Siseministeeriumi infotehnoloogia- ja arenduskeskus

KÄSKKIRI

Tallinn 01.07.2025 nr 1-1/106

Siseministeeriumi infotehnoloogia- ja arenduskeskuse infoturbe kord

Siseministri 17. veebruari 2020 määruse nr 8 „Siseministeeriumi infotehnoloogia- ja arenduskeskuse põhimäärus“ § 10 lg 2 alusel:

1. Kehtestan käskkirja lisaks oleva Siseministeeriumi infotehnoloogia- ja arenduskeskuse infoturbe kord

2. Käskkiri jõustub 1. augustil 2025.

3. Tunnistan alates 1. augustist 2025 kehtetuks peadirektori 25.04.2024 käskkirja 1-1/25 „Siseministeeriumi infotehnoloogia- ja arenduskeskuse infoturbe kord“.

4. Panen kontrolli käskkirja täitmise üle infoturbeosakonna juhatajale.

LISAD:

Lisa 1: Siseministeeriumi infotehnoloogia- ja arenduskeskuse infoturbe kord

(allkirjastatud digitaalselt)

Mart Nielsen
peadirektor

Lisa 1. Siseministeeriumi infotehnoloogia- ja arenduskeskuse infoturbe kord

Sisukord

1. Üldsätted

1.1. Infoturbe kord (edaspidi kord) sätestab infoturbe halduse põhimõtted ja korralduse, mida rakendatakse kõigi Siseministeeriumi infotehnoloogia- ja arenduskeskuse (edaspidi SMIT) teenuste ja infovarade turvalisuse tagamisel, sh kasutaja käitumise juhendamisel ja reguleerimisel, infovara arendamisel ja haldamisel, taristu muudatuste planeerimisel ja läbiviimisel, kordade, juhiste ja muude reeglite kehtestamisel.
1.2. Korraga kehtestatud infoturbe nõuded lähtuvad siseturvalisuse valdkonna spetsiifikast, rahvusvahelistest ja riigisisestest regulatsioonidest, valdkonna parimast praktikast ning on kooskõlas SMITis rakendatud ISO/IEC 27001 infoturbestandardiga.
1.3. Korra eesmärk on infoturbemeetmete rakendamise kaudu tagada teenuste konfidentsiaalsus, terviklus ja käideldavus vastavalt nõuetele ja vajadustele kõigis SMITi protsessides ning kaitsta seeläbi organisatsiooni kui tervikut ning pakkuda turvalisi teenuseid klientidele.
1.4. Kord ei reguleeri riigisaladuse ja salastatud välisteabe alaseid protsesse.
1.5. Kord kohaldub SMITi töötajatele, praktikantidele ja välistele partneritele.
1.6. Korras sätestatud nõuete rikkumist loetakse töökohustuse või lepingu rikkumiseks. Infoturbeosakond võib seada infosüsteemide kasutamise eelduseks infoturbe koolituse ja/või testi läbimise.
1.7. Korra täitmist korraldab infoturbejuht ja erisused korras sätestatule tuleb taasesitatavas vormis kooskõlastada infoturbeosakonnaga. Erand peab olema ajaliselt piiritletud ja põhjendatud.
1.8. Korra iga-aastase ülevaatamise ja ajakohastamise korraldab infoturbeosakonna juhataja (edaspidi infoturbejuht).

Vaata lisaks: Infoturbeosakonna põhimäärus

2. Mõisted

2.1. **Andmekandja** on andmete talletuseks või edastuseks kandev vahend.
2.2. **Andmesidevõrk** on SMITi kasutajavõrk ja lõpptarbija seadmed.
2.3. **Infoturbe halduse süsteem (*ingl Information Security Management System,* ISMS)** on struktureeritud raamistik, mis koosneb poliitikatest, protseduuridest, juhistest ning nendega seotud ressurssidest ja tegevustest, mida organisatsioon kollektiivselt haldab, püüdes kaitsta oma varasid.
2.4. **Infoturve** on turvameetmete loomise, valimise ja rakendamise protsesside kogum, aga ka teabe konfidentsiaalsuse, tervikluse ja käideldavuse säilitamine.
2.5. **Infovara** on informatsioon, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid või muu vara, mis sisaldab või kannab väärtuslikku informatsiooni SMITi jaoks. Näiteks teave, andmed, tarkvara, füüsiline vara (taristu, hoone, riistvara, sisseseade vm), rahaline vara, teenus, inimressurss (inimesed, kvalifikatsioon, oskused, kogemused), oskusteave, mitteaineline vara (maine, kuvand jms).
2.6. **Infovara kasutaja** on infovara kasutama volitatud isik.
2.7. **Infovara omanik** on ühe või mitme infovara eest vastutav isik, kes eraldab nende varade turvameetmete tagamiseks ressursid, kinnitab meetmed, volitab juurdepääsu ja seirab meetmete toimivust.
2.8. **Irdandmekandja** on seade, mida kasutatakse andmete transportimiseks ja säilitamiseks või neile mobiilse juurdepääsu tagamiseks. Irdandmekandjate hulka kuuluvad näiteks välised kõvakettad, CD-d, DVD-d, magnetlindid, mälukaardid, mälupulgad, SD-kaardid, fotoaparaadid jmt.
2.9. **Kohustuste lahusus** on tööprotsessi sammude jaotamine inimestele nii, et toimingu kinnitaja ei oleks selle toimingu sooritaja.

2.10. **Konfidentsiaalne teave** on igasugune mitteavalikuks määratud teave, mis on mõeldud piiratud arvule isikutele ja piiratud kasutamiseks.
2.11. **Konfidentsiaalsus** on teabe omadus olla kättesaamatu või paljastamatu volitamata isikutele, olemitele või protsessidele.
2.12. **Käideldavus** on teabe, IT-süsteemide, inimeste, protsesside omadus olla volitatud olemi nõudel kättesaadav ja kasutuskõlblik.
2.13. **Nõrkus** on infovara, meetme või protsessi haavatav osa, nõrk koht (turvalisuse puudus), mille saab ära kasutada nii, et toimub negatiivse tagajärjega sündmus. Nõrkuse saab ära kasutada üks või mitu ohtu.
2.14. **Oht** on sündmus või asjaolu, mis omab potentsiaali nõrkuse ärakasutamiseks ja seeläbi riski realiseerumise põhjustamiseks. Süsteemi või asutust kahjustada võiva soovimatu intsidendi potentsiaalne põhjus (sündmus või asjaolu, mis on võimeline nõrkust ära kasutama).
2.15. **Klient** selle korra tähenduses on asutus, kellele SMIT osutab info- ja kommunikatsioonitehnoloogia (IKT) teenust. Klienti esindab vastava teenuse **peakasutaja**.
2.16. **Risk** on määramatuse toime eesmärkidele. Toime on positiivne või negatiivne hälve oodatavast. Infoturvariskid on harilikult seotud määramatuse negatiivse toimega infoturvaeesmärkidele.. Riskid tehakse kindlaks ja hinnatakse riskikontrolli käigus ning hoitakse ohjes riskihalduse abil.
2.17. **Terviklus** on andmete õigsus ja täielikkus, lubamatute muudatuste puudumine, hõlmab ka autentsust ja salgamatust kogu andmete elutsükli jooksul.
2.18. **Tooteomanik** on SMITi teenuste portfellis määratud IKT teenuse ja/või toote omanik.
2.19. **Turvaintsident** on infoturvasündmus, mis võib kahjustada SMITi toimepidevust ja infovara ning ohustada teabe turvalisust.
2.20. **Vastutav töötleja** on juriidiline isik, kes määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid, st otsustab, miks ja kuidas isikuandmeid töödeldakse. Vastutav töötleja vastutab selle eest, et andmete töötlemine toimuks kooskõlas isikuandmete kaitse üldmääruse (GDPR) ja õigusaktidega. SMITi vaates on vastutav töötleja enamasti klient.
2.21. **Volitatud töötleja** töötleb isikuandmeid vastutava töötleja nimel ning ainult vastutava töötleja dokumenteeritud juhiste alusel, vastava lepingu või õigusakti alusel. Volitatud töötleja ei või isikuandmete töötlemise eesmärke ega vahendeid iseseisvalt määrata ning on kohustatud tagama andmete töötlemisel turvalisuse ja vastavuse kehtivatele andmekaitsenõuetele,, nt Siseministeeriumi valitsemisala kontekstis SMIT.
2.22. **Väline partner** on SMITile teenuseid osutava lepingu alusel tegutseva organisatsiooni (lepingupartneri või tarnija) volitatud esindaja, kes teostab SMITile lepingulisi töid ning vajab selleks ligipääsu SMITi hallatavale infovarale (sealhulgas infosüsteemidele, andmetele või füüsilisele infrastruktuurile), vastavalt kokkulepitud tingimustele ja juurdepääsuõigustele.

3. Rollid ja kohustused

3.1. Infoturbe tagamisel, järelevalvetoimingute tegemisel ja teenuste haldamisel rakendatakse kohustuste lahususe põhimõtet, mis tagab, et erinevad ülesanded ja volitused on jaotatud nii, et vähendada võimalikke riske ja konflikte ning tagada turvalisus ja läbipaistvus.
3.2. Infoturbekorra rakendamise ja infoturbe halduse süsteemi käitamise eest vastutab SMITi peadirektor, keda toetavad ja nõustavad struktuuriüksuste juhid (peadirektori asetäitja äriteenuste valdkonnas, peadirektori asetäitja baasteenuste valdkonnas, peadirektori asetäitja inimeste ja kultuuri valdkonnas, strateegiajuht, õiguse ja hangete osakonna juht ning finantsosakonna juht).
3.3. Peadirektor koostöös struktuuriüksuste juhtidega tagab infoturbe halduse süsteemi vastavuse SMITi strateegilistele eesmärkidele, integreerimise äriprotsessidesse, poliitika kujundamise ja formuleerimise ning ressursside olemasolu.

3.4. Peadirektori asetäitjad vastutavad enda valdkonna infoturbe halduse süsteemi toimivuse eest.
3.5. Infoturbejuht vastutab infoturbe halduse süsteemi SMITis rakendatavale infoturbe standardile vastavuse tagamise eest ja teavitab peadirektorit infoturbe tegevustest ja tulemustest. Infoturbejuht SMITis on infoturbeosakonna juhataja, kelle õigused, kohustused ja vastutus on sätestatud Siseministeeriumi valitsemisala infoturvapoliitikas, infoturbeosakonna põhimääruses, tema töölepingus ning teistes dokumentides.
3.6. Riskijuht vastutab SMITi riskihalduse poliitika evitamise, riskide hindamise korraldamise ja iga-aastase ülevaatamise ning ISMSi rakendamise üldise koordineerimise, dokumentide halduse ja infoturbe halduse süsteemi parendusmeetmete täitmise jälgimise eest.
3.7. Siseaudiitor teostab infoturbe halduse süsteemi toimimise ülevaatust üks kord aastas, kaasates vajadusel sisemisi ja välised eksperte.
3.8. Üldine infoturbealane vastutus on igal töötajal. Töötaja peab täitma infoturbe nõudeid, infoturbejuhi korraldusi ning on kohustatud teavitama infoturbeosakonda avastatud turvaintsidentidest, -nõrkusest, potentsiaalsest turvasündmusest või muust turvaohust asutusele või osutatavatele teenustele või nende kahtlusest.
3.9. Teenuste infoturbealane vastutus oma teenuste piires on struktuuriüksuse või osakonna juhil, kes korraldab, vastutab ja teostab järelevalvet korrast ning teenuse ja selles käideldavate andmete spetsiifikast tulenevate nõuete rakendamise eest oma vastutusvaldkonnas. Struktuuriüksuse või osakonna juhil on õigus võtta vastu otsuseid oma teenuste ning nende liidestuste osas, et tagada teenuste ja seal töödeldavate andmete turvalisus vastavalt infoturbealastele nõuetele. Teenuste ja protsesside konkreetsed infoturbealased nõuded on kirjeldatud WIKI infoturbejuhendites ja põhiprotsessis.
3.10. Struktuuriüksuse või osakonna juht teostab järelevalvet juurdepääsude ning teenustes töödeldavate andmete kasutamise üle, sealhulgas teenuste testimiseks kasutatavate andmete ning lisakeskkondade loomise üle. Andmete volitatud töötlejana kooskõlastab ta andmete ja teenuse keskkondades / infovarades, sh andmetes tehtavaid muudatusi ja nõudeid andmete vastutava töötlejaga (Service Deskis või lepingus sätestatud tingimustel).
3.11. Struktuuriüksuse või osakonna juht võib punktis 3.9 ja 3.10 kirjeldatud õigused, kohustused ja vastutuse delegeerida, näiteks tooteomanikele, arhitektidele jne.
3.12. Tooteomanik vastutab õigusnormidest ja lepingutest tulenevate teenusele kehtivate nõuete rakendamise eest. Teenus- ja tarnelepingud peavad sisaldama ka teenust või toodet mõjutavatest turvanõrkustest, andmeleketest, rünnetest ja muudest ohtudest, juhtumitest ja intsidentidest teavitamise kohustust ja korda.
3.13. Kliendil või tema volitatud isikul on õigus kontrollida kokku lepitud nõuete täitmist ja teenuse talitluspidevust (nt kas teenuse talitluspidevuse plaan on koostatud, testitud, logide olemasolu ja säilitamine jne), seejuures ka nõuete ja vastutuste täitmist (nt keskne logihaldus, arendusnõuded, talitluspidevuse nõuete täitmine, infoturbe korra täitmine jne).
3.14. Tooteomaniku kohustus on tagada teenuse talitluspidevus vastavalt kokkulepitud käideldavuse, konfidentsiaalsuse ja tervikluse tasemetele, korraldada rikete ja turva-nõrkuste tähtaegne likvideerimine. Riskide aktsepteerimine ja maandamine muul viisil peab olema põhjendatud ja proportsionaalne ning vastama riskihalduse poliitika nõuetele.
3.15. Keskse infoturbe vastutused ja üldised teenuseülesed turvanõuded töötab välja infoturbeosakond.

Vaata lisaks: Infoturbeosakonna põhimäärus, ISO 27001 infoturbe juhtimise käsiraamat, Nõuded talitluspidevuse tagamise korraldamisele, Põhiprotsess, Riskihalduse poliitika, Siseministeeriumi valitsemisala infoturvapoliitika

4. Personali turve

4.1. Kõigi töökohakandidaatide, praktikale kandideerivate ja SMITile teenust osutavate väliste partnerite, tausta kontrollitakse. Tausta kontrollimisel järgitakse õigusaktidest tulenevaid reegleid. Kõiki, kellelt oodatakse taustakontrolli läbimist, teavitatakse taustakontrolli teostamisest. Taustakontrolli teostamise aluseks on nõusolekuankeedi täitmine. Taustakontrolli teostab Politsei- ja piirivalveamet politsei ja piirivalve seaduse alusel.
4.2. Infoturbe reeglite kohaldamist personali värbamisel korraldab personaliosakond ja kooskõlastab need SMITi infoturbejuhiga.
4.3. Töölepingu sõlmimise eelduseks on edukas taustakontrolli läbimine ja tutvumine korraga. Enne taustakontrolli tulemuse selgumist lepingu sõlmimine või välise partneri lepingu täitmisele lubamine on keelatud.
4.4. Infoturbealaste teadmiste täiendamiseks ja süvendamiseks korraldatakse vastavalt vajadusele turbealaseid koolitusi ning õppusi ja toimub töötajate infoturbealane juhendamine. Igal töötajal on vähemalt üks kord aastas kohustus läbida infoturbekoolitus, uuel töötajal on kohustus see läbida katseaja jooksul.
4.5. Personali operatiivne turbeteavitus toimub e-posti, siseveebi, mobiiltelefoni ja/või sõnumiteenuse vahendusel.

Vaata lisaks: Väliste partnerite taustakontroll ja juurdepääsuõiguste taotlemine

5. Andmekandjate käsitlemine

5.1. Andmekandjad tuleb märgistada ja hoida viisil, mis tagab vajadusel nende asukoha tuvastamise ja kasutamise töötaja asendaja või muu volitatud isiku poolt.
5.2. Konfidentsiaalseid andmeid tuleb digitaalsetel andmekandjatel hoida märgistatult, lukustatud kapis tööruumides ja krüpteeritult.
5.3. SMITi kasutuses olnud ja mittevajalikuks muutunud ning säilitamisele mittekuuluvad andmekandjad tuleb hävitada kehtivate kordade kohaselt.
5.4. Andmekandjate hävitamise või taaskasutamise korral hindab kasutaja ja/või omanik koos andmete vastutava töötlejaga andmekandjal olevate andmete säilitamise või hävitamise vajalikkust.
5.5. Andmete varundamist ja taastamist reguleerib kehtiv peadirektori kinnitatud kord „Nõuded talitluspidevuse tagamise korraldamisele“.
5.6. Igasuguse SMITi poolt väljastatud andmekandja või seadme kadumisest või vargusest või kolmanda osapoole võimalikust ligipääsust selle andmetele tuleb viivitamatult teavitada kliendituge.
5.7. Tööalaste andmete töötlemiseks, sh säilitamiseks ja transpordiks tohib kasutada vaid SMITi poolt väljastatud irdandmekandjaid.
5.8. SMITis kasutatav irdandmekandja peab toetama riistvaralist krüpteeringut, olema sisestatud ja arvele võetud vara haldamise ja arvestuse korra nõuete kohaselt ning vormistatud kasutaja vastutusele.
5.9. Tööülesannete täitmiseks vajalikku irdandmekandjat, mis ei ole SMITi poolt väljastatud, ei tohi ühendada SMITi väljastatud keskhalduses oleva seadme külge. Selliselt irdandmekandjalt andmete kätte saamiseks tuleb kasutada irdmeediakioskit või anda seade SMITi IT-tehnikule, kes võtab sealt andmed välja.
5.10. SMITi väljastatud irdandmekandjad ja välised andmekandjad, mis on vahepeal ühendatud valitsusalavälisesse seadmesse, tuleb enne SMITi arvuti külge ühendamist kontrollida irdmeediakioskis või anda SMITi IT-tehnikule kontrollimiseks.
5.11. Irdandmekandjat tohib kasutada vastutava töötleja nõusolekul vaid andmete kriisiolukorras taastamiseks või transportimiseks, kuid ei tohi kasutada IKT teenuses / andmekogus olevate

andmete alaliseks säilitamiseks. Volitatud töötlejana säilitab SMIT teenuste/andmekogu andmeid andmekeskustes ja varundab vastutava töötlejaga kokkulepitud nõuete ja kehtivate kordade kohaselt. Vastavad toimingud ja kokkulepped vastutava ja volitatud töötleja vahel on dokumenteeritud teenuste portfellis.

Vaata lisaks: Vara haldamise ja arvestuse kord, Dokumentide liigitusskeem, Nõuded talitluspidevuse tagamise korraldamisele, Teenuste portfell

6. Infovarale juurdepääsu reguleerimine

6.1. Töötajal ja välisel partneril võib olla juurdepääs ainult sellele teabele, andmekogule, võrgule ja neile võrguteenustele, mida tal on tööülesanneteks vaja kasutada.
6.2. Igale töötajale ja vajadusel välisele partnerile võimaldatakse kahefaktorilist autentimist toetavad tehnilised töövahendid ja tagatakse tööülesannete täitmiseks vajalikud juurdepääsuõigused infovaradele elektrooniliste juurdepääsude haldamise korra alusel ning eeldusel, et:
  6.2.1. ta on tutvunud selle korraga ja kohustub seda järgima;
  6.2.2. tal on tööülesannetest tulenevalt vastavate andmete töötlemiseks vajalik juurdepääsuluba (nt juurdepääsuõiguse andmine on kooskõlastatud andmete vastutava töötlejaga) ja põhjendatud teadmisvajadus.
6.3. Igal töötajal ja vajadusel välisel partneril peab olema SMITi aktsepteeritud kahefaktorilise autentimise võimekus.
6.4. Infoturbeosakond kooskõlastab privilegeeritud juurdepääsuõiguste andmise ja teostab selle üle tehnilist järelevalvet.

Vaata lisaks: Elektrooniliste juurdepääsude haldamise kord

7. Füüsilise keskkonna turve

7.1. Füüsilise keskkonna turve hõlmab SMITi varade ning kõigi SMITile kuuluvate või majutamiseks antud infovarade füüsilist turvet tagavate protsesside haldamist.
7.2. Füüsilise keskkonna turvet, sealhulgas kohalduvate turbenõuete rakendamist korraldab haldusosakonna juhataja ja kooskõlastab need SMITi infoturbejuhiga.
7.3. Juurdepääs SMITi varale on lubatud ainult tööülesannete täitmiseks.
7.4. Lepingupartnerite või klientide juures asuvatele SMITi töökohtadele ja hoitavatele SMITi varadele rakenduvad lisaks SMITiga kirjalikult kokku lepitud turvanõuetele täiendavalt ka partnerite või klientide füüsilise turbe meetmed.
7.5. IKT-vahendite paigutamisel ja kasutamisel tuleb silmas pidada, et neid ei oleks võimalik volitamata kasutada ning teisaldada, sh näha neis sisalduvat teavet ja volitamata kasutada seal olevaid andmeid.
7.6. Kasutaja peab välistama kõrvaliste isikute ligipääsu infovarale.
7.7. Väljaspool Siseministeeriumi valitsemisala asutuste asukohti ei ole töötajal lubatud jätta talle kasutamiseks antud IKT-vahendeid järelevalveta lukustamata ruumidesse või avalikesse kohtadesse, mis võiksid soodustada nende vargust, hävimist või muul moel ärakasutamist.
7.8. Füüsilise turbe nõuetest tulenevaid meetmeid rakendatakse vastavalt hoonete ja ruumide turbevajadusele, arvestades kaitstavate varade väärtust.

Vaata lisaks: Arvutitöökoha kasutamise kord, Mobiilseadmete ja -teenuste kasutamise ja kulude katmise kord, Serveri- ja seadmeruumide kasutamise kord, SMITi ruumidele ligipääsu kord, SMITi töökorralduse reeglid, Välismaal töötamise ja/või SMITi töövahenditega välispiiri ületamise juhend

8. Taristu haldamine ja võrguturve

8.1. Kasutusel oleval riistvaral ja kommertslitsentsiga kaetud tarkvaral peab olema tootja tugi, erandiks on spetsiifiline tarkvara vältimatu vajaduse ning kaalutud riski olukorras. Seda hindab infoturbeosakond tooteomaniku selgituste põhjal. Olukorras, kus taakvara pole võimalik välja vahetada, vastutab taakvara turbe ja sellega kaasnevate riskide eest vastava struktuuriüksuse juht.
8.2. SMITis kasutatava riist- ja tarkvara tehnilist dokumentatsiooni tuleb kaitsta volitamata juurdepääsu eest, erandid tuleb kooskõlastada infoturbeosakonnaga.
8.3. SMITi andmesidevõrk peab olema üles ehitatud selliselt, et erinevad kasutajasegmendid on loogiliselt üksteisest eraldatud.
8.4. Segmentide vaheliseks andmesideks peab kasutama minimaalset ühenduste arvu ja segmentide vaheline andmeside peab võimalusel läbima tulemüüri ja olema krüpteeritud.
8.5. Kõik SMITi andmesidevõrku ühendatud seadmed peavad olema tuvastatavad ja omama vastavat võrgusertifikaati (IEEE 802.1x).
8.6. Avaliku võrgu kaudu sisevõrgu ressursside poole pöördumine ja konfidentsiaalsete andmete välisvõrgus edastamine on lubatud vaid turvalise virtuaalse privaatvõrgu (VPN) kaudu. VPN-tarkvara peab olema konfigureeritud selliselt, et ühenduse loomiseks on vaja vähemalt kahefaktorilist autentimist. Erandid tuleb kooskõlastada infoturbe-osakonnaga.

Vaata lisaks: Tarkvara haldamise kord, Võrguhalduse kord

9. Töökohtade standardkonfiguratsioon

9.1. SMITi arvutitöökohad on reeglina standardkonfiguratsiooniga ning neid hallatakse keskselt. SMITi töötajatel ei ole lubatud muuta kasutatavate seadmete turvaseadistusi või konfiguratsiooni, sh katkestada seadmes automaatselt käivitatud protsesse (nt pahavaratõrje, lõppseadme kaitse lahendus jne).
9.2. Standardkonfiguratsiooniga arvutitöökohtade tarkvara konfiguratsiooni, kasutatava tarkvara ja selle ajakohastamise üle otsustab ning selle eest vastutab töökohateenuste osakond.
9.3. Tarkvaraprofiili täiendamise otsused võtab vastu töökohateenuste osakond, hinnates lisatava tarkvara vajadust, litsentseerimistingimusi, keskset hallatavust, turvapaikamise võimalust, alternatiivide olemasolu tarkvaraprofiilis jmt. Uue tarkvara kasutuselevõtu eelduseks on infoturbeosakonna kooskõlastus.
9.4. Standardkonfiguratsioonist erinevat arvutitöökoha konfiguratsiooni on lubatud kasutada erandina, kui vajadus tuleneb tööülesannetest ja on kooskõlastatud infoturbeosakonnaga.
9.5. Standardkonfiguratsioonist erineva arvuti kasutamise puhul vastutab arvuti kasutaja, et seadmes on rakendatud infoturbe tagamiseks ette nähtud meetmed, mida rakendatakse ka standardkonfiguratsiooniga arvutitöökohtade puhul ning et on tagatud korra nõuded. Seadmes olevate andmete töötlemise, seadme ja andmete turvalisuse ning seadme töökorras olemise, konfigureerimise ja turvapaikamise eest vastutab täielikult seadme kasutaja.

Vaata lisaks: Arvutitöökoha kasutamise kord, Tarkvara haldamise kord

10. Infovara turve

10.1. Tööülesannete täitmiseks on SMITi arvutitesse lubatud paigaldada ainult selleks volitatud tarkvara. Volitatud tarkvara nimekiri ja juhised soovitud tarkvara kooskõlastamiseks on kirjeldatud tarkvarakataloogis.

10.2. Töötajatel ei ole lubatud salvestada ja printida tööalaseks kasutamiseks mõeldud teavet SMITi poolt mittehallatavatesse infosüsteemidesse ja seadmetesse, välja arvatud juhul kui see tuleneb seadusandlusest.
10.3. Töötajatel ei ole lubatud väärkasutada infosüsteemide iseärasusi või (tarkvaralisi ega riistvaralisi) lisavahendeid, et saada privilegeeritud ligipääsuõigusi või häirida infosüsteemide tööd.
10.4. Vastavasisulise teate korral peab kasutaja süsteemiuuenduste laadimiseks taaskäivitama seadme. Selle eiramisel võib seade taaskäivituse ise sooritada. Lubatud on taaskäivitust mõistlikuks ajaks edasi lükata, et lõpetada teavituse hetkel pooleliolevad tööd.
10.5. Pahavara puudutava hoiatuse ekraanile ilmudes peab kasutaja viivitamatult teavitama SMITi kliendituge ja ootama klienditoelt/infoturbeosakonnalt edasisi juhtnööre vajalike toimingute teostamiseks. Enne seda on keelatud igasugune tegevus, muu hulgas iseseisvalt pahavara eemaldamine.
10.6. SMITi töötaja ei tohi omavoliliselt SMITi võrku edasi jagada SMITivälistele kasutajatele, kasutades sealhulgas nt Bluetoothi, 4G-d, WiFi-t jms.
10.7. Bluetooth lisaseadmete kasutamine SMITi arvutites ja telefonides on asutusesiseseks kasutamiseks mõeldud teabe töötlemiseks keelatud, v.a arvutihiired. Kõrvaklappe ja mikrofone on asutusesiseseks kasutamiseks mõeldud teabe töötlemiseks lubatud kasutada ainult kaabliga ühenduses ning Bluetooth ühendus peab olema sellistel seadmetel välja lülitatud. Bluetooth kõrvaklappe on lubatud kasutada, kui seal ei töödelda asutusesisest teavet (näiteks kuulatakse taskuhäälingut või muusikat).
10.8. Siseministeeriumi valitsemisala arvutivõrku (v.a SMITi avalik WiFi võrk) ei ole lubatud ühendada isiklikke seadmeid ilma SMITi VPN-lahenduseta.
10.9. SMITi seadmeid on keelatud ühendada USB-kaabli abil avalike laadimispunktidega (nt lennujaamades jne). Kasutaja tohib ühendada SMITi seadmega üksnes järgmisi isiklikke seadmeid: monitor, klaviatuur, hiir, dokkimisjaam, turvatud ruuter, SMITi keskselt hallatav mobiilne seade.
10.10. SMITi seadmega välismaale mineku (ükskõik millisel põhjusel) ja välismaalt kaugtöö tegemise reeglites lepivad kokku töötaja ja tema töölepingus märgitud juht, järgides seda korda ning koostöökokkuleppeid, mis on kirjeldatud SMITi töövahendite välismaal kasutamise korras.

Vaata lisaks: Tarkvara haldamise kord, Arvutitöökoha kasutamise kord, Mobiilseadmete ja -teenuste kasutamise ja kulude katmise kord, SMITi töövahendite välismaal kasutamise kord

11. **E-post ja kiirsõnumivahetus**

11.1. Kogu e-posti liiklus SMITi võrgust või SMITi võrku peab läbima SMITi hallatava e-posti serverit. Tööülesannetega seotud elektrooniliseks kirjavahetuseks võib kasutada ainult SMITi hallatavat e-posti aadressi.
11.2. Tööülesannetega mitteseotud kirjavahetus (näiteks palgateatised, töötajate ja tiimide omavaheline suhtlus töövälise kokkusaamise kokkuleppimiseks) peab olema selgelt eristatud, näiteks kausta pealkirjaga „Isiklik".
11.3. Töötaja on kohustatud kontrollima e-kirja saatmisel adressaatide õigsust.
11.4. Töötaja on kohustatud veenduma, et saadetav sõnum ei sisaldaks adressaatidele mittevajalikku teavet ning jälgima, et teave, mille kohta kehtib juurdepääsupiirang, ei satuks juurdepääsuõiguseta isikute kätte.
11.5. Väljaspoole Siseministeeriumi valitsemisala elektrooniliselt saadetava asutusesiseseks kasutamiseks liigitatud teabe peab töötaja krüpteerima või muul viisil volitamata töötlemise eest kaitsma.

11.6. Töötaja peab veenduma e-postiga saabunud viidete ja failide ohutuses sõltumata saatja isikust enne nende avamist. Kahtluse tekkimisel tuleb edastada kiri aadressile spam@smit.ee. Faile saab kontrollida failide turvakontrolli süsteemiga või saates failid ja/või failijagamiskeskkondade lingid aadressile failikontroll@smit.ee. Kontrollitud failid saab alla laadida vastavast keskkonnast. Pahavara sisaldavale lingile, manusele vms klõpsamise puhul tuleb viivitamatult teavitada kliendituge.

11.7. Töötaja poolt välisvõrku saadetud kirjad peavad sisaldama saatja pärisnime.

11.8. Osakonna või struktuuriüksuse meililisti omanik on vastava üksuse juht või juhi poolt delegeeritud töötaja. Meililisti omanikul on kohustus hoida meililisti e-posti adressaate ajakohasena ning esitada meililisti vajalikkuse kadumisel klienditoele meililisti kustutamise taotlus. Meililisti omanikul on lubatud määrata meililistidesse ainult Siseministeeriumi valitsemisala e-posti aadresse.

11.9. Asutusesiseseks kasutamiseks mõeldud teabe vahetamiseks ei tohi kasutada isiklikku e-posti ega isiklikke kiirsuhtlusrakendusi. Kogu tööalane teabevahetus peab toimuma ainult asutuse ametlike ja turvaliste kanalite kaudu.

11.10. Faili- ja kiirsõnumivahetuseks tohib tööalase teabe edastamisel kasutada SMITi poolt lubatud rakendusi, mis on leitavad tarkvarakataloogis.

Vaata lisaks: Töökorralduse reeglid, Tarkvara haldamise kord

12. **Süsteemide hankimine, väljatöötamine ja hooldus**

12.1. Vajalikud turvameetmed infovarale peab rakendama infovara omanik infoturbeosakonna kehtestatud nõuete ning kehtivate kordade ja õigusnormide kohaselt.

12.2. Struktuuriüksused peavad tuvastama oma infovarad, need nõuetekohaselt dokumenteerima, määrama nende turbeastme (turvaklassi) ja omaniku. Tooteomanik peab dokumenteerima oma teenused teenuste portfellis ja hoidma need ajakohasena. Kirjeldada tuleb muu hulgas teenuse osutamiseks vajalikud infovarad, keskkonnad, talitluspidevuse nõuded, teenused, millest sõltutakse, ja mõju teistele teenustele.

12.3. Teenuses töödeldavate andmete turbeastme määrab klienti esindav peakasutaja, kes peab eelnevalt hindama andmete tähtsust ning andmete turvalisuse puudumisest tulenevaid kahjusid.

12.4. Andmekogu andmete korral peab turbeastme ja turvaklassi määrama andmekogu vastutav töötleja.

12.5. Turbeaste ja turvaklass määratakse Vabariigi Valitsuse 13. detsembri 2022. aasta määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 7–10 alusel (https://www.riigiteataja.ee/akt/113122022030).

12.6. SMITi teenuste planeerimisel tuleb järgida arendusnõudeid (IKT arendusprotsess) ning arenduse ja turvalisuse häid tavasid.

12.7. Teenustes tehtavaid muudatusi peab tooteomanik enne muudatuste rakendamist põhjalikult analüüsima infoturbe seisukohast, hindama muudatusega seotud riske, kooskõlastama kliendi ja infoturbeosakonnaga. Muutunud nõuete ja/või tekkinud ohtude korral tuleb üle vaadata võimalikud muutused käideldavuse, konfidentsiaalsuse ja tervikluse osaklassides ning vajadusel muuta turvameetmeid. Muudatused peavad kajastuma teenuste portfellis.

12.8. Kui teenusega seotud rakenduses tuvastatakse turvanõrkus, peab tooteomanik või muu rakenduse eest vastutav isik teavitama sellest infoturbeosakonda ja klienti ning kõrvaldama turvanõrkuse nõuete kohaselt. Infoturbeosakond kontrollib ja koordineerib turvanõrkuste kõrvaldamist ja vajadusel edastab teabe tuvastatud turvanõrkuse kohta IKT teenuse omanikule.

12.9. SMITi ülesannete täitmisel töödeldavad andmed peavad olema otstarbekohased, usaldusväärsed ja terviklikud, kooskõlas kliendi / vastutava töötleja nõuetega. Andmete vajaduseta kopeerimist ja koopiate arvu suurendamist tuleb vältida. Juhul kui koopia tegemine on mõõdapääsmatu, tuleb selleks järgida SMITi erakorraliste koopiate tegemise ning haldamise korda.

12.10. Pilveteenuste omandamise, kasutamise, haldamise ja neist väljumise protsessid peavad vastama infoturbeosakonna kehtestatud nõuetele ning kehtivatele kordadele ja õigusnormidele. Võrgu- ja infosüsteemi turvameetmete nõudeid ja nende kohaldamise ulatust pilveteenuse kasutamisel reguleerib Vabariigi Valitsuse 03.01.2024 määrus nr 1 (https://www.riigiteataja.ee/akt/109012024025). Pilveteenuste kaudu saadetava asutuse-siseseks kasutamiseks liigitatud teabe peab töötaja krüpteerima või muul viisil volitamata töötlemise eest kaitsma.

12.11. Teenuse ja infovara kasutajad ja nende tehtavad toimingud peavad olema üheselt tuvastatavad ja logitud.

12.12. Arendus-, testimis- ja käituskeskkonnad peavad olema üksteisest lahus.

Vaata lisaks: IKT arendusprotsess, IKT teenuste üldtingimused, Muudatusehalduse kord, Nõuded talitluspidevuse tagamise korraldamisele, Põhiprotsess, SMITi erakorraliste koopiate tegemise ning haldamise kord, Siseministeeriumi valitsemisala infosüsteemide turvatestimise, turvanõrkuste haldamise ning logimise nõuete kord, Teenuste portfell

13. **Välised partnerid**

13.1. Kõigi väliste partnerite suhtes viiakse läbi taustakontroll.

13.2. Struktuuriüksuse või osakonna juht, kelle vastutusalas toimub välise partneri tegevus, korraldab välise partneri tegevust ja tagab selle vastavuse kordadega.

13.3. Välisele partnerile kehtivad korrad ja nõuded lisatakse hanke alusdokumentidesse.

13.4. SMITi keskkondadesse ühendamiseks kasutab väline partner kas SMITi tööjaama või isiklikku seadet. SMITi tööjaama kasutamine on kohustuslik haldustoimingute teostamisel, mille raames väljastatakse ka vajalikud haldusligipääsud (privilegeeritud kasutaja konto), erandid tuleb kooskõlastada infoturbeosakonnaga.

13.5. SMITi tööjaamaga välismaale mineku ja välismaalt kaugtöö tegemise korral peab väline partner järgima SMITi töövahendite välismaal kasutamise korda.

13.6. Väline partner peab olema teadlik turbenõuete süülise rikkumise tagajärgedest. Turbenõuete ja -põhimõtete rikkumise korral võib välisele partnerile kohaldada sanktsioone, sh nõuda tema poolt tekitatud kahju hüvitamist vastavalt lepingus sätestatule.

13.7. Väline partner on kohustatud teavitama struktuuriüksuse või osakonna juhti, kelle vastutusalas toimub välise partneri tegevus, avastatud turvanõrkusest, potentsiaalsest turbesündmusest või muust turbeohust.

Vaata lisaks: Väliste partnerite taustakontrolli ja juurdepääsuõiguste taotlemise juhend, SMITi töövahendite välismaal kasutamise kord

14. **Turvaintsidentide haldus**

14.1. Kasutajaga seotud infosüsteemi kasutamisandmeid kogutakse eesmärgiga tuvastada selles korras ja muudes infoturvet reguleerivates õigusaktides sätestatud keelatud tegevused (nt sündmused, intsidendid).

14.2. Infosüsteemi ja võrgu kasutamisandmete kogumine on automatiseeritud ning andmete töötlemine võib olla nii automaatne kui ka manuaalne.

14.3. SMITi infoturbeosakonnal on õigus dekrüpteerida, inspekteerida, jälgida ja salvestada kogu andmeside liiklust või suunata seda läbi vastavate kontrollmehhanismide, tagamaks teabe kaitse lähtudes korra punktis 14.1 sätestatud eesmärgist.

14.4. SMITi infoturbeosakonnal ja klienditoel on intsidendi lahendamiseks õigus tuvastada kasutajale antud seadmete füüsiline asukoht, sealhulgas kasutades seadme GPS-liidest.

14.5. SMITi infoturbeosakond on kohustatud registreerima tuvastatud turvasündmused ja/või -intsidendid, koordineerima nende lahendamist ning abistama toote/teenuse meeskonda, klienditoe osakonda ja/või kliente nende lahendamisel. Turvakaalutlustel on SMITi infoturbeosakonnal õigus piirata ligipääsu turvasündmustele ja -intsidentidele.

14.6. Kasutaja peab turvaintsidendist viivitamatult teavitama SMITi kliendituge ja/või infoturbeosakonda.

14.7. Kasutaja on kohustatud igakülgselt kaasa aitama intsidendi uurimisele ja lahendamisele, tagades selleks vajaliku juurdepääsu Siseministeeriumi valitsemisala poolt väljastatud seadmetele ning andes intsidenti uuriva struktuuriüksuse või osakonna nõudel suulisi või kirjalikke selgitusi.

14.8. SMITi infoturbeosakonnal on õigus peatada osaliselt või täielikult üksikute tööjaamade või rakenduste võrguliiklus või kasutamine, teavitades kasutajat keelatud tegevusest või toimunud turvaintsidendist ja juhendada kasutajat edasistes tegevustes turvaintsidentide vältimiseks. Samuti on SMITi infoturbeosakonnal õigus turvaintsidendi eskaleerumise takistamiseks kasutajale antud IKT-vahendite sisu täielikult kustutada.

Vaata lisaks: Turvaintsidentide menetlemise juhend

15. **Konfidentsiaalsuskohustuse nõue**

15.1. Konfidentsiaalsuskohustuse nõue kehtib konfidentsiaalse teabe kohta ja on sõltumatu isikute ametiseisundist või füüsilisest töökohast ning kohaldub ka neile töötajatele, kellel puuduvad otsesed infovara kasutamise volitused.

15.2. SMITi jaoks on konfidentsiaalne teave, mille avaldamine või volitamata kättesaamine võib kahjustada SMITi toimimist, julgeolekut või muid olulisi huve, näiteks, kuid mitte ainult:

- 15.2.1. sisemised dokumendid ja aruanded, mis ei ole avalikud;
- 15.2.2. lepingud, mis sisaldavad ärisaladusi või tundlikku infot ja ei ole avalikud;
- 15.2.3. andmed SMITi infosüsteemide ja tehniliste lahenduste kohta, mis võivad olla sihtmärgiks küberrünnakutele;
- 15.2.4. isikuandmed ja muud andmed, mille avalikustamine rikub privaatsust või seadust;
- 15.2.5. riigisaladus;
- 15.2.6. füüsilised turvameetmed;
- 15.2.7. privilegeeritud õigused ja nende kasutajad;
- 15.2.8. riigikaitselised töökohad.

15.3. Töötaja, kes puutub tööülesannete täitmisel või töö käigus juhuslikult kokku konfidentsiaalsete andmetega, kohustub:

- 15.3.1. mitte avalikustama ega edastama kolmandatele osapooltele temale teatavaks saanud konfidentsiaalset teavet, välja arvatud õigusaktides sätestatud juhtudel;
- 15.3.2. järgima kehtivaid andmekaitset puudutavaid õigusakte ja kordasid;
- 15.3.3. täitma konfidentsiaalsuskohustuse nõudeid nii töösuhte ajal kui ka peale selle lõppemist õigusaktides sätestatud ulatuses.

15.4. Kui isik teostab töid võlaõigusliku lepingu alusel, peavad lepingu konfidentsiaalsussätted sisaldama korra punktis 15.3 sätestatud põhimõtteid.

Vaata lisaks: Töökorralduse reeglid