardeissa ja teknisissä eritelmissä.

Ohjelmistokehitys		**Suuntaa antava ulkoinen vaatimus (ENISA Cyber Resilience Act Requirements Standards Mapping); Työn alla olevat harmonisoidut standardit täydentävät**
Valmistaja	**CRA:n kohta**	
Turvallisuuden huomioiminen alusta alkaen ja rakentaminen sisään tuotteeseen sen koko elinkaaren ajaksi.	Liite I, Osa I: 1) | Digitaalisia elementtejä sisältävät tuotteet on suunniteltava, kehitettävä ja tuotettava siten, että niiden kyberturvallisuuden taso on oikeassa suhteessa riskeihin.	EN ISO/IEC 27001:2022 (ISMS) EN ISO/IEC 27002:2022 (tietoturvakontrollit) EN ISO/IEC 27005:2022 (riskienhallinta) EN IEC 62443-4-1:2018 (Secure product development lifecycle) EN IEC 62443-3-2:2020 (Risk assessment IACS)
Ei tunnettuja hyväksikäytettäviä haavoittuvuuksia julkaisun hetkellä	Liite I, Osa I: 2) | Digitaalisia elementtejä sisältävien tuotteiden on tämän asetuksen 13 artiklan 2 kohdassa tarkoitetun kyberturvallisuusriskien arvioinnin perusteella ja soveltuvin osin täytettävä seuraavat vaatimukset: | a) | ne on asetettava saataville markkinoilla ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia;	EN ISO/IEC 30111:2019 (Vulnerability handling) EN ISO/IEC 29147:2020 (Vulnerability disclosure) EN ISO/IEC 18045:2022 (Evaluation assurance methodology) ITU-T X.1214:2018 (Vulnerability assessment)

Turvallinen oletuskonfiguraatio ja palautus alkuasetuksiin (secure by default)	Liite I, Osa I, 2) b) ne on asetettava saataville markkinoilla oletusarvoisesti tietoturvallisin asetuksin, jolleivät valmistaja ja yrityskäyttäjä ole digitaalisia elementtejä sisältävän räätälöidyn tuotteen osalta sopineet toisin, ja ne on voitava palauttaa alkuperäiseen tilaansa;	ETSI EN 303 645 V2.1.1:2020 (IoT baseline security) ISO/IEC 18031:2011 (Random bit generation, secure default parameters)
SBOM: komponenttien ja haavoittuvuuksien dokumentointi	Liite I, Osa II, 1) tunnistettava ja dokumentoitava digitaalisia elementtejä sisältävään tuotteeseen sisältyvät haavoittuvuudet ja komponentit muun muassa laatimalla vähintään tuotteiden ylimmän tason riippuvuudet kattava ohjelmistojen materiaaliluettelo yleisesti käytetyssä ja koneluettavassa muodossa Artikla 13, kohta 24: Komissio voi antaa täytäntöönpanoasetuksen SBOM:n muodosta ja osatekijöistä.	EN ISO/IEC 30111:2019 EN ISO/IEC 29147:2020
Haavoittuvuuksien hallinta ja korjaaminen viipymättä	Liite I, Osa II, 2) digitaalisia elementtejä sisältäviin tuotteisiin kohdistuvien riskien yhteydessä puututtava haavoittuvuuksiin ja korjattava ne viipymättä, esimerkiksi tarjoamalla tietoturvapäivityksiä; jos se on teknisesti mahdollista, uudet tietoturvapäivitykset on tarjottava erillään toimintopäivityksistä	EN ISO/IEC 30111:2019 EN ISO/IEC 29147:2020
Haavoittuvuuksien julkistaminen ja tiedottaminen	Liite I, Osa II, 4) kun tietoturvapäivitys on asetettu saataville, jaettava ja julkistettava tiedot korjatuista haavoittuvuuksista, mukaan lukien kuvaus haavoittuvuuksista, tiedot, joiden avulla käyttäjät voivat tunnistaa kyseisen digitaalisia elementtejä sisältävän tuotteen, haavoittuvuuksien vaikutukset ja vakavuus sekä selkeät ja saavutettavat tiedot,	EN ISO/IEC 29147:2020

	jotka auttavat käyttäjiä korjaamaan haavoittuvuudet; asianmukaisesti perustelluissa tapauksissa, joissa valmistajat pitävät julkistamisen turvallisuusriskejä sen turvallisuushyötyjä merkittävämpinä, ne voivat lykätä korjattua haavoittuvuutta koskevien tietojen julkistamista, kunnes käyttäjille on annettu mahdollisuus asentaa asiaankuuluva korjaava päivitys	
Koordinoidun haavoittuvuuksien vastuullisen ilmoittamisen (CVD) politiikka	Liite I, Osa II, 5) otettava käyttöön koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet ja valvottava niiden noudattamista	EN ISO/IEC 29147:2020
Haavoittuvuuksien ilmoitusyhteyspiste (Single Point of Contact)	Liite I, Osa II, 6) toteutettava toimenpiteitä, joilla helpotetaan tietojen jakamista oman digitaalisia elementtejä sisältävän tuotteensa ja kyseisen tuotteen sisältämien kolmannen osapuolen komponenttien mahdollisista haavoittuvuuksista, muun muassa ilmoittamalla yhteysosoite digitaalisia elementtejä sisältävässä tuotteessa havaittujen haavoittuvuuksien raportointia varten Liite II, 2) keskitetty yhteyspiste, johon voi ilmoittaa ja josta saa tietoja digitaalisia elementtejä sisältävän tuotteen haavoittuvuuksista ja josta löytyvät valmistajan soveltamat koordinoitua haavoittuvuuksien julkistamista koskevat periaatteet	EN ISO/IEC 30111:2019
Tietoturvapäivitysten turvallinen ja maksuton jakelu	Liite I, Osa II, 7) huolehdittava mekanismeista digitaalisia elementtejä sisältävien tuotteiden päivitysten tietoturvallisen jakelun	EN ISO/IEC 30111:2019 EN IEC 62443-4-1:2018

	varmistamiseksi, jotta haavoittuvuudet korjataan tai niiden vaikutuksia lievennetään pikaisesti ja tietoturvapäivitysten tapauksessa soveltuvin osin automaattisesti Liite I, Osa II, 8) varmistettava, että jos havaittujen tietoturvaongelmien ratkaisemiseksi on saatavilla tietoturvapäivityksiä, niitä levitetään viipymättä ja, jolleivat valmistaja ja yrityskäyttäjä ole digitaalisia elementtejä sisältävän räätälöidyn tuotteen osalta sopineet toisin, maksutta ja että niihin liitetään tarvittavat ohjeet, myös mahdollisista käyttäjältä edellytettävistä toimista	
Kyberturvallisuus		
Valmistaja	**CRA:n kohta**	
Suojata tuotteet tunnettujen kyberturvauhkien mukaan (esim. salaus, vahva tunnistautuminen, käyttöoikeuksien hallinta, lokitus ja valvonta, suojautuminen haittaohjelmia vastaan)	Liite I, Osa I, 1) Digitaalisia elementtejä sisältävät tuotteet on suunniteltava, kehitettävä ja tuotettava siten, että niiden kyberturvallisuuden taso on oikeassa suhteessa riskeihin.	EN ISO/IEC 27002:2022 (turvallisuusohjaus, kontrollit: autentikointi, pääsynhallinta), EN ISO/IEC 27002:2022 EN IEC 62443-4-2:2019 (Technical security requirements for IACS components) ISO/IEC 9798 (Osat 1–6, authentication mechanisms, ETSI EN 303 645 IoT-ympäristössä EN IEC 62443-4-1:2018 (tuotekehityksen ohjeet, uhkamallinnus)
Varmistaa, että tuote on suojattu luvattomalta käytöltä asianmukaisilla valvontamekanismeilla, kuten todennuksella, identiteetin- ja pääsynhallinnalla, sekä ilmoittaa käyttäjälle mahdollisesta luvattomasta käytöstä.	Liite I Osa I, 2) d niissä on varmistettava suojaaminen luvattomalta käytöltä asianmukaisin valvontamekanismein, joita sovelletaan muun muassa todennus-, identiteetinhallinta- tai pääsynhallintajärjestelmiin, ja ilmoitettava mahdollisesta luvattomasta käytöstä;	EN ISO/IEC 27002:2022 (valvonta, lokitus), standardit valvonnasta ja tapahtumien käsittelystä; EN IEC 62443-4-2:2019 ETSI EN 303 645
Suojata henkilötietojen ja muiden tietojen luottamuksellisuus käyttämällä uusimman	Liite I Osa I, 2) e niissä on suojattava tallennettujen, siirrettyjen tai muulla tavoin käsiteltyjen henkilötietojen tai	EN ISO/IEC 27001:2022 - EN ISO/IEC 27002:2022 - ISO/IEC 27701:2019 (Privacy extension to ISMS)

tekniikan mukaisia mekanismeja, kuten salausmenetelmiä, tiedonsiirron ja tietojen tallennuksen aikana.	muiden tietojen luottamuksellisuus esimerkiksi salaamalla asiaankuuluvat tiedot uusimman tekniikan mukaisilla mekanismeilla tietoja siirrettäessä tai säilytettäessä ja käyttämällä muita teknisiä keinoja;	
Suojata tallennetut, siirretyt ja muutoin käsitellyt henkilötiedot ja muut tiedot sekä komennot, ohjelmat ja asetukset luvattomalta manipuloinnilta tai muuttamiselta ja ilmoittaa käyttäjälle mahdollisesta turmeltumisesta.	Liite I Osa I, 2) f niissä on suojattava tallennettujen, siirrettyjen tai muulla tavoin käsiteltyjen henkilötietojen tai muiden tietojen eheys, komennot, ohjelmat ja asetukset kaikelta manipuloinnilta tai muuttamiselta, johon käyttäjä ei ole antanut lupaa, ja ilmoitettava turmeltumisesta	EN ISO/IEC 27002:2022 EN IEC 62443-4-2:2019
Huolehtia siitä, että tuotteessa käsitellään asianmukaisia, olennaisia ja käyttötarkoituksen kannalta tarpeellisia tietoja eli toteuttaa tietojen minimointi.	Liite I Osa I, 2) g niissä on käsiteltävä ainoastaan sellaisia henkilötietoja tai muita tietoja, jotka ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa digitaalisia elementtejä sisältävän tuotteen käyttötarkoitukseen (tietojen minimointi)	EN ISO/IEC 27002:2022 ISO/IEC 27701:2019 ETSI TS 103 485 V1.1.1:2020 (Privacy assurance)
Varmistaa tuotteen keskeisten toimintojen ja perustoimintojen saatavuus myös poikkeustilanteissa ja toteuttaa toimenpiteitä, joilla ehkäistään ja lievennetään palvelunestohyökkäysten vaikutuksia	Liite I Osa I, 2) h niissä on suojattava olennaisten toimintojen ja perustoimintojen saatavuus, myös poikkeaman jälkeen, mihin kuuluvat myös palvelunestohyökkäysten varalta toteutettavat häiriönsietokykyä parantavat ja hyökkäysten vaikutuksia lieventävät toimenpiteet	ISO/IEC 27002:2022 EN IEC 62443-4-2:2019 ETSI EN 303 645 V2.1.1 (2020-06)
Minimoida tuotteen ja siihen liitettyjen laitteiden kielteinen vaikutus muiden laitteiden ja verkkojen tarjoamien palvelujen saatavuuteen	Liite I Osa I, 2) i niissä on minimoitava kielteinen vaikutus, joka tuotteilla itsellään tai verkkoon liitetyillä laitteilla on muiden laitteiden tai verkkojen tarjoamien palvelujen saatavuuteen	EN IEC 62443-4-2:2019 ETSI EN 303 645

Suunnitella, kehittää ja tuottaa tuote siten, että sen hyökkäyspinta, kuten ulkoiset rajapinnat, on mahdollisimman pien	Liite I Osa I, 2) j ne on suunniteltava, kehitettävä ja tuotettava siten, että hyökkäyspintoja, kuten ulkoisia rajapintoja, on mahdollisimman vähän;	EN IEC 62443-4-2:2019 ETSI EN 303 645
Suunnitella, kehittää ja tuottaa tuote siten, että poikkeamien vaikutukset pysyvät mahdollisimman vähäisinä hyödyntämällä tarkoituksenmukaisia vaikutusten lieventämismekanismeja ja -tekniikoita	Liite I Osa I, 2) k ne on suunniteltava, kehitettävä ja tuotettava siten, että poikkeaman vaikutukset pidetään mahdollisimman vähäisinä käyttäen asianmukaisia haavoittuvuuden hyödyntämisen vaikutusten lieventämismekanismeja ja -tekniikoita	ISO/IEC 27002:2022
Tuottaa tietoturvaan liittyvää informaatiota tallentamalla ja seuraamalla tuotteen sisäistä toimintaa, kuten tietojen, palvelujen tai asetusten käyttöä ja muutoksia, sekä tarjota käyttäjälle estomekanismi	Liite I Osa I, 2) l niiden on tuotettava tietoturvaan liittyvää informaatiota tallentamalla ja seuraamalla asiaan liittyvää sisäistä toimintaa, kuten tietojen, palvelujen tai toimintojen käyttöä tai muutoksia, sekä tarjottava käyttäjän käyttöön estomekanismi	ISO/IEC 27002:2022
Tarjoaa käyttäjille mahdollisuus poistaa kaikki tiedot ja asetukset pysyvästi turvallisella ja helpolla tavalla sekä varmistaa, että tietojen siirtäminen toisiin tuotteisiin tai järjestelmiin on mahdollista ja tapahtuu turvatusti	Liite I Osa I, 2) m tarjottava käyttäjille mahdollisuus poistaa kaikki tiedot ja asetukset pysyvästi turvallisella ja helpolla tavalla ja, jos tällaisia tietoja voidaan siirtää muihin tuotteisiin tai järjestelmiin, varmistettava, että tämä tapahtuu turvatusti.	EN ISO/IEC 27002:2022 ISO/IEC 27701:2019
Turvalliset päivitys- ja korjausmenetelmät	Liite I, Osa II, 2) digitaalisia elementtejä sisältäviin tuotteisiin kohdistuvien riskien yhteydessä puututtava haavoittuvuuksiin ja korjattava ne viipymättä, esimerkiksi tarjoamalla tietoturvapäivityksiä; jos se on teknisesti mahdollista, uudet tietoturvapäivitykset on tarjottava erillään toimintopäivityksistä	EN ISO/IEC 30111:2019 EN IEC 62443-4-1:2018

	Liite I, Osa II, 7) huolehdittava mekanismeista digitaalisia elementtejä sisältävien tuotteiden päivitysten tietoturvallisen jakelun varmistamiseksi, jotta haavoittuvuudet korjataan tai niiden vaikutuksia lievennetään pikaisesti ja tietoturvapäivitysten tapauksessa soveltuvin osin automaattisesti Liite I, Osa II, 8) varmistettava, että jos havaittujen tietoturvaongelmien ratkaisemiseksi on saatavilla tietoturvapäivityksiä, niitä levitetään viipymättä ja, jolleivat valmistaja ja yrityskäyttäjä ole digitaalisia elementtejä sisältävän räätälöidyn tuotteen osalta sopineet toisin, maksutta ja että niihin liitetään tarvittavat ohjeet, myös mahdollisista käyttäjältä edellytettävistä toimista	
Testaus- ja arviointimenetelmät		
Valmistaja	**CRA:n kohta**	
Säännöllinen turvallisuustestaus	Liite I, Osa II, 3) tehtävä säännöllisesti digitaalisia elementtejä sisältävän tuotteen tietoturvaan liittyviä tehokkaita testejä ja arviointeja	ISO/IEC 27002:2022, ISO/IEC 62443: 3-2:2020 ja ETSI EN 303 645