**SISUKORD**

# 1 ÜLDSÄTTED

## 1.1 Eesmärk

Infoturbe poliitika eesmärk on kehtestada asutuseülesed põhimõtted ja juhised, mis tagavad Transpordiametis (edaspidi TRAM-is) teabe, infosüsteemide ja infovarade kaitse konfidentsiaalsuse, tervikluse ja käideldavuse põhimõtetest lähtudes. Poliitika aitab ennetada infoturbeintsidente, maandada riske ning tagada õigusaktidest tulenevate ja lepinguliste nõuete täitmist. Samuti loob see aluse teenistujate ja teiste isikute infoturbealase teadlikkuse tõstmisele ning ühtse turbekultuuri kujundamisele TRAM-is.

TRAM lähtub infoturbe põhimõtete kehtestamisel ISO/IEC 27001 standardist, arvestades konkreetsele teenusele seadustest või nende alusel kehtestatud õigusaktidest tulenevaid erisusi või nõudeid.

## 1.2 Infoturbe poliitika rakendamise ulatus ehk käsitlusala

Infoturbe poliitika rakendub kogu asutuse ulatuses ning on kohustuslik kõigile teenistujatele, praktikantidele, lepingulistele partneritele, alltöövõtjatele ning muudele füüsilistele ja juriidilistele isikutele, kellel on volitatud juurdepääs asutuse teabele või infovaradele.

Poliitika hõlmab kõiki infovarade töötlemise, säilitamise ja edastamisega seotud tegevusi, sõltumata infokandjast (sh digitaalne, paberkandjal) või kasutatavast tehnoloogilisest vahendist (sh tööjaamad, sülearvutid, mobiilsed seadmed, serverid, pilveteenused, võrguseadmed jms).

Infoturbe poliitika kehtib ka kolmandate osapoolte (mh arenduspartnerid ja lepingupartnerid näit OIXIO) hallatavatele teenustele ja süsteemidele juhul, kui need sisaldavad või töötlevad asutuse teavet.

Kõigil asjaomastel osapooltel on kohustus järgida infoturbe poliitika nõudeid ning rakendada vastavaid meetmeid, et tagada teabe konfidentsiaalsus, terviklus ja käideldavus vastavalt kehtivatele õigusaktidele, asutusesisesele korrale ning lepingulistele kohustustele.

Infoturbe poliitika alusel kehtestatud spetsiifilised töökorrad ja juhendid (näiteks varunduse ja logimise reeglid) peavad lähtuma käesolevas poliitikas kirjeldatud põhimõtetest ja olema ajakohased.

## 1.3 Sihtgrupp

- TRAM teenistujad
- TRAM praktikandid
- TRAM-is lepingu alusel teenust osutavad füüsilised ja juriidilised isikud, kes omavad juurdepääsu või vahetut kokkupuudet TRAM-i teabega või infovaradega.

## 1.4 Huvigrupid

- Ameti peadirektor
- Järelevalve asutused
- Õiguskaitseorganid

# 2 MÕISTED JA LÜHENDID

- **Infovara** – TRAM-i infosüsteemi kuuluvad varad sh võrgud, IT seadmed, tarkvara, rakendused ja andmekogud.

- **VPN** – krüpteeritud virtuaalne privaatvõrk sh MACsec krüpteering.
- **Wi-Fi** – traadita kohtvõrk.
- **CERT-EE** – RIA struktuurüksus, kes tegeleb küberintsidentide registreerimise ja lahendamisega.
- **Andmekogu** – riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks
- **Juhtumite haldussüsteem** – Atlassiani perekonda kuuluv Jira service desk kuhu tehakse pöördumised ja tööülesannete jagamine töötajatele.

## 3 OSAPOOLED JA VASTUTUS

| Osapool | Vastutus protsessi raames |
|---|---|
| Ameti peadirektor | • Kehtestab infoturbe poliitika. |
| Ameti juhtkond | • Kiidab heaks infoturbe poliitika põhimõtete rakendamist täpsustavad asutuseülesed nõuded.<br>• Määrab infovaradele Peakasutajad ja kinnitab infovaradele omanike määratud turvaklassid.<br>• Kiidab heaks teenuste infoturbe riskianalüüsi ja aktsepteerib jääkriskid.<br>• Kiidab heaks teenuse toimimiseks vajaliku sisemise andmekogu asutamise ja lõpetamise ning määrab Peakasutaja. |
| Infoturbejuht | • Tagab infoturbe poliitika ja infoturbe põhimõtete ajakohasuse.<br>• Nõustab infovarade ja sisemiste andmekogude omanikke ning valdkonnajuhte ja teenuseomanikke turbemeetmete rakendamise ja turvaklasside määramise osas.<br>• Nõustab, eesmärgiga tagada kvaliteetne ja turvaline teenus ja teenustele sobilikud IT lahendused.<br>• Kontrollib infoturbe nõuetest kinnipidamist ja koostab aruandeid kontrollide kohta.<br>• Korraldab teenustele ja infovaradele nõuetekohaste turvatestide ja -auditite tegemist.<br>• Viib infoturbeintsidendi korral läbi menetluse ja teavitab küberturbe intsidendist CERT-EE'd. |

## 4 SEOTUD DOKUMENDID

### 4.1 Õigusaktid

- Avaliku teabe seadus (AvTS);
- Isikuandmete kaitse seadus (IKS);
- Küberturvalisuse seadus (KüTS);

### 4.2 Seotud juhendid ja muud dokumendid

- TT_03_K1_Infosüsteemide kasutamise kord
- TT_13_P1_Riskijuhtimise poliitika
- ISO/IEC 27001

## 5 INFOTURBE PÕHIMÕTTED

### 5.1 Õiguste haldus

5.1.1 TRAM-i infovarade kasutajaõiguste andmisel tuleb lähtuda minimaalsuse printsiibist ja vajaduspõhisusest. See tähendab, et kasutajaõigusi antakse üksnes tööülesannete täitmisest tingitud vajadusest ja üksnes ulatuses, mis on vajalik konkreetsete tööülesannete täitmiseks. Kasutajaõiguste ajakohasuse eest vastutab Peakasutaja, kes viib läbi kasutajaõiguste auditi tulenevalt ISKK-st.

5.1.2 Infovarade kasutajaõigused jagunevad tavakasutaja õigusteks ja administraatori õigusteks. Tööülesandeid, mis ei eelda administraatori õigusi, tohib täita üksnes tavakasutaja õigustes.

5.1.3 Infovarade kasutajaõigusi kinnitab Peakasutaja või süsteemi administraator.

5.1.4 Kasutajaõigusi taotleb ja vajaduse ära langemisel esitab sulgemise taotluse töötaja vahetu juht. Kõik taotlused registreeritakse juhtumite haldussüsteemis.

5.1.5 Infovarade kasutajaõigused on üksnes personaalsed ja kasutajal on keelatud enda kontoga seotud salasõna avalikustamine teistele isikutele v.a IT seadmetes, kus personaalse kasutaja loomine ei ole võimalik ja infoturbe riskid on maandatud teiste meetmetega.

5.1.6 Kasutajaõigustega seotud salasõna kehtivuse aeg on 90 päeva. Selle möödudes nõuab kasutajate keskhaldus salasõna vahetamist või lukustab konto. Kui infovarale ei rakendu kasutajate keskhaldus on infovara omanik kohustatud tagama salasõna muutmise 90 päeva möödudes. Nõue ei rakendu punktis 5.3 kirjeldatud deponeeritud kasutajatunnustele sh salasõnadele.

5.1.7 Administraatorite õigustega salasõna kehtivuse aeg keskhaldussüsteemi puudumisel on erandkorras maksimaalselt 1 (üks) aasta. Selle tingimuseks on personaalse ja keeruka salasõna kasutamine, mis koosneb vähemalt 14 tähemärgist, suur- ja väiketähtedest ning numbritest, sh ei tohi salasõna sisaldada isikule viitavaid andmeid. Ühe (1) aastase tähtaja möödudes tagab infovara omanik salasõna vahetamise ning fikseerib tegevuse taasesitamist võimaldavas vormis. Nõue ei rakendu punktis 5.3 kirjeldatud deponeeritud kasutajatunnustele sh salasõnadele.

5.1.8 Kasutajaõiguste taotlemise ja andmise töökorraldus on kirjeldatud TRAM TT_03_K1_Infosüsteemide kasutamise korras.

5.1.9 TRAM-i infosüsteemi kasutajaõiguse saamisega kaasneb TRAM teenistujatel küberteadlikkuse e-koolituse läbimise ja -testi tegemise kohustus. TRAM-i infosüsteemi kasutaja peab läbima küberteadlikkuse e-koolituse ja testi kord aastas ning uued teenistujad nelja kuu jooksul tööle asumisest. Küberteadlikkuse e-koolituse ja -testi sisu ajakohasuse eest vastutab infoturbejuht.

## 5.2 Konfidentsiaalsuskohustus

5.2.1 Konfidentsiaalsuskohustuse alusel on TRAM-i infosüsteemi kasutaja (sh töövõtu-, käsunduslepingus või muus lepingulises suhtes olev isik) kohustatud järgima käesoleva infoturbe poliitika ja selle alusel kehtestatud töökordadest tulenevaid nõudeid piiratud kasutusega teabe ja andmete kasutamiseks üksnes tööülesannetest või lepingust tulenevate ülesannete täitmiseks.

5.2.2 TRAM-i infosüsteemi kasutaja on kohustatud:

5.2.2.1 hoidma saladuses temale tööülesannete ja lepingust tulenevate kohustuste täitmiseks usaldatud piiratud kasutusega andmeid, sh infovarade kasutamiseks vajalikku salasõna ja teavitama koheselt infoturbejuhti, kui see on saanud teatavaks kolmandatele isikutele;

5.2.2.2 hoidma saladuses TRAM-i infosüsteemi tehnilist teavet, mis seotud infosüsteemi turvalisusega või mis ei ole avalik teave;

5.2.2.3 hoidma saladuses TRAM-i klientidega seotud teavet, mis liigitub ärisaladuse alla või mis on klientide poolt märgistatud piiratud kasutusega teabeks;

5.2.2.4 hoidma saladuses tööülesannete või lepingust tulenevate kohustuste täitmise käigus teatavaks saanud füüsilise isiku andmeid ja andma selgitusi andmete töötlemise kohta, kui see on vajalik andmesubjekti õiguste tagamiseks;

5.2.2.5 täitma kõiki TRAM-i TT_03_K1_Infosüsteemide kasutamise korrast tulenevaid kohustusi, mis on seotud andmete turvalisuse ja konfidentsiaalsuse tagamisega.

5.2.3 Välise teenuseosutajaga lepingu sõlmimisel on TRAM-i teenistujast teenuse tellija kohustatud korraldama teenuseosutajaga konfidentsiaalsusleppe sõlmimise, kui teenuse osutamine on seotud TRAM-i infosüsteemile ja seal paiknevatele andmetele juurdepääsuga. Konfidentsiaalsusleping registreeritakse dokumendihaldussüsteemis.

## 5.3 Kasutajatunnuste deponeerimine

5.3.1 Administraatoriõiguste deponeerimise eesmärk on TRAM-i teenuste toimepidevuse tagamine ja tööülesannete jätkuv täitmine nii planeeritavate (puhkus, töölähetus) kui ettenägematute juhtumite (haigus, õnnetus, töölt lahkumine) puhul.

5.3.2 Deponeerimise alla kuuluvad infovara administraatoriõiguste kasutajanimed ja salasõnad, millel on oluline mõju infosüsteemile. Deponeerimisprotsessi viivad läbi infovara administraator ja infoturbejuht, kes hoiustavad asjakohast teavet suletud turvaümbrikus, mis asub TRAM-i Tallinn, Valge 3 aadressil asuvas seifis. Turvaümbrikule kantakse järgmine informatsioon:

- infosüsteemi või -vara nimetus;
- administraatori nimi;
- deponeerimise kuupäev.

5.3.3 Deponeerimisele kuuluv salasõna peab olema vähemalt 14 tähemärki pikk ja see genereeritakse programmiliselt (näiteks KeePass) tagamaks selle võimalikult keeruka ja raskesti ära arvataval kujul. Deponeerimisele kuuluva salasõna muutmine ja uue salasõna deponeerimine toimub vastavalt konkreetsele infovarale sätestatud nõuetele, kuid mitte harvem kui kord 4 (nelja) aasta jooksul, tingimusel, et salasõna ei ole vahepeal kasutatud. Salasõna kasutamisel genereeritakse uus deponeerimisele kuuluv salasõna.

5.3.4 Deponeerimise järgselt kannab toimingu teinud infovara administraator deponeeritud kasutajaõiguste registrisse järgmise info:

- registreerimisnumber;
- deponeerija nimi ja deponeerimise kuupäev;
- infovara või selle osa nimetus;
- muutmise kuupäev ja põhjus.

5.3.5 Deponeeritud kasutajaõiguste aktiveerimine leiab aset juhul, kui infovara administraatori asendamine muutub vajalikuks või kui tekib muu eriolukord, mis takistab administraatoril oma tööülesandeid täitmast, kuid nõuab samas kiiret sekkumist. Sellisel juhul teavitatakse koheselt infoturbejuhti, kes vastutab turvaümbriku avamise ja selle kasutamise fikseerimise eest deponeeritud kasutajaõiguste registris. Turvaümbriku avamisel peab kohal olema vähemalt infoturbejuht ja süsteemi administraator, erandjuhtudel võib infoturbejuhti asendada asutuse juht. Eriolukorra lõppedes muudetakse deponeerimisele kuuluv salasõna, järgides deponeerimise reegleid.

5.3.6 Vähemalt kord aastas kontrollib infoturbejuht deponeerimise nõuete täitmist ja esitab selle kohta aruande juhtkonnale.

## 5.4 Infovarade soetamine ja haldus

5.4.1 Infovarade soetamisel peab lähtuma teenusele esitavatest käideldavuse, tervikluse ja konfidentsiaalsuse nõuetest, millele hakkab soetatav infovara riist- või tarkvaralist tuge pakkuma. See tähendab, et lisaks kasutamise funktsionaalsusele tuleb hinnata:

5.4.1.1 infovara funktsionaalset võimekust pakkuda kõrgekäideldavat töökindlust;

5.4.1.2 infovara koostoimet teiste TRAM-i infosüsteemi kuuluvate infovaradega;

5.4.1.3 infovara kasutajaõiguste halduse olemasolu;

5.4.1.4 infovara võimekust töödelda krüpteeritud andmeid;

5.4.1.5 infovaras andmete töötlemise fakti salvestamist logifaili ning logi talletamise või keskse arhiveerimise võimekust.

5.4.2 Infovara eelkirjeldatud turvanõuded tagab struktuurüksuse juht, kes vastutab infovara soetamise eest. Vastutaja kooskõlastab infovara turvanõuded või selle sobivuse TRAM-i infosüsteemiga infoturbejuhiga ja IT osakonnaga.

5.4.3 Soetatava infovara liidestamisel TRAM-i infosüsteemiga peab vastutaja tagama, et infovarale koostatakse taasteplaan, mis sisaldab konkreetse infovara konfiguratsiooni juhiseid intsidendist lähtuva katkestuse kõrvaldamiseks ja toimimise taastamiseks. Taasteplaan peab olema koostatud taasesitamist võimaldavas vormis (soovitatavalt elektroonsel kujul). Vastutaja peab tagama, et taasteplaani testitakse regulaarselt ja seda vajadusel täiendatakse, kui toimub infovara tarkvara uuendamine.

5.4.4 TRAM-i teenuste toimimiseks vajalikud ja TRAM-i infosüsteemiga liidestatud rakendused ja tarkvara peab lisaks vastama autoriõiguste nõuetele – soetatud vastavalt litsentseerimistingimustele.

5.4.5 Uue rakenduse ja tarkvara kasutusele võtmise peab eelnevalt kooskõlastama IT osakonna juhataja ja infoturbejuhiga. Eelnevat kooskõlastust läbimata rakenduste ja tarkavara lisamine tööarvutitesse on kasutajatel keelatud.

5.4.6 TRAM-i infovarade Kaughaldus (*remote desktop*) on lubatud infovara Peakasutaja loal ja turvatud keskkonna kaudu. Alalise kaughalduse juurdepääsu annab süsteemi administraator ja see tellitakse läbi juhtumite haldussüsteemi.

5.4.7 TRAM-i lepingulistele partneritele võimaldatakse Kaughalduse juurdepääs TRAM-i infosüsteemis paiknevale infovarale üksnes vajaduspõhise teenuse osutamiseks ja teenuse tellijast TRAM-i töötaja kontrolli all olevas keskkonnas. Kõik teenuseosutajate Kaughalduse juurdepääsu avamised registreeritakse juhtumite haldussüsteemis. Peale juurdepääsu vajaduse ära langemist peab teenuse tellijast Peakasutaja esitama juhtumite haldussüsteemis taotluse juurdepääsu sulgemiseks.

5.4.8 Infovarade soetamise ja haldusega seotud töökorraldus on kirjeldatud TRAM-i TT_03_K1_Infosüsteemide kasutamise korras.

## 5.5 Piiratud kasutusega andmete töötlemine ja andmekogud

5.5.1 TRAM-i piiratud kasutusega andmed on mistahes kujul talletatud:

5.5.1.1 tehniline teave teenuste ja neid toetavate infovarade kohta, millel on määrav roll teenuse toimepidevusele;

5.5.1.2 avaliku teabe seaduse alusel asutusesiseks kasutamiseks mõeldud teave;

5.5.1.3 klientide ärisaladus ja lepinguga piiratud kasutamiseks mõeldud andmed;

5.5.1.4 füüsilise isiku andmed;

5.5.1.5 riigisaladuse ja salastatud välisteabe kaitse korraga hõlmatud teave.

5.5.2 TRAM-i valduses olevaid piiratud kasutusega andmeid peab kaitsma nõuetekohaste ja piisavate organisatsiooniliste, füüsiliste ja infotehnoloogiliste turvameetmetega, et tagada nende salajasus ja üksnes reeglipärane töötlemine.

5.5.3 Mõjusate infotehnoloogiliste turvameetmete rakendamiseks peab andmeid hoidma andmekogus, millele on rakendatud kasutajate haldus, andmetöötluse logimine ja andmete varundamine. Vajalikud infotehnoloogilised turvameetmed määrab kirjalikult teenuse või infovara omanik, kooskõlastades need infoturbejuhiga.

5.5.4 Mõjusate organisatsiooniliste turvameetmete rakendamiseks on oluline, et Andmekogule on määratud arendamise ja kasutamise eest vastutav omanik ning kasutajate haldust ja tuge pakkuv Peakasutaja.

5.5.5 Andmekogu juurdepääsu andmise otsustab ja annab andmeomanik, tehes seda ise või Peakasutaja kaudu. Kui andmekogu omanik on andmekogus määranud kasutajarollid ja õiguste andmise rollipõhiselt, siis võib juurdepääsu otsustada Peakasutaja

5.5.6 TRAM-i andmekogud asutatakse ja nende kasutamine lõpetatakse vastavalt kehtivatele õigusaktidele. Ainult asutuse sisemise töökorralduse vajadusteks peetavad ja riigi infosüsteemi mittekuuluvad andmekogud asutatakse ja lõpetatakse juhtkonna otsuse alusel.

5.5.7 Mõjusate füüsiliste turvameetmete rakendamiseks peab Andmeomanik selle asutamise ja paigutamise TRAM-i taristusse kooskõlastama infoturbejuhiga, kes tagab andmetest tulenevate turvariskide hindamise ja nõutavate turvameetmete rakendamise.

## 5.6 Andmevarundus ja arhiveerimine

5.6.1 Andmevarunduse eesmärk on andmete elektroonilise ja regulaarse varundamisega tagada TRAM-i teenuste nõuetekohane käideldavus ja teenustega seotud andmete vajalik terviklus.

5.6.2 Konkreetse teenusega seotud andmete varundamise nõuded (sagedus, säilitusaeg ja nõuded arhiveerimisele) määrab teenuseomanik, kooskõlastades selle IT osakonna süsteemihalduse üksusega.

5.6.3 TRAM-i Peakasutaja, kellele ei rakendu teenuseomaniku varundamise nõuded, otsustab lähtuvalt infovara funktsionaalsusest ja seal sisalduvate andmete kooseisust kas infovara andmetele peab varunduse rakendama või mitte. Otsus kooskõlastatakse infoturbejuhiga ja informeeritakse IT osakonna juhatajat.

5.6.4 TRAM-is on andmete varundamiseks kasutusel varundussüsteem Veeam/Nutanix. Kui infosüsteemi infovara ei ole liidestatud Veeami või Nutanixiga, tagab infovara administraator varundamise dokumenteerimise ja läbiviimise vastavalt käesoleva dokumendi punktis 5.6.6. kirjeldatud üldistele varundusnõuetele.

5.6.5 Kui TRAM-i infosüsteemi infovarale ei ole määratud varunduse nõudeid, kuid lähtuvalt infovara ja seal sisalduvate andmete olulisusest on see vajalik, siis on IT osakonna süsteemihalduse üksusel ja infoturbejuhil õigus rakendada üldisi varundusnõudeid.

5.6.6 TRAM-i üldised varundusnõuded on:

5.6.6.1 varunduse sagedus kord päevas – säilitatakse 14 päeva ja seejärel kustutakse;

5.6.6.2 kuu täisvarundus – säilitatakse 12 kuud ja seejärel kustutakse;

5.6.6.3 aasta varundus – säilitatakse 3 aasta ja seejärel kustutatakse;

5.6.6.4 varunduse käivitusaeg peale tööaega.

5.6.7 Varunduseplaani teenuste ja infovarade lõikes haldab varunduse IT osakonna süsteemihalduse üksus.

5.6.8 Varundatud andmetele juurdepääs antakse juhtumite haldussüsteemis registreeritud teenuseomaniku või infovara Peakasutaja taotluse alusel.

5.6.9 Varundatud andmete taastamise kontrolli tehakse vähemalt kord aastas juhuvaliku alusel ja selle eest vastutavad infoturbejuht ja IT osakonna süsteemihalduse üksus.

## 5.7 Andmeside- ja kaabelvõrgud ja võrguseadmed

5.7.1 TRAM-i andmeside- ja kaabelvõrgud peavad olema projekteeritud ja paigaldatud selliselt, et nad töö- ja purunematuse kindluselt tagaksid TRAM-i teenuste toimepidevuse. Andmeside- ja kaabelvõrgud millel on otsene mõju TRAM-i teenustele, peavad vastama kõrgkäideldavuse taseme turbemeetmetest tulenevatele nõuetele. Kui andmeside- ja kaabelvõrgud tagavad teenuse toimimise, millele rakenduvad õigusaktidest tulenevad erinõuded, siis peavad need olema rakendatud ka konkreetsele andmeside- või kaabelvõrgule.

5.7.2 Andmeside- ja kaabelvõrkude projekteerimisel ja võrguseadmete paigaldamisel tuleb koostada nõuetekohane (projekti)dokumentatsioon, sh plaanid, mis tuleb talletada TRAM-i dokumendihaldussüsteemis ja/või sisemisse andmekogusse, mille peab kooskõlastama süsteemihalduse üksusega.

5.7.3 TRAM-i andmeside välisühendus peab olema tagatud rohkem kui ühe välislingiga. Välisühendused võivad olla kasutusel paralleelselt. Peab olema tagatud, et ühe välislingi tõrke korral marsruuditakse kogu asutuse välisliiklus toimivale lingile.

5.7.4 Sisevõrgud peavad olema füüsiliselt ja loogiliselt segmenteeritud viisil, mis tagab piisava tõrkekindluse või nõuetekohase eraldatuse TRAM-i erisuguste eesmärkide ja andmetega süsteemidele. Iga sellise segmendi juures peab olema kindlaks määratud segmendi detailne

kaitsevajadus. Kaitsevajaduse määramine toimub segmenti kasutava TRAM-i teenuseomaniku antud nõuetest konfidentsiaalsusele, käideldavusele ja terviklusele, mis on läbi arutatud ja kooskõlastatud infoturbejuhi ning IT osakonna süsteemihalduseüksuse juhiga.

5.7.5 Organisatsiooni kogu võrk peab olema kaitstud vastava turvalüüsi abil, mille hoiatusteateid analüüsitakse ja lähtuvalt riskiastmest rakendatakse täiendavaid turvameetmeid.

5.7.6 VPN-i all tuleb vaadelda nii mobiilsete kaugtöökohtade ühendamist asutuse sisevõrguga kui ka asutuse erinevates hoonetes asuvate kohtvõrkude liitmist üle turvalise ühenduskanali. Erandkorras ja osutatava teenuse tagamiseks ühendatakse TRAM-i sisevõrk VPN-iga koostööpartneri võrguga, kuid tagades siiski võrkude segmenteerimise ja teenusega mitteseotud andmete eraldatuse. Iga TRAM-i sisevõrku pääsemine peab toimuma läbi turvalüüsi. Väliste ühenduste loomisel on turvalüüsist möödaminek keelatud. Kaugligipääsude puhul tuleb tagada, et kogu andmesideliiklus oleks marsruuditud üle turvalise VPN-kanali.

5.7.7 TRAM-i hoonetes on võimalik kasutada krüpteeritud Wi-Fi teenust. Wi-Fi kohtvõrguteenus ei ole samaväärne asutuse sisevõrguteenusega ja mõeldud mobiilsete seadmete ühendamiseks võrku. Ilma VPN-ühenduse aktiveerimiseta ei tohi olla Wi-Fi kohtvõrgust pääsu TRAM-i sisevõrgu teenustele ega seadmete haldusliidestele. Wi-Fi't saavad kasutada nii TRAM-i töötajad kui külalised. TRAM-i töötajatel on Wi-Fi kohtvõrgust sisevõrgu teenustele juurdepääsuks tarvilik aktiveerida VPN-ühendus. Asutuse külalised saavad kasutada Wi-Fi't nõuete kinnitamisega. TRAM-i töötajate isiklike seadmete kasutamine TRAMi Wi-Fi's toimub külalistele kehtiva korra alusel.

5.7.8 TRAM-i võrguseadmed peavad vastama ajakohastele turvanõuetele sh seadmete enda tarkavara peab olema ajakohane ja uuendatud viimasele stabiilsele versioonile. Uuenduste eest vastutab seadme eest vastutav administraator.

5.7.9 Seadmete haldust tohib teha turvalise ühenduse kaudu ja kui võimalik tuleb pääsupunktide administratiivne õhuliides deaktiveerida.

5.7.10 Võrguseadme kasutusse võtmise konfiguratsioon tuleb dokumenteerida (taasteplaanid või -kirjeldus) selliselt, et administraator või tema asendaja suudaks alati dokumentatsiooni abil tuvastada, millise konfiguratsiooniga on tegu ja selle järgi taastada seadme vajalik töövõimekus. Taasteplaanide testimine toimub kord aastas juhuvaliku alusel või intsidendi käigus, mis võimaldab sellist taasteplaani rakendamist, tulemused registreeritakse juhtumite haldussüsteemis.

5.7.11 Võrguseadmete kasutusele võtmisel tuleb muuta algupärane salasõna ja määrata uus, lähtuvalt käesolevast poliitikast tulenevatest nõuetest. Olenevalt võrguseadme konfiguratsioonist ja kasutusotstarbest tuleb salasõna deponeerida käesoleva poliitikaga kehtestatud reeglite kohaselt.

5.7.12 TRAM-i infosüsteemi kasutaja tohib TRAM-i võrku ühendada üksnes TRAM-i poolt väljastatud seadmeid. Uute või ajutiste TRAM-i väliste seadmete ühendamine võrku tuleb eelnevalt kooskõlastada infoturbejuhi ja IT osakonna arvutitöökoha eest vastutava spetsialistiga.

## 5.8 Logimine ja monitooring

5.8.1 Logimise eesmärgiks on tuvastada ründed ja volitamata tegevused, et selle informatsiooni abil tõhustada asutuse infosüsteemi turvalisust ja tagada asutuse töövõime ja teabesaladuse

nõuetekohane hoidmine. Salvestatud ja analüüsitud logi võib olla tõendiks TRAM-i sisekontrolli menetluses või intsidendi menetlemisel.

5.8.2 TRAM-i infovarad sh andmekogud ja registrid, mis sisaldavad isikuandmeid, ärisaladust või muud piiratud kasutusega andmeid, peavad talletama auditlogis teavet vähemalt järgmiste tegevuste kohta:

5.8.2.1 kes töötles andmeid;

5.8.2.2 millal ja millises infovaras töödeldi andmeid;

5.8.2.3 milliseid andmeid töödeldi.

5.8.3 Auditlogi salvestatakse analüüsikeskkonda (SIEM), kus tagatakse selle puutumatus ja üksnes vajaduspõhine juurdepääs. Auditlogi hoitakse 1 (üks) aasta ja säilitamise tähtaja möödudes see kustutatakse.

5.8.4 TRAM-i toimepidevust toetavate infovarade süsteemi ja turvalogi kasutatakse infosüsteemi turvalisust ja käideldavust ohustavate sündmuste avastamiseks ja ennetamiseks. Samal eesmärgil talletatakse TRAM-i andmesidevõrgu kasutamise logi. Süsteemi ja turvalogi talletatakse logi agregaatorisse ja seda hoitakse 90 päeva.

5.8.5 TRAM-i teenuste ja infosüsteemi käideldavuse tagamiseks on rakendatud monitooringusüsteem Zabbix. Automatiseeritud monitooringusüsteemi eesmärk on teavitada TRAM-i süsteemihaldust kõrvalekaldest infosüsteemi infovara määratud tasemest (intsidendist), mis võimaldab kohese reageerimise ja infosüsteemist sõltuva teenuse taastamise. Intsidendid registreeritakse juhtumite haldussüsteemis.

5.8.6 TRAM-i teenustele, millele rakendub kõrgkäideldavuse nõue, peab olema rakendatud monitooringusüsteem. Selleks määratleb teenuseomanik teenusele ja sellega seotud infosüsteemi infovara käideldavuse taseme ja sellest tulenevalt intsidendile reageerimise ja lahendamise prioriteetsuse, mis fikseeritakse TRAM-i sisemises teenusleppes.

5.8.7 TRAM-i teenuste, millele ei rakendu kõrgkäideldavuse nõue, monitooringusüsteemiga liidestamise otsustab teenuseomanik. Liidestuse korral peab teenuseomanik kirjeldama infovara käideldavuse taseme ja sellest tulenevalt intsidendile reageerimise ja lahendamise prioriteetsuse.

## 5.9 Infoturbeintsident ja kriisihaldus

5.9.1 Infoturbeintsidendiks nimetatakse sündmust, mille tagajärjel:

- toimus TRAM-i teenuse planeerimata pikemaajaline katkestus, mis ületab SLA-ga määratud teenuse käideldavuse %;
- toimus piiratud kasutusega andmete või füüsilise isiku andmete lekkimine;
- toimus TRAM-i vara hävimine või ründest tingitud oht, millel on kahjustav mõju;
- toimus tegevus, mis kahjustab TRAM-i kui teenuspakkuja mainet.

5.9.2 Kõik infoturbeintsidendid registreeritakse juhtumite haldussüsteemis ja kõrge tasemega intsidentidest teavitatakse infoturbejuhti esimesel võimalusel. Intsidentide lahendamist juhib vastava teenuse või valdkonna juht. Juhtumite haldussüsteemis intsidentide registreerimise ja menetlemise kord kehtestatakse intsidentide halduse juhendiga.

5.9.3 Kahjustava mõjuga sh mainekahjuga lõppenud infoturbeintsidentide korral, mis eeldavad intsidendi põhjuste välja selgitamist, viib infoturbejuht läbi menetluse lähtuvalt

TT_13_K3_Sisekontrolli korrast. Teenistuskohustuste rikkumisena käsitletavate infoturbeintsidentide korral menetleb teenistuskohustuste rikkumist sisekontrolör.

5.9.4 Kahjustav mõju ehk kriitiline tagajärg on kui:

- Intsident puudutab elutähtsa teenuse osutamisega seotud infovara.
- Avalike teenuste osutamine ei ole võimalik.
- Mõjutatud on väga suur hulk kasutajaid, sh kliendid, avalikkus, partnerid.
- Rahaline kulu / kahju enam kui 50000 eurot ja kaasnevad kulud kolmandale osapoolele. Kaasneb oluline maine kahju, sh negatiivne meediakajastus, avalikkuse pahameel, regulaatorite negatiivne reageering.

5.9.5 Kriis infoturbe mõistes on kõrge (I) tasemega intsident või ootamatu või haruldane sündmus või kahju tekitav olukord, kus TRAM-i teenuse kokkulepitud tööprotsessid ei toimi nii nagu nad peaksid ja mis vajab kiiret, kohandatud ning asjakohast reageerimist.

5.9.6 Kriisis toimimise reeglid, kriisimeeskond ja nende ülesanded on kehtestatud juhendis TT_13_K5_Transpordiameti kriisiplaan.

5.9.7 Küberintsidentide korral koostab infoturbejuht intsidendi raporti ja esitab selle CERT-EE'le ja asutuse juhile.

### 5.10 Riskide hindamine ja audit

5.10.1 TRAM-i teenustega seotud infoturberiskide hindamisel tuleb lähtuda konkreetsele teenusele seaduse või teenustasemelepingus (SLA) sätestatud turbenõuete rakendamise ja nende auditeerimise kohustusest.

### 5.11 Infoturbenõuete rakendamine

5.11.1 Infoturbe poliitikast tulenevate infoturbenõuete rakendamise tagavad struktuurüksuste juhid, kelle pädevuses on käesolevas poliitikas kirjeldatud nõuete rakendamine.

5.11.2 Infoturbe poliitikaga kehtestatud turbenõuete järgimist kontrollib infoturbejuht. Infoturbejuhil on õigus vajaduspõhise kontrolli eesmärgil saada juurdepääs mistahes TRAM infosüsteemi kuuluvale infovarale, andmetele või tehnilisele teabele.

## 6 TOETAVAD INFOSÜSTEEMID

- Atlassian Jira – projektihalduse, juhtumite halduse ja probleemide jälgimise infosüsteem.