Osa-alue	Vaatimus	Esimerkki tai todentamisen tapa	Selvitys toimittajalta mikäli vaatimusta ei voida täyttää tai soveltaa kyseisessä hankinnassa.	Tilaajan 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. Tilaaja arvioi selvitykset ja hyväksyy tai hylkää ne. Hylätty selitys johtaa tarjouksen hylkäämiseen, koska pakollista vaatimusta ei ole voitu täyttää.			
2. Fyysinen turvallisuus ja ympäristökontrollit				
2001	Toimittajan tiloissa, joissa käsitellään tai säilytetään Tilaajan 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 kontrolleja, kuten lukitukset ja kameravaltonta ym.		
2002	Toimittajan laitetilojen 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 Tilaajalle, että toimittajaa koskevat fyysistä turvallisuutta ja ympäristökontrolleja koskevat vaatimukset toteutuvat myös ulkoisen konesalipalvelun tarjoajan osalta.	Katselmoimalla ulkoisen konesalipalvelun tarjoajan osoittama varmennuslausunto tai sertifikaatti, josta nämä kontrollit käyvät ilmi. Tällainen tieto voi löytyä esim. Palvelusopimuksesta.		
2004	Toimittajan on kyettävä osoittamaan ne fyysiset lokaatiot, joissa Tilaajan tietoja käsitellään.	Jos tietoja käsitellään muissa kuin Toimittajan omissa tiloissa, tulisi näiden tilojen sijainti olla myös Tilaajan tiedossa, etenkin jos tietoja poistuu Suomen tai Euroopan talousalueen ulkopuolelle.		
2005	Mikäli toimittajan fyysisissä lokaatioissa tapahtuu muutoksia, on Toimittajan ilmoitettava niistä tilaajalle heti kun muutos vahvistetaan sopimuksella, ilmoituksella tai muulla menetelmällä toimittajan edustajalle.	Jos toimittaja muuttaa toimitilojaan tai tietojen käsittelypaikkaa, on ilmoitus tehtävä Tilaajalle 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 Tilaajan tiedot muiden tilaajien tiedoista tarvittavilla teknisillä ja organisatorisilla kontrolleilla. Nämä tekniset ja organisatoriset kontrollit on voitava osoittaa Tilaajalle pyydettäessä.	Katselmoidaan dokumentaatio, josta käy ilmi mainitut kontrollit. Nämä toteutetut tekniset ja organisatoriset kontrollit tulisi olla dokumentoituna ja ajantasaiset.		
3002	Kaikki muuten kuin palvelimen paikalliselta fyysiseltä konsolilta tapahtuva etäylläpito tulee tapahtua suojattujen yhteyksien 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.	Katselmoidaan 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 Tilaajalle.	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 Tilaajalle tarjottavaan palveluun tai tuotteeseen. Lokitiedot on säilytettävä vuoden ajan.	Katselmoidaan esimerkiksi tiketit 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 Tilaajan data ei kulje suojaamattomana internetin yli.
3009	Toimittajan tulee varmistaa palomuurisääntöjen asianmukainen dokumentointi.	Katselmoidaan dokumentoidut palomuurisäännöt 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 jäätävä 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	Toimittajan palvelin-, työasema- ja verkon aktiivilaitteiden asetukset tulee koventaa käyttäen ajantasaista kansainvälisesti tunnustettua kovennusstandardia; -Kaikki tarpeettomat palvelut tulee olla on poistettu käytöstä. Mikäli käytettävälle teknologialle ei ole yleistä standardia olemassa, voidaan käyttää sovellus- tai laitetoimittajan tietoturvasuosituksia. Koventaminen tulee pystytä osoittamaan. -Oletussalasanat on vaihdettu. -Laitteiden hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista.	Katselmoidaan palvelinten, työasemien ja verkon aktiivilaitteiden asetukset. Esimerkiksi NIST SP 800-123 tai CIS Benchmarks.
4002	Toimittaja vastaa tietoturvapäivitysten ajantasaisesta jakamisesta hallitsemilleen palvelimille ja työasemille, joilla Tilaajan tietoja käsitellään.	Katselmoimalla tietoturvapäivityksiin liittyvä järjestelmäloki.
4003	Mikäli toimittaja havaitsee tietoturvapäivitysten jakelussa häiriön, jonka johdosta päivitykset eivät ole tapahtuneet tarkoitetulla tavalla ajantasaisesti, on tomittajan ilmoitettava poikkeamasta tilaajalle havaitsemisajankohtaan nähden viimeistään seuraavan arkipäivän kuluessa.	
4004	Toimittajan ylläpitämiin käyttöjärjestelmiin, joissa käsitellään Tilaajan tietoja tai Tilaajalle tarjottavan tuotteen tai palvelun tietoja, tulee asentaa haittaohjelmien torjuntaohjelmisto, jonka tunnistetiedot päivitetään automaattisesti vähintään päivittäin.	Katselmoidaan haittaohjelmien torjuntaohjelmiston asetukset.
4005	Toimittajan tulee varmistaa laitteiden käytöstä poiston yhteydessä, ettei Tilaajan tietoja sisältäviin laitteisiin tai tietoon päästä käsiksi laitteen poistamisen jälkeen. Tämä on varmistettava esim. Tilaajan tiedot asianmukaisesti tuhoamalla tai tiedon ylikirjoituksella. Pyydettäessä Toimittaja on velvollinen palauttamaan käsittelemänsä tiedot Tilaajalle.	Katselmoimalla laitteiden ylläpitoon liityvät ohjeistukset ja politiikat
5.Hankinnan kohteena oleva tietojärjestelmä		
5001	Toimittaja huomioi tietoturvan Tilaajalle tuotettavassa tuotekehityksessä.	Turvallisen kehittämisen politiikka/ohjeet, security coding practices, kooditarkastusohjelmat. Kehittäjien osallistuminen tietoturvakoulutuksiin, turvalliset kehittämismenetelmät
5002	Toimittaja suorittaa säännöllisesti itse tai kolmannen osapuolen toimesta tietoturvatestauksia kohdistuen Tilaajalle tuotettavaan palveluun.	Toimittajan tulee dokumentoida suoritetut testaukset ja ne tulee pystyä esittämään Tilaajan pyynnöstä.
5003	Tilaajalle tarjottavien järjestelmien, ohjelmistojen ja palveluiden konfiguraatio tulee olla dokumentoitu. Vaatimus voidaan täyttää esim. automaattisella CMDB-järjestelmällä.	Katselmoidaan tiedot järjestelmien, ohjelmistojen ja palveluiden konfiguraatioista.
5004	Toimittaja sitoutuu tuotteen tai palvelun olemassaolevien tai tulevien tietoturvahaavoittuvuuksien 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, kokousmuistiota tai muuta dokumentaatiota, josta nimetyt yhteyshenkilöt ja yhteystiedot sekä heille nimetyt varahenkilöt käyvät ilmi.	

	Hyväksytään / ei hyväksytä	**Perustelut**	**Hyväksyjä**
Tilaajan päätös			