Tietoturvatarkastuksen tulokset

<Hankkeen tunnus ja nimi>

<pp.kk.vvvv>

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

VAASA.

Dokumentin tiedot

Dokumentin nimi	Tietoturvatarkastuksen tulokset
Käyttötarkoitus	Tarkistuslista ja pöytäkirja tietoturvatarkastukselle
Versio	1.0
Tila	Hyväksytty
Laatija	Sami Varjo
Tarkastaja	Timo Grev
Hyväksyjä	Teemu Lehtonen
Tiedon luokittelu	Julkinen asiakirja

Versionhallinta

Versio	Pvm	Laatija	Muutoksen lyhyt kuvaus
0.1	20.01.2021	Sami Varjo	Ensimmäinen luonnos muokkaukseen
0.2	21.01.2021	Sami Varjo	Muokattu tarkistuslistan kohteista
0.3	22.01.2021	Sami Varjo	Teemu L:n kommentoinin pohjalta tehty korjauksia tekstiin ja tarkistuslistan kohteiden päällekkäisyyttä korjattu
0.4	25.01.2021	Timo Grev, Teemu Lehtonen	Katselmointi ja kommentointi
0.5	25.01.2021	Sami Varjo	Katselmoinnin perusteella tehty muutokset dokumenttiin
1.0	25.01.2021	Teemu Lehtonen	Dokumentti hyväksytty versioon 1.0

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Sisällysluettelo

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

VAASA.

1. Johdanto

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen.

Tietojen turvallisuudesta on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa muodoissa sen koko elinkaaren ajan. Vaasan kaupungin kunkin yksikön luonne ja mahdolliset turvallisuuden tehostamistarpeet otetaan huomioon. Tietojen turvaamisesta on huolehdittava yksiköissä, jotka käsittelevät runsaasti luottamuksellista tai turvaluokiteltua tietoa. Tietojen turvaamisessa huomioidaan omina osa-alueinaan hallinnollinen, henkilöstö-, fyysinen, tietoaineisto-, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuus.

Tiedon turvaaminen on osa toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua, varautumista uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö niin Vaasan kaupungin omien kuin sen toimesta käsiteltävien sidosryhmienkin tietojen käsittelyyn.

Tietoturvariskien hallitsemiseksi Vaasan kaupunki suorittaa jokaiselle uudelle tietojärjestelmälle toteutustavasta riippumatta tietoturvatarkastuksen.

2. Tarkastuksen kohde ja rajaukset

Tarkastuksen kohteen tiedot:

Toimittajan nimi	Toimittaja Oy
Järjestelmä tai pilvipalvelu nimi	Järjestelmä X
Hallinnollinen yhteyshenkilö	Toimittajan edustaja Y
Tietoturvan yhteyshenkilö	Toimittajan edustaja Z
Tietosisällöt:	
Sisältää henkilötietoja?	Kyllä/Ei
Sisältää salassapidettäviä tietoja?	Kyllä/Ei
Sisältää erityisiä henkilötietoryhmiä?	Kyllä/Ei
Taustatiedot:	
Selvitys tietojen käsittelystä ja suojauksesta	Kyllä/Ei
Järjestelmän tietoturvasuunnitelma	Kyllä/Ei
Vaikutusten arviointi	Kyllä/Ei
Tietoturvakuvaus	Kyllä/Ei
Toteutustapa	Pilvipalvelu/On-premise
Laadittu tietovirtakuvaus	Kyllä / Ei / Sovittu (tilaaja + toimittaja)

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Tarkastuksen sisältö ja rajaukset

Toimittaja on luovuttanut tilaajalle riittävät tiedot, joiden perusteella tilaaja arvioi toimittajan tietoturvan hallintamallin täyttävätn hallinnollisen tietoturvan vaatimukset. Toimittajan tietoturvakuvauksessa on kuvattu hallinnollisia ja teknisiä tietoturvan hallintakeinoja.

Käyttöönottoprojektin aikana projektisuunnitelma sisältää tehtäviä eri vaiheissa, joilla dokumentoidaan toteutus ja kuvataan toteutukseen liittyvät riskit sekä keinot joilla testauksen aikana riskiä lasketaan.

Tarkastuksen laajuus rajataan tarkastuslistan kohteiden läpikäyntiin.

3. Käytetyt menetelmät

Järjestelmän hankintaprosessi pyrkii tukemaan kokonaisuutena hyvää tietoturvan toteutumista. Tarkastuksessa on käytetty toimittajan selvityksiä, haastattelua ja tarkastuslistaa, jolla varmistetaan että järjestelmään ei jää tarpeettomasti tietoturvaa heikentäviä kohteita.

Luokitus	Tarkastuksen kohde	Toteutuminen	Lisätiedot
Hallinnollinen tietoturva	Onko tietojen turvalliseen käsittelyyn, säilytykseen, varmuuskopiointiin ja hävittämiseen tai arkistointiin olemassa tarvittavat välineet ja toimintatavat? (pilvipalveluissa toimittaja vastaa, On-premise tilaajan palveluntuottaja vastaa)	Kyllä / Ei / Osittain	
Henkilöturvallisuus	Onko sovittu, että toimittaja ilmoittaa oman henkilökunnan muutoksista ja poistaa tarvittaessa omilta käyttäjiltään käyttöoikeudet sopimuksen kohteeseen ilman aiheetonta viivytystä?	Kyllä / Ei / Osittain	
Henkilöturvallisuus	Toimittajan kaikkien työtekijöiden roolit ja pääsyoikeudet on määritelty järjestelmään, joka sisältää tilaajan tietoa. Toimittaja toimii tilaajan tietojen käsittelijänä vain perustellusta syystä.	Kyllä / Ei / Osittain	
Koventaminen	Järjestelmien tietoturvataso on kovennettu. Toimittaja vastaa siitä, että mm. käytöstä on poistettu kaikki tarpeettomat kohteet mm. palvelut, portit ja käyttäjätunnukset.	Kyllä / Ei / Osittain	
Käyttöoikeudet	Pääsy ohjelmointiympäristöihin tai koko järjestelmä koskeviin asetuksiin on rajoitettu ja sen käyttö on valvottu?	Kyllä / Ei / Osittain	

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Käyttöoikeudet	Kaikki järjestelmässä olevat käyttäjätunnukset on toimittajalla dokumentoituna ja kuvattu käyttötarkoitus. Kaikki tarpeettomat tunnukset poistetaan tai passivoidaan (esim. testitunnukset).	Kyllä / Ei / Osittain
Käyttöoikeudet	Service Account-tunnuksissa käytetään vain vahvoja salasanoja ja toimittaja huolehtii näiden salassapidosta ja tarvittaessa vaihtaa salasanan säännöllisesti.	Kyllä / Ei / Osittain
Käyttöoikeudet	Järjestelmän kaikki ulkoiset yhteydet on dokumentoitu ja määritelty käyttötarkoitus ja vastuuhenkilöineen.	Kyllä / Ei / Osittain
Käyttöoikeudet	Kaikki tallennetut salasanat säilytetään salatussa muodossa, ei selväkielisenä. Salauksen tulee olla vahva nykyisten ja tulevien standardien mukaisesti.	Kyllä / Ei / Osittain
Riskienhallinta	Palvelun tai järjestelmän ICT-ympäristön suunnittelu ja riskienhallinta on vastuutettu ja varmistettu.	Kyllä / Ei / Osittain
Tekninen tietoturva	Käyttävien palvelimien ja muiden laitteiden tietoturvallisuus on huolehdittu.	Kyllä / Ei / Osittain
Tekninen tietoturva	Varmenteet ovat voimassa olevia ja toimittaja huolehtii niiden uusimisesta.	Kyllä / Ei / Osittain
Tekninen tietoturva	Järjestelmästä on varmuuskopiointisuunnitelma.	Kyllä / Ei / Osittain
Tekninen tietoturva	Järjestelmä on toimittajan tai tilaajan valvonnassa (poikkeukset ja häiriöt).	Kyllä / Ei / Osittain
Tekninen tietoturva	Tuotanto ja testausympäristöt on eriytetty toisistaan.	Kyllä / Ei / Osittain
Tekninen tietoturva	Toimittajalla on käytäntö, joka mahdollistaa, että havaitut tietoturvahaavoittuvuudet korjataan, tilapäisellä tai pysyvällä korjauksella korkeintaan 2 työpäivän kuluessa.	Kyllä / Ei / Osittain
Testaus	Toimittaja testaa osana tuotekehitysprosessiaan ohjelmistoa hyödyntäen esim. OWASP Top10 -tarkastuslistoja.	Kyllä / Ei / Osittain

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

Tietoliikenne	Etäyhteyksien tietoturva toteutetaan ja yhteydenotot hallitaan organisaation hyväksymällä tavalla. (Käyttäjätunnukset ovat henkilökohtaisia ja toimittaja vastaa tunnuksella tehdyistä vahingoista)	Kyllä / Ei / Osittain
Tietoliikenne	Tietoliikenteessä käytetään vain turvallisia yhteyksiä ja niiden kapasiteetti ja käytettävyys ovat riittävät.	Kyllä / Ei / Osittain
Tietoliikenne	Kaikki tarpeettomat tietoliikenneportit on suljettu oletuksena ja mahdollisuuksien mukaan yhteydet sallitaan vain tietyistä ip-osoitteista ja integraatioissa käytetään käyttäjän tunnistusta (Service Account), mikäli kyse ei ole julkisesta tiedosta.	Kyllä / Ei / Osittain
Tietoliikenne	Kaikki tiedonsiirto tapahtuu suojatulla yhteydellä.	Kyllä / Ei / Osittain

4. Tulokset

Jokaisesta tarkastuslistan löydöksestä kirjataan havainnot ja pyydetään toimittajalta selvitys, miten ongelma korjataan.

Kirjaa tähän havainnot ja ratkaisut näihin

1. Järjestelmässä on auki testitunnuksia.
    a. Ratkaisu: Toimittaja passivoi tunnukset ja ilmoittaa tilaajalle kun tehtävä on suoritettu.
2. Järjestelmässä on käytössä heikkoja salasanoja Service Accounteilla.
    a. Ratkaisu: Toimittaja vaihtaa tilaajan policyn mukaiset salasanat ja ilmoittaa tilaajalle kun tehtävä on suoritettu.
3. Ei havaittu tietoturvaa heikentäviä kohteita.

5. Johtopäätökset

Toimittaja käyttää palvelun tuotekehitysprosessissa alan yleisesti hyväksyttyjä menetelmiä ja suorittaa palvelulle vähintään kerran vuodessa sisäisen tietoturvakatselmoinnin. Katselmoinnissa käydään läpi palvelun tietovuot, niihin liittyvät uhat ja toimenpiteet uhkien torjumiseksi tai minimoimiseksi. Apuna käytetään mm. OWASP Top Ten -projektin tarkistuslistoja, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Kyseessä on valmisohjelmisto tai pilvipalvelu, jonka tietoturvan testaus rajoittuu hallinnollisen kohteiden analysointiin ja tarkastuslistan läpikäyntiin. Tarkastuksessa ei ole havaittu puuteita tai tietoturvaongelmia / on havaittu korjattavia kohteita, joiden korjauksesta on sovittu toimittajan kanssa.

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi

6. Tarkastuksen suorittajat

Vaasan kaupunki

ICT-pääsuunnittelija Sami Varjo

ICT-erityisasiantuntija, oto tietoturvapäällikkö Timo Grev

Järjestelmän omistajan edustaja/projektipäällikkö Etunimi Sukunimi

Toimittaja X

Edustaja 1

Edustaja 2

Konsernihallinto
PL 3, 65101 Vaasa
Vaasanpuistikko 10, 3 krs
Puh +358 (0)6 325 1111
etunimi.sukunimi@vaasa.fi