LISA nr 1
KINNITATUD
Peadirektori KK nr 1-1/25

Siseministeeriumi infotehnoloogia- ja arenduskeskuse infoturbe kord

Hea smitikas ja väline partner!

Oled liitunud Eesti riigi suurima IT-majaga. Kui oled uus töötaja, aitab infoturbe kord Sul paremini mõista SMITis kehtivaid turvameetmeid ja teha oma tööd viisil, mis ei ohusta SMITi infovara ega töötajate turvalisust. Ka siis, kui oled juba ammu meie tiimi liige, saad lugedes mälu värskendada ja leida vastuseid tekkinud küsimustele. Alati saad täpsemalt juurde küsida infoturbeosakonnast aadressil sec@smit.ee. Kasulikku teavet leiad ka infoturbepesast https://portaal.smit.sise/sites/infoturbepesa.

Sisukord

1. Üldsätted

1.1. Käesolev 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 ning valdkonna parimast praktikast ning on kooskõlas SMITis rakendatava 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. Need on reguleeritud kohalduvate õigusnormide, SMITi riigisaladuse ja salastatud välisteabe kaitse juhendi jt asjaomaste juhistega.
1.5. Kord kohaldub SMITi töötajatele, praktikantidele, välistele partneritele ning nende protsessidele, protseduuridele ja tegevustele.
1.6. Korras sätestatud turbenõuete ja -põhimõtete rikkumist loetakse töökohustuse või lepingu rikkumiseks. Korduva infoturbe korra või muu sisemise korra rikkumise puhul võib infoturbeosakond seada infosüsteemide kasutamise õiguse taastamise 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 selgelt piiritletud ja põhjendatud.
1.8. Infoturbe korra ning teiste infoturbeosakonna vastutusala kordade iga-aastase ülevaatamise ja vajadusel ajakohastamise korraldab 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 süstemaatiline lähenemine ärieesmärkide saavutamiseks vajaliku infoturbe rajamisele, evitamisele, käigus hoidmisele, seirele, läbivaatusele, hooldamisele ja täiustamisele.
2.4. **Infoturve** on turvameetmete loomise, valimise ja rakendamise protsesside kogum, aga ka teabe konfidentsiaalsuse, tervikluse ja käideldavuse säilitamine.
2.5. **Infovara** on teave, andmed ja nende töötlemiseks vajalikud infotehnoloogilised rakendused ning tehnilised vahendid.
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 turvameetmeteks 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 muu hulgas USB-pulgad, välised kõvakettad, CD-d, DVD-d, magnetlindid, mälukaardid, mälupulgad, fotoaparaadid jms.
2.9. **Kohustuste lahusus** on tööprotsessi sammude jaotamine inimestele nii, et toimingu kontrollija või sanktsioneerija 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, üks teabe turvalisuse kolmest põhikomponendist.
2.12. **Käideldavus** on teabe, IT-süsteemide, inimeste, protsesside omadus olla volitatud olemi nõudel kättesaadav ja kasutuskõlblik, üks teabe turvalisuse kolmest põhikomponendist.
2.13. **Nõrkus** on vara, meetme või protsessi haavatav osa, nõrk koht (turvalisuse puudus), mille ära kasutamine võib põhjustada riski realiseerumise. 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 **peakasutaja**.
2.16. **Risk** on hinnanguline määratlus olukorrale, mille realiseerumine avaldab mõju asutuse eesmärkide saavutamisele. Riskid tehakse kindlaks ja hinnatakse riskianalüüsi käigus ning hoitakse ohjes riskihalduse abil.
2.17. **Terviklus** on õigsus ja täielikkus, lubamatute muudatuste puudumine, hõlmab ka autentsust ja salgamatust, üks teabe turvalisuse kolmest põhikomponendist.
2.18. **Tooteomanik** on asutus, kes osutab IKT teenust. Korra tähenduses on tooteomanik SMITi teenuste portfellis määratud IKT teenuse ja/või toote omanik.
2.19. **Vastutav töötleja** on füüsiline või juriidiline isik või muu (isiku)andmete töötlemise eest vastutav organ, kes määrab kindlaks andmete töötlemise eesmärgi ja vahendid. SMITi kontekstis on vastutav töötleja enamasti klient.
2.20. **Volitatud töötleja** töötleb andmeid vastutava töötleja nimel lepingu alusel, nt Siseministeeriumi valitsemisala kontekstis SMIT.
2.21. **Väline partner** on SMITile teenuseid andva organisatsiooni (lepingupartneri/tarnija) esindaja.

3. Rollid ja kohustused

3.1. Infoturbe tagamisel, järelevalvetoimingute tegemisel ja teenuste haldamisel rakendatakse kohustuste lahususe põhimõtet.

3.2. Infoturbekorra rakendamise ja infoturbe halduse süsteemi käitamise eest vastutab SMITi juhtkond järgmises koosseisus: peadirektor, peadirektori asetäitja äriteenuste valdkonnas, peadirektori asetäitja baasteenuste valdkonnas, peadirektori asetäitja inimeste ja kultuuri valdkonnas, strateegiajuht.

3.3. Juhtkond 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 juhtkonda infoturbe tegevustest ja tulemustest. Infoturbejuht SMITis on infoturbeosakonna juhataja, kelle õigused, kohustused ja vastutus on sätestatud Siseministeeriumi valitsemisala infoturbepoliitikas, 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 turbesündmusest või muust turbeohust asutusele või osutatavatele teenustele või nende kahtlusest.

3.9. Teenuste infoturbealane vastutus oma teenuste piires on struktuuriüksuse juhil, kes korraldab, vastutab ja teostab järelevalvet korrast ning teenuse ja selles käideldavate andmete spetsiifikast tulenevate nõuete rakendamise eest oma vastutusvaldkonnas. Struktuuriüksuse 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 juht teostab järelevalvet juurdepääsude ning teenustes töödeldavate andmete kasutamise üle, sealhulgas teenuste testimiseks kasutatavate andmete ning lisakeskkondade loomise üle. Andmete volitatud töötlejana kooskõlastab andmete ja teenuse keskkondades / infovarades, sh andmetes tehtavaid muudatusi ja nõudeid andmete vastutava töötlejaga (Service Deskis või lepingus sätestatud tingimustel).

3.11. Struktuuriüksuse 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 turvanõrkuste tähtaegne likvideerimine. Riskide aktsepteerimine ja maandamine muul viisil peab olema põhjendatud ja proportsionaalne ja 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 infoturbepoliitika

4. Personali turve

4.1. Kõigi töökohakandidaatide, praktikale kandideerivate ja SMITile teenust osutavate väliste partnerite (inimeste) tausta kontrollitakse. Tausta kontrollimisel järgitakse õigusaktidest tulenevaid piiranguid. Kõiki, kellelt oodatakse taustakontrolli läbimist, teavitatakse taustakontrolli teostamisest. Taustakontrolli teostamise aluseks on politsei ja piirivalve seadus.
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 käesoleva 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. Töötajal on kohustus läbida uue töötaja sisseelamiskavasse kuuluv infoturbekoolitus ja kohustuslikud regulaarsed infoturbekoolitused.
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 leidmise töötaja asendaja või muu volitatud isiku poolt.
5.2. Konfidentsiaalseid andmeid sisaldavaid digitaalseid andmekandjaid tuleb hoida märgistatult lukustatud kapis, tööruumides ja krüpteeritult.
5.3. SMITi kasutuses olnud ja mittevajalikuks muutunud ning säilitamisele mittekuuluvad andmekandjad tuleb õigeaegselt ja kehtivate kordade kohaselt hävitada, välistades andmete taastamise.

5.4. Andmekandjate hävitamise või taaskasutamise korral hindab selle määratud kasutaja ja/või omanik koos andmete vastutava töötlejaga andmekandjal olevaid andmeid säilitamise või hävitamise eesmärgil.
5.5. Andmete varundamist ja taastamist reguleerivad nõuded talitluspidevuse tagamise korraldamisele.
5.6. Igasuguse SMITi poolt väljastatud andmekandja või seadme kadumisest või vargusest või kolmanda osapoole võimalikust ligipääsust selle andmetele tuleb võimaliku kahju vähendamiseks viivitamatult teavitada kliendituge.
5.7. Tööalaste andmete töötlemiseks, sh säilitamiseks ja transpordiks tohib kasutada vaid SMITi poolt väljastatud irdandmekandjaid (USB-andmekandjaid ja -seadmeid, andmemassiive, mälukaarte, väliseid kõvakettaid jmt).
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. Andmete irdandmekandjast 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 virtuaalserverites 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 oma allkirjaga või teadmiseks võtmisega dokumendihaldussüsteemis kinnitab, et ta 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 tuleb silmas pidada, et neid ei oleks võimalik volitamata kasutada ning teisaldada, sh tuvastada töödeldava dokumendi sisu.
7.6. Kasutaja peab välistama kõrvaliste isikute ligipääsu töövahenditele (arvuti ja mobiilsed seadmed).
7.7. Väljaspool Siseministeeriumi valitsemisala asutuste asukohtasid ei ole töötajal lubatud jätta talle kasutamiseks antud IT-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 selle eest tootetiim.
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 kasutajatuvastust. 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 tarkvara tööd (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 info-süsteemide 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, kasutades sealhulgas nt Bluetoothi, 4G-d, WiFi-t jms.

10.7. Bluetooth lisaseadmete kasutamine SMITi seadmetes 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.

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 selliseid isiklikke seadmeid, mille kaudu ei toimu andmevahetust (nt monitor, klaviatuur, hiir). Samuti tohib ühendada SMITi keskselt hallatavat mobiilset seadet.

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

11. E-post ja kiirsõnumivahetus

11.1. Kogu e-posti liiklus SMITi võrgust või SMITi võrku peab läbima SMITi hallatava e-posti serveri. Tööülesannetega seotud elektrooniliseks kirjavahetuseks võib kasutada ainult SMITi hallatavat e-posti aadressi.

11.2. Töötaja tohib kasutada talle eraldatud e-posti aadressi ainult tööülesannetega seotud kirjavahetuseks.

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 MetaVaulti failide turvakontrolli süsteemiga (https://wiki.smit.sise/pages/viewpage.action?pageId=152539601) või saates failid ja/või failijagamiskeskkondade lingid aadressile failikontroll@smit.ee. Kontrollitud failid saab alla laadida https://metavault.smit.sise 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. Töötajal ei ole lubatud kasutada isiklikku e-posti aadressi või kiirsuhtlusrakendusi asutusesiseseks kasutamiseks mõeldud teabe vahetuseks.
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. Kui tegemist on andmekogu andmetega, 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. 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 möödapääsmatu, tuleb selleks järgida SMITi erakorraliste koopiate tegemise ning haldamise korda.
12.9. 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.

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

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

Vaata lisaks: IKT arendusprotsess, Muudatusehalduse kord, Nõuded talitluspidevuse tagamise korraldamisele, Põhiprotsess, SMITi erakorraliste koopiate tegemise ning haldamise kord, Teenuste portfell

13. Välised partnerid

13.1. Kõigi väliste partnerite suhtes viiakse läbi taustakontroll.

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

13.3. Välisele partnerile, kes ülesannete täitmisel puutub kokku SMITi infovaradega, tutvustatakse turbenõudeid ja nendega seotud juhendeid ning kordasid ulatuses, mis vastab välise partneri töö iseloomule. Väline partner kinnitab, et on tutvunud lepingu täitmiseks vajalike kordadega. Kordade tutvustamise eest vastutab SMITi poolne lepingu kontaktisik.

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. 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.

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

Vaata lisaks: Väliste partnerite taustakontrolli ja juurdepääsuõiguste taotlemise kord

14. Infoturvaintsidentide haldus

14.1. Kasutaja isikuga 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 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. Töötaja, kes puutub tööülesannete täitmisel või töö käigus juhuslikult kokku konfidentsiaalsete andmetega, kohustub:
  15.2.1. mitte avalikustama ega edastama kolmandatele osapooltele temale teatavaks saanud konfidentsiaalset teavet, välja arvatud õigusaktides sätestatud juhtudel;
  15.2.2. järgima kehtivaid andmekaitset puudutavaid õigusakte ja kordasid;
  15.2.3. täitma konfidentsiaalsuskohustuse nõudeid nii töösuhte ajal kui ka peale selle lõppemist.
15.3. Kui isik teostab töid töövõtu- või muu võlaõigusliku lepingu alusel, peavad lepingu konfidentsiaalsussätted sisaldama korra punktis 15.2 sätestatud põhimõtteid.

Vaata lisaks: Töökorralduse reeglid

Lisa 1. Viidatud dokumendid

Paljud infoturbega seotud teemad on reguleeritud muudes SMITi dokumentides. Viidatud dokumendid ja lingid leiad siit:

1. https://wiki.smit.sise/display/SEC/SMITi+infoturvet+reguleerivad+korrad
2. Infoturbejuhendid leiad siit: https://wiki.smit.sise/display/SEC/Juhendid