

Lisa
RMK ja [Sisesta juriidilise isikunimi
vahelise [Vali kuupäev] lepingu nr
[Sisesta number] juurde

Turvanõuded tarnijale

1. Eesmärk

- 1.1. Turvanõuded tarnijale kirjeldab kohustuslikke infoturbeturbe nõudeid tarnijale, et tagada **RMK varade, sh teabe, konfidentsiaalsus, terviklus ja käideldavus**.

2. Vastutus

- 2.1. RMK vastutab käesolevate töötlemissuuniste määramise eest;
2.2. **Tarnija** vastutab:
2.2.1. käesolevate töötlemissuuniste rakendamise eest, sh alltöövõtjate korral;
2.2.2. täiendava teenuslepingu ja konfidentsiaalsusnõuete täitmise eest.

3. Sisemise infoturbe halduse meetmed

- 3.1. Tarnija tagab organisatsioonisisesel meetodilisel ja süstemaatilisel infoturbe haldamisel, eelistatult laialdaselt tunnustatud turvameetodika põhjal (nt ISO/IEC 27001, SOC2, CIS Security Controls, Eesti riiklik infoturbe standard E-ITS vms), sh rakendades:
3.1.1. infoturbe riskihalduse;
3.1.2. varahalduse, sh arvestades RMK varadega;
3.1.3. infoturbe rollide ja vastutuse kindlaksmääramise;
3.1.4. pääsuõiguste halduse;
3.1.5. turvaintsidentide halduse;
3.1.6. jätkuvuse halduse, sh oma tarneahela ulatuses;
3.1.7. tööjaamade ja teiste IT-seadmete ja tarkvarade tugevdamise ja konfiguratsioonihalduse;
3.1.8. kahjurvara tõrje;
3.1.9. krüptograafiliste meetmete halduse;
3.1.10. auditilogi ja turvaseire olemasolu;
3.1.11. nõrkuse ja paigalduse;
3.1.12. füüsiliste turvameetmete halduse;
3.1.13. turvameetmete perioodilise läbivaatuse (vähemalt kord aastas).
3.2. Kõik need infoturbe protsessid peavad tagama RMK varade konfidentsiaalsuse, tervikluse, käideldavuse ja organisatsiooni kohanemisvõime muutuvast küberohtude keskkonnas.

4. Andmete minimeerimise, piiratud säilitamise ja kustutamise meetmed

- 4.1. Tarnija tohib RMK teavet töödelda, üksnes minimaalses vajalikus mahus ja ajaperioodil, mis on vajalik lepinguliste tööülesannete täitmiseks.
4.2. Käesoleva lepingu raames tuleb andmeid säilitada [Sisesta tähtaeg] aastat. Selle aja möödudes tuleb andmed Tarnija süsteemidest automaatselt kustutada.

- 4.3. Peale teenuslepingu lõppemist tuleb RMK teave Tarnija hallatavatest süsteemidest turvaliselt kustutada, küsides enne selleks RMK-lt kirjaliku kinnituse. Kinnituse küsimisel tuleb kirjeldada plaanitav turvalise kustutuse meetod.

Kommenteerinud [EE1]: Punktid kohalduvad, kui RMK andmeid töödeldakse Tarnija süsteemides ja sellel andmekategoorial on säilitamistähtaeg määratud.

5. Andmete turvalisus edastamisel ja talletamisel

- 5.1. Konfidentsiaalse teabe edastamisel arvutivõrgu kaudu peab teave olema krüpteeritud turvalise krüptomeetme abil vastavalt kokkulepitud andmeedastuse viisile, kas:
- 5.1.1. rakenduste vahelisel suhtlusel üle API kasutades turvalist šifrikomplektiga TLS (HTTPS) veebiseanssi;
 - 5.1.2. inimkasutajale andmete jagamisel üle veebiliidese kasutades turvalist šifrikomplektiga TLS (HTTPS) veebiseanssi;
 - 5.1.3. kaugpääsuga andmete jagamisel kasutades VPN ühendust turvalise konfiguratsiooniga;
 - 5.1.4. e-kirjaga andmete edastamisel kasutades krüpteeritud manuseid (.doc).
- 5.2. Konfidentsiaalse teabe talletamisel (andmed jõudeolekus) peab rakendama turvalisi krüptomeetmeid. Näiteks kogu ketta krüpteerimine, mälu pulga krüpteerimine, krüpteeritud andmebaas või andmebaasi kirjed.
- 5.3. Turvaline krüptomeetode on lahendus, mis rakendab turvalist krüptoalgoritmi, võtmepikkust, krüptovõtme käsitlemist, tarkvara jms. Valikul peab lähtuma uusimast RIA avaldatud krüptograafiliste algoritmide elutsükli uuringust (https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid?view_instance=2¤t_page=1&sort_property=1&sort_direction=desc#krüptouuringud).

6. Turvaintsidenti käsitlemise ja jätkuvuse meetmed

- 6.1. Tarnija peab RMK-d teavitama esimesel võimalusel, kuid mitte hiljem kui 20 tunni jooksul igast tuvastatud turvaintsidentist, mis võib mõjutada RMK vara, sh teavet. Teavitus tuleb edastada:
- 6.2. e-posti aadressile: andmekaitse@rmk.ee;
 - 6.3. telefonil: +372 676 7000.
 - 6.4. Teavitus peab sisaldama piisavalt detailset infot turvaintsidenti ulatuse, mõju, kronoloogia ja tehnilise olemuse kohta, et RMK saaks vajadusel rakendada täiendavaid meetmeid oma varade kaitseks.
 - 6.5. RMK teavitab vajadusel kolmandaid osapooli, avalikkust ja järelevalveasutusi, sh Andmekaitse Inspektsiooni, Riigi Infosüsteemi Ametit ja Politsei- ja Piirivalveametit. Tarnija ei teosta avalikku suhtlust osas, mis võimaldab tuvastada RMK-d ja tema kliente.
 - 6.6. Teavet turvaintsidentide kohta loetakse konfidentsiaalseks ja see tuleb edastada krüpteeritult.
 - 6.7. Tarnija teeb RMK-ga igakülgset koostööd turvaintsidentide käsitlemisel, sh analüüsimisel, isoleerimisel ja normaalse olukorra taastamisel.
 - 6.8. Tarnija peab oma sisemised lahendused ja protsessid korraldama selliselt, et intsidenti korral RMK-ga seotud äriprotsessid ja -teenused toimiksid võimalikult vähese häiringuga.

7. Pääsuhalduse meetmed

- 7.1. Juurdepääs RMK varadele, sh teabele on lubatud [tee valik]:
- 7.1.1. X ja Y rakenduste vahel üle API;
 - 7.1.2. veebiliidese kaudu RMK rakenduses X;
 - 7.1.3. VPN ja RDP/SSH kaugpääsu lahenduste kaudu;
 - 7.1.4. [mõni muu variant].

Kommenteerinud [EE2]: Tee valik ja teised valikud eemalda

Kommenteerinud [EE3]: Märgi X ja Y asemele konkreetset rakendused

- 7.2. RMK konfidentsiaalse teabega dokumentatsioon peab olema vastavalt märgistatud, kui vastav märgistus on juba seotud alusdokumentatsioonil või kui need juhised on RMK poolt antud. Dokumentatsioonil saab kasutada märgistust: asutusesiseks kasutamiseks ning vastav viide õigusaktile või "RMK siseseks kasutamiseks".
- 7.3. RMK süsteemides talletatud ja üksnes seal töötlemiseks mõeldud teavet ei tohi kopeerida Tarnija süsteemidesse, kui ei ole kirjalikult kokku lepitud teisiti.
- 7.4. RMK konfidentsiaalsele teabele juurdepääsu jagamisel tuleb arvestada konkreetsete töötajate teadmiskajadusega ning rakendada minimaalõiguste printsiipi.
- 7.5. Juurdepääsu võimaldavat teavet (nt paroolid, PIN-koodid, salajased või privaatsvõtted, tookenid jne) tohib talletada ainult krüpteeritud kujul (nt tarkvaraline paroolihoidla, vault) või füüsiliselt kaitstud hoidlas (nt seifis).
- 7.6. Juurdepääsul peab kõikidele kasutajatele jõustama mitmetasemelised autentimisviisid ja keelama üksnes ühetasemelised autentimisviisid.
- 7.7. RMK süsteemides loodud kasutajakontosid võib kasutada ainult Tarnija töötaja, kellele nimeline konto on loodud ja kellele on pääsuõigused üle antud. Konto jagamine on keelatud.
- 7.8. Tarnija peab RMK-d viivitamata teavitama kasutajakonto sulgemise vajadusest, kui mõni Tarnija töötajatest on töölt lahkunud, ei ole enam seotud lepingu täitmisega või pääsuandmed on sattunud ohtu (nt lekkinud).

8. Töötuskoha füüsilise turbe meetmed

- 8.1. RMK konfidentsiaalset teavet tohib töödelda ainult nendes ruumides, kus on tagatud piisav kaitse füüsiliste turvaohude eest, näiteks seadme vargus või volitamata juurdepääs, ekraani või klaviatuuri jälgimine jms.
- 8.2. Käesoleva lepinguga seotud RMK konfidentsiaalset teavet tohib töödelda üksnes Tarnija ametlikes ja turvatud kontoriruumides. Töötajate kaugtöö ei ole lubatud.

Kommenteerinud [EE4]: Igakordselt otsustada, kas see punkt jääb sisse.

9. Andmete kvaliteedi tagamise meetmed

- 9.1. Tarnija peab RMK konfidentsiaalset teavet töötleva viisil, et andmete õigsus, täielikkus ja ajakohasus oleks tagatud. Võimalusel peab rakendama sisendandmete valideerimist, töödeldud andmete testimist ja kindlustama Tarnija poolt kasutatava tarkvara korrektne toimimine.

10. Sündmuste logimine ja seire

- 10.1. Tarnija tagab konfidentsiaalse teabe töötlemisega seotud revisjonlogi (audit logi) olemasolu ja pideva turvaseire.
- 10.2. Logisid peab säilitama 2 aastat.

11. Jätkuvuse ja muudatuse meetmed

- 11.1. Tarnija tagab oma teenuste kättesaadavuse, arvestades võimalike probleemidega enda tarneahelas.
- 11.2. RMK pooltel pärimisel annab Tarnija teavet oma toodetes kasutatavatest süsteemikomponentidest ja turvafunktsioonidest.
- 11.3. Teenuseid mõjutavatest muudatustest ja võimalikest plaanilistest katkestustest antakse RMK-le teada enne muudatust või katkestust.

12. Meetmete teavitus ja kontroll

- 12.1. Tarnija tagab oma töötajate teavitamise käesolevatest turvameetmetest.

- 12.2. Tarnija tagab iseseisvalt enda ja alltöövõtjate organisatsioonis pideva turvameetmete rakendatuse kontrolli.
- 12.3. Tarnija organisatsioonisisest infoturbehaldust peab auditeerima sõltumatu osapool vähemalt üks kord aastas. Selle korraldab Tarnija.
- 12.4. Tunnustatud turvasertifikaadi (nt ISO/IEC 27001, SOC2) või auditaruande (E-ITS auditi aruanne) korral ei pea eraldiseisvat sõltumatud auditit lisaks läbi viima, kui sertifikaat või auditi aruanne:
 - 12.4.1. on kehtiv;
 - 12.4.2. käsitusala katab ära RMK varadega seotud teenused või tooted;
 - 12.4.3. tehakse RMK-le kättesaadavaks.
- 12.5. Võimalikud erandid ja kõrvalekalded nimetatud meetmetest tuleb kirjalikult kooskõlastada RMK-ga enne erandi rakendamist.
- 12.6. RMK võib igal ajahetkel kontrollida ja auditeerida nimetatud turvameetmete rakendatust ja Tarnija peab seda toetama.