

Osa-alue	Vaatus	Esimerkki tai todentamisen tapa	Selvitys toimittajalta mikäli vaatimusta ei voida täyttää tai soveltaa kyseisessä hankinnassa.	Tilaaajan kommentit
1. Yleistä				
1001	Kaikki vaatimukset ovat pakollisia ja saman arvoisia. Mikäli toimittaja ei pysty täyttämään asetettua vaatimusta, tai sitä ei voida soveltaa kyseisessä hankinnassa, on toimittajan tehtävä selvitys kunkin vaatimuksen osalta sarakkeeseen D. Tilaaaja arvioi selvitykset ja hyväksyy tai hylkää ne. Hylätty selvitys johtaa tarjouksen hylkäämiseen, koska pakollista vaatimusta ei ole voitu täyttää.			
2. Fyysinen turvallisuus ja ympäristökontrollit				
2001	Toimittajan tiloissa, joissa käsitellään tai säilytetään Tilaaajan tietoa, ei saa toimia muita kuin toimittajaan virka- tai työsuhteessa tai työharjoittelussa olevia työntekijöitä ilman lupaa tai valvontaa.	Katselmoimalla Toimittajan tilaturvallisuutta koskevaa politiikkaa tai muuta ohjeistusta sekä fyysisiä kontrolloja, kuten lukitukset ja kameravalvonta ym.		
2002	Toimittajan laitteiden fyysinen turvallisuus tulee järjestää siten, ettei laitteisiin pääse fyysisesti käsiksi ilman valtuutusta. Kaikista pääsyistä tulee pitää kirjaa, esim. sähköisen kulunvalvonnan avulla. Lokien säilytysajan on oltava kaksi vuotta tapahtumasta.	Sama kuin yllä.		
2003	Toimittaja on velvollinen varmistamaan ja osoittamaan Tilaaajalle, että toimittajaa koskevat fyysisistä turvallisuutta ja ympäristökontrolloja koskevat vaatimukset toteutuvat myös ulkoisen konesalipalvelun tarjoajan osalta.	Katselmoimalla ulkoisen konesalipalvelun tarjoajan osoittama varmennuslausunto tai sertifiointi, josta nämä kontrollit käyvät ilmi. Tällainen tieto voi löytyä esim. Palvelusopimuksesta.		
2004	Toimittajan on kyettävä osoittamaan ne fyysiset lokaatiot, joissa Tilaaajan tietoja käsitellään.	Jos tietoja käsitellään muissa kuin Toimittajan omissa tiloissa, tulisi näiden tilojen sijainti olla myös Tilaaajan tiedossa, etenkin jos tietoja poistuu Suomen tai Euroopan talousalueen ulkopuolelle.		
2005	Mikäli toimittajan fyysisissä lokaatioissa tapahtuu muutoksia, on Toimittajan ilmoitettava niistä tilaaajalle heti kun muutos vahvistetaan sopimuksella, ilmoituksella tai muulla menetelmällä toimittajan edustajalle.	Jos toimittaja muuttaa toimitilojaan tai tietojen käsittelypaikkaa, on ilmoitus tehtävä Tilaaajalle kun sopimus, suunnitelma tai muu niihin verrattava tekijä, josta johtuen tietoja käsitellään paikassa, jossa niitä ei ole ennen käsitelty Toimittajan toimesta.		
3. Palveluympäristön looginen suojaus				
3001	Toimittaja pitää loogisesti erillään Tilaaajan tiedot muiden tilaajien tiedoista tarvittavilla teknisillä ja organisatorisilla kontrolloilla. Nämä tekniset ja organisatoriset kontrollit on voitava osoittaa Tilaaajalle pyydettyäessä.	Katselmoimaan dokumentaatio, josta käy ilmi mainitut kontrollit. Nämä toteutetut tekniset ja organisatoriset kontrollit tulisi olla dokumentoituina ja ajantasaisina.		
3002	Kaikki muuten kuin palvelimen paikalliselta fyysiseltä konsolilta tapahtuva etäylläpito tulee tapahtua suojattujen yhteysien yli. Käytettävä käyttäjän vahvaa tunnistamista ja vahvasti salattua tietoliikenneprotokollaa (esim. VPN-yhteys). Toimittajan hallinnoima operointilaite (työasema) on tunnistettava yksilöidysti ja kiistattomasti (esim. VPN-yhteys) ja suojattava asianmukaisesti.	Katselmoimaan etäylläpidon mahdollistavat järjestelmät.		

3003	Palvelun tuottamiseen käytettävien ja Toimittajan ylläpitämien järjestelmien komponentit tulee segmentoida mahdollisuuksien mukaan. Kaikki paitsi erikseen sallittu liikenne tulee estää kaikkien verkkosegmenttien (esimerkiksi internet/DMZ/sisäverkko) välillä.	Katselmoidaan verkkokuva tai muu dokumentaatio, josta segmentointi käy ilmi.
3004	Toimittajan tulee varmuuskopioida omat, tarjoamaansa palveluun tai tuotteeseen liittyvät palvelimet ja tietojärjestelmät niiltä osin, kun se on olennaista palvelun tai tuotteen jatkuvuuden ja palautuskyvyn kannalta Tilajalle.	Katselmoidaan dokumentaatio, josta sovitut varmuuskopiointikäytännöt käy ilmi.
3005	Toimittajan varmuuskopioimien kohdan 3004 mukaisten tietojen varmuuskopiot on säilytettävä noudattaen vähintään samoja turvallisuusvaatimuksia kuin varsinaisten tietojen kohdalla.	
3006	Toimittajan ylläpitämien palvelinten tulee tuottaa riittävät käyttöjärjestelmätason lokitiedot kattavien tapahtumaketjujen muodostamiseen esimerkiksi tietoturvaloukkaustilanteessa niiltä osin, kuin se liittyy Tilajalle tarjottavaan palveluun tai tuotteeseen. Lokitiedot on säilytettävä vuoden ajan.	Katselmoidaan esimerkiksi ticketit tai sähköpostikeskustelu poikkeaman käsittelystä.
3007	Toimittajan tulee varmistaa palvelun tuottamiseen käytettävien pilvipalveluiden verkkoturvallisuus esimerkiksi palomuurilla, virustorjunnalla ja IDS/IPS-ohjelmilla.	Katselmoimalla verkkoturvallisuutta lisäävät ohjelmistot tai dokumentaatio, josta käy ilmi mainittujen järjestelmien käyttö.
3008	Toimittaja, tai sen tarjoama palvelu tai tuote ei saa välittää dataa tai informaatioa suojaamattomana internetin yli.	Katselmoimalla esim. dokumentaatio, josta käy ilmi käytäntö, jolla Tilajaan data ei kulje suojaamattomana internetin yli.
3009	Toimittajan tulee varmistaa palomuurisääntöjen asianmukainen dokumentointi.	Katselmoidaan dokumentoidut palomuurisääntöt järjestelmästä.
3010	Toimittajan ja sen tarjoaman palvelun tai tuotteen on mahdollistettava VPN-yhteys silloin, kuin ei voida toimia rajatussa sisäverkossa. VPN-yhteyksiä on voitava seurata ja niistä on jätävä lokitieto.	Katselmoimalla VPN-ohjelmistoa ja sen asetuksia, joista lokitiedon tallennus tulisi käydä ilmi.
3011	Mikäli hankinnan kohteeseen sisältyy palveluita, jotka ovat Internetiin päin avoimia, on niihin kirjautumisessa oltava käytössä monivaiheinen tunnistautuminen (MFA)	
3012	Toimittajan on käytettävä Kyberturvallisuuskeskuksen suositusten mukaisia salasanoja ja niiden kompleksisuusvaatimuksia kaikissa tilaajan kanssa suoraan ja välillisesti vaikuttavissa järjestelmissä.	

4. Tietojärjestelmien operointi- ja ylläpitokäytännöt

4001	<p>Toimittajan palvelin-, työasema- ja verkon aktiivilaitteiden asetukset tulee koventaa käyttäen ajantasaista kansainvälisesti tunnustettua kovenusstandardia;</p> <p>-Kaikki tarpeettomat palvelut tulee olla on poistettu käytöstä. Mikäli käytettävälle teknologialle ei ole yleistä standardia olemassa, voidaan käyttää sovellus- tai laite-toimittajan tietoturvasuosituksia. Koventaminen tulee pystyttyä osoittamaan.</p> <p>-Oletussalasanat on vaihdettu.</p> <p>-Laitteiden hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista.</p>	Katselmoidaan palvelinten, työasemien ja verkon aktiivilaitteiden asetukset. Esimerkiksi NIST SP 800-123 tai CIS Benchmarks.
4002	<p>Toimittaja vastaa tietoturvapäivitysten ajantasaisesta jakamisesta hallitsemilleen palvelimille ja työasemille, joilla Tilaaajan tietoja käsitellään.</p>	Katselmoimalla tietoturvapäivityksiin liittyvä järjestelmäloki.
4003	<p>Mikäli toimittaja havaitsee tietoturvapäivitysten jakelussa häiriön, jonka johdosta päivitykset eivät ole tapahtuneet tarkoitetulla tavalla ajantasaisesti, on toimittajan ilmoitettava poikkeamasta tilaajalle havaitsemisajankohtaan nähden viimeistään seuraavan arkipäivän kuluessa.</p>	
4004	<p>Toimittajan ylläpitämiin käyttöjärjestelmiin, joissa käsitellään Tilaaajan tietoja tai Tilaaajalle tarjottavan tuotteen tai palvelun tietoja, tulee asentaa haaittaohjelmien torjuntaohjelmisto, jonka tunnistetiedot päivitetään automaattisesti vähintään päivittäin.</p>	Katselmoidaan haaittaohjelmien torjuntaohjelmiston asetukset.
4005	<p>Toimittajan tulee varmistaa laitteiden käytöstä poiston yhteydessä, ettei Tilaaajan tietoja sisältäviin laitteisiin tai tietoon päästä käsiksi laitteen poistamisen jälkeen.</p> <p>Tämä on varmistettava esim. Tilaaajan tiedot asianmukaisesti tuhoamalla tai tiedon ylikirjoituksella. Pyydettyessä Toimittaja on velvollinen palauttamaan käsittelemänsä tiedot Tilaaajalle.</p>	Katselmoimalla laitteiden ylläpitoon liittyvät ohjeistukset ja politiikat
5.Hankinnan kohteena oleva tietojärjestelmä		
5001	<p>Toimittaja huomioi tietoturvan Tilaaajalle tuotettavassa tuotekehityksessä.</p>	Turvallisen kehittämisen politiikka/ohjeet, security coding practices, kooditarkastusohjelmat. Kehittäjien osallistuminen tietoturvakoulutuksiin, turvalliset kehittämismenetelmät
5002	<p>Toimittaja suorittaa säännöllisesti itse tai kolmannen osapuolen toimesta tietoturvatestauksia kohdistuen Tilaaajalle tuotettavaan palveluun.</p>	Toimittajan tulee dokumentoida suoritettavat testaukset ja ne tulee pystyä esittämään Tilaaajan pyynnöstä.
5003	<p>Tilaaajalle tarjottavien järjestelmien, ohjelmistojen ja palveluiden konfiguraatio tulee olla dokumentoitu. Vaatimus voidaan täyttää esim. automaattisella CMDB-järjestelmällä.</p>	Katselmoidaan tiedot järjestelmien, ohjelmistojen ja palveluiden konfiguraatioista.

5004	Toimittaja sitoutuu tuotteen tai palvelun olemassaolevien tai tulevien tietoturvaavaoittuvuuksien päivittämiseen sopimuksessa määritetyksi ajaksi. Toimittaja on velvollinen ilmoittamaan Tilaajalle havaitut haavoittuvuudet.	Katselmoidaan esimerkki haavoittuvuudesta, joka on havaittu.
5005	Toimittajan tuottamaa palvelua tai tuotetta voidaan käyttää alustoilla, joihin on saatavilla ylläpito-, kehitys- ja tukipalveluita.	Katselmoidaan alustojen tiedot niiltä osin, kun ylläpito-, kehitys- ja tukipalvelut saadaan selville.
5006	Kohdan 5005 mukaisen palvelun tai tuotteen alustan ylläpito- kehitys- tai tukipalveluiden on jatkuttava vähintään yhtä pitkään kuin toimitettavan palvelun tai tuotteen käyttöikä on.	Alustan valmistajan ilmoittama End Of Life ei saa olla aiempi päivämäärä kuin aiottu käyttöikä järjestelmälle.
5007	Toimittajan tuottaman palvelun tai tuotteen pitää mahdollistaa Tilaajalle pääsynhallinnan prosessi, jolla varmistetaan käyttöoikeuksien elinkaaren asianmukainen hallintaa. Prosessiin kuuluu pääsyoikeuksien myöntäminen, poistaminen, katselmointi ja päivittäminen.	Katselmoimalla tuotteen ominaisuudet.
5008	Tilaajan tulee pystyä jälkikäteen yksilöidysti selvittämään, kuka on käsitellyt tietoja järjestelmästä, koska tämä on tapahtunut sekä miltä laitteelta ja mihin tietoihin toimenpide on kohdistunut.	Katselmoidaan esimerkit muutamien järjestelmän käyttäjien kohdalta, joista käy ilmi vaatimuksenmukaiset tiedot.
5009	Toimittajalla tulee olla kyvykkyys palvelusta kerättävien lokien reaaliaikaiseen tai lähes reaaliaikaiseen siirtämiseen kolmannen osapuolen keskitettyyn lokienhallintajärjestelmään.	Siirto viimeistään seuraavana arkipäivänä kolmannen osapuolen keskitettyyn lokienhallintajärjestelmään.
5010	Toimittajan tuottaman palvelun tai tuotteen pitää mahdollistaa häiriöiden ja poikkeamien hallinta Tilaajan prosessin mukaisesti, sekä asianmukainen datan kerääminen häiriö- ja poikkeamatapauksissa.	Tilaajan ja Toimittajan on sovittava tästä prosessista erikseen ja häiriöiden tai poikkeamien käsittelystä jääneiden lokien avulla osoittaa, että prosessia on noudatettu. Katselmoidaan esim. Incident management process.
5011	Toimittajalla on oltava menettelytavat ja sopivat menetelmät, joilla taataan sisäänrakennetut, hallitut sekä dokumentoidut muutokset.	Katselmoidaan muutoksenhallintaprosessia.

6. Jatkuvuuden varmistaminen

6001	Toimittaja valvoo Tilaajalle tarjottavaan tuotteeseen tai palveluun liittyvien ja Toimittajan ylläpitovastuulla olevien palvelinten, työasemien, sovellusten ja verkon aktiivilaitteiden häiriöitä ja virheilmoituksia sekä tietoturvallisuuteen liittyviä tapahtumalokeja. Ohjeistuksen laatiminen ja ylläpito on osa toimittajan tarjoamaa ylläpitopalvelua.	Katselmoidaan järjestelmää, jonka avulla häiriöitä ja virheilmoituksia valvotaan ja havaitaan. Katselmoidaan valittu määrä tapahtumalokeja ja niiden käsittely.
------	--	---

7. Tietoturvallisuuden varmentaminen ja auditointi

7001	Tilaajalla on oikeus suorittaa toimittajan fyysiseen ja tekniseen ympäristöön tietoturva-auditointi enintään kerran vuodessa.	
7002	Toimittajan on käytettävä ulkoista hyökkäyspintaa määrittävää järjestelmää	Käytettävä EASMIa tai vastaavaa työkalua tai järjestelmää

8. Raportointi ja viestintä

8001

Toimittajan ja Tilaajan väliseen yhteydenpitoon voidaan nimittää molempiin tahoihin nimetyt yhteyshenkilöt, joihin voi olla yhteydessä tietoturva-asioissa. Henkilöt on nimettävä tehtävän perusteella siten, että jos henkilö ei toimi enää toimittajan palveluksessa, hänen tilalleen nimetään tai nimeytyy välittömästi uusi henkilö siten, että katkosta tehtävään nimetyn henkilön suhteen ei tapahdu.

Katsotaan sopimusta, kokousmuistiot tai muuta dokumentaatiota, josta nimetyt yhteyshenkilöt ja yhteystiedot sekä heille nimetyt varahenkilöt käyvät ilmi.

Tilaajan päätös

Hyväksytään / ei hyväksytä

Perustelut

Hyväksyjä

