TARBIJAKAITSE JA
TEHNILISE JÄRELEVALVE
AMET

KÄSKKIRI

28.04.2025 nr 1-2/25-030

Tarbijakaitse ja Tehnilise Järelevalve Ameti infovahendite kasutamise ja andmete töötlemise korra kinnitamine

Majandus- ja taristuministri 07.12.2018 määruse nr 62 „Tarbijakaitse ja Tehnilise Järelevalve Ameti põhimäärus“ § 5 lõike 3 punkti 1 alusel:

kinnitan

Tarbijakaitse ja Tehnilise Järelevalve Ameti infovahendite kasutamise ja andmete töötlemise korra.

(allkirjastatud digitaalselt)
Kristi Talving
peadirektor

Koostaja: Vahur Viigimäe

KINNITANUD
peadirektor
28.04.2025
käskkirjaga nr 1-2/25-030

Tarbijakaitse ja Tehnilise Järelevalve Ameti infovahendite kasutamise ja andmete töötlemise kord

Sisukord

1. Üldsätted

1.1 Tarbijakaitse ja Tehnilise Järelevalve Ameti (edaspidi **TTJA**) infovahendite kasutamise ja andmete töötlemise korra (edaspidi **kord**) eesmärk on kehtestada ühtne regulatsioon IT-varade[1] ja seadmete kasutamiseks ning sätestada IT-alaste pöördumiste tegevusjuhised.

1.2 Kord lähtub TTJA infoturvapoliitikast ning TTJA infoturbekontseptsioonist ning rakendub kõikidele TTJA ametnikele ja töötajatele, kes asutuse IT-varasid kasutavad (edaspidi ühiselt **kasutajad** või **teenistujad**).

1.3 TTJA kasutab välist IT-teenuseosutajat, kes tagab IT kasutajatoe (edaspidi ka **IT-abi**), arvutitöökohtade halduse, äritarkvara kasutajatoe ning süsteemihalduse teenused. IT-teenuseosutaja kontaktid on leitavad käesoleva korra lisas 2.

1.4 Kontroll käesoleva korra järgimise üle sätestatakse TTJA infoturvapoliitikas.

2. IT-varade kasutamine

2.1 Kasutaja on kohustatud:

2.1.1 kasutama töövahendeid ainult tööülesannete täitmiseks ning hoidma neid kolmandatele isikutele kättesaamatuna;

2.1.2 kasutama IT-varasid ja töövahendeid heaperemehelikult;

2.1.3 töötlema asutusesiseseks kasutamiseks (edaspidi **AK**) mõeldud informatsiooni vaid tööandja lubatud seadmes ning tagama teabe konfidentsiaalsuse;

2.1.4 teavitama koheselt kõigist tuvastatud ja potentsiaalsetest IT-alastest probleemidest vastavalt korra p-s 15 ettenähtule;

2.1.5 kasutama ressursse optimaalselt ja mitte koormama töövahendeid ja sisevõrku mittetööalaste tegevustega;

2.1.6 sooritama tööle asudes ning vähemalt kord aastas e-postile saadetava küberturbe e-kursuse kõik moodulid;

2.1.7 osalema võimalusel infoturbekoolitustel, -õppustel ja -infopäevadel.

2.2 Kasutajal on keelatud:

2.2.1 jätta seadet järelevalveta või kasutada seda viisil, mis ei ole heaperemehelik ja sihtotstarbeline;

2.2.2 isikliku seadme omavoliline ühendamine tööandja arvutivõrku, välja arvatud juhul, kui see toimub külalistele mõeldud juhtmevabasse kohtvõrku, millega ühendumine mistahes seadmega on lubatud;

2.2.3 muuta või lubada muuta omavoliliselt seadme tark- või riistvaralist koosseisu (muuta konfiguratsiooni, eemaldada või lisada komponente, paigaldada seadmesse mistahes tarkvara, rakendusi, skripte jne), välja arvatud käesoleva korra p-s 4.3 toodud erisuse kohaselt;

2.2.4 külastada seadmest ja/või arvutivõrgust veebilehekülgi (nt illegaalse voogedastuse ja tarkvara allalaadimise lehed, täiskasvanutele mõeldud sisulehed,

[1] Kõik terminid ja nende selgitused vt „Lisa 1“

hasartmängud, vägivalda ja vihkamisele õhutavad lehed), mille külastamine võib tekitada tööandjale mainekahju või kahjustada seadme turvalisust;

2.2.4.1 erandina on lubatud eelmainitud keskkondade külastamine vahetute tööülesannete täitmiseks. Vajadusel tehakse seda eriotstarbelistest, TTJA IT-süsteemidega mitteühendatud seadmetest..

2.2.5 avada kahtlusi tekitava pealkirjaga ja/või kahtlust äratavatelt e-posti aadressidelt saabuvates e-kirjades sisalduvaid manuseid või linke. Sellises olukorras tuleb vastavalt korra p-s 15 ettenähtule pöörduda IT-abi poole;

2.2.6 lülitada välja pahavarakaitset tagavaid süsteeme või minna mööda arvutivõrgus kehtestatud piirangutest;

2.2.7 ühendada väljastatud seadme külge kontrollimata andmekandjaid (USB pulgad, mälukaardid, välised kõvakettad, salvestusvõimekusega interneti pulgad jne).

2.3 Kasutajal on õigus:

2.3.1 kasutada töökohustuste täitmiseks IT-varasid vastavalt käesolevale korrale;

2.3.2 keelduda tööjaama ekraanipildi, kaamera ja mikrofoni ülevõtmisest IT-abi poolt (tegevust ei rakendata ilma kasutaja loata);

2.3.3 pöörduda vastavalt korra p-s 17 ettenähtule IT-välistest probleemidest teavitamiseks või juhiste saamiseks TTJA töökorralduse reeglites ja/või TTJA siseveebis määratud vastutava isiku või üksuse poole;

2.3.4 käidelda tööalast informatsiooni TTJA sisevõrgus ning TTJA poolt sätestatud infosüsteemides;

2.3.5 ühendada tööjaama külge sisendseadmeid (hiir, klaviatuur), esitlus- ja helitehnikat (sh isiklik monitor, kõrvaklapid jms).

2.4 Teenuseosutaja infoturbevaldkonnal ja teistel vastava teenusega seotud osakondadel on õigus kontrollida kasutaja valduses olevaid seadmeid, tegevust ja selle salvestusi, logisid ning võrguliiklust tööjaama ja internetiteenuse vahel infoturbeintsidendi ennetamiseks, avastamiseks ja lahendamiseks.

2.5 Infoturbeintsidendi ennetamise ja lahendamise eesmärgil on IT-teenuseosutaja infoturbevaldkonnal õigus peatada või piirata kasutusõigusi ning võtta seade oma valdusesse kuni asjaolude selgitamiseni.

3. Juurdepääsuõiguste haldus ja paroolid

3.1 Infovahendite kasutamine toimub personaalse kasutajakonto alusel. Kontode ühiskasutus ja/või pääsuinfo jagamine teistele kasutajatele ega kolmandatele osapooltele ei ole lubatud.

3.2 TTJA personalitöötaja algatab uutest teenistujatest ning teenistujate liikumisest või andmete muutumisest töövoo, mille alusel IT-teenuseosutaja loob teenistujale kasutajakonto või muudab seda.

3.3 Pääsuõiguseid jagatakse ainult IT-teenuseosutaja poolt IT-abi kaudu registreeritud tellimuste alusel.

3.4 Kasutajakontode paroolid edastatakse alati personaalselt e-kirja teel ja krüpteeritud Digidoc konteineris. Erandiks on kasutaja tööle asumisel väljastatud esmane parool, mis edastatakse töötaja otsesele juhile ning mille kasutaja peale esmast sisselogimist muudab.

3.5 Kasutaja peab muutma oma parooli:

3.5.1 koheselt peale esmast sisselogimist;.

3.5.2 vähemalt üks kord aastas, vastavalt IT-teenuseosutaja poolt seadistatud paroolide aegumise teavitustele;

3.5.3 kui on tuvastatud parooli väärkasutus või avalikuks tulek.

3.6 Parool peab vastama minimaalselt järgmistele nõuetele:

3.6.1 pikkus peab olema vähemalt 14 sümbolit;

3.6.2 peab olema piisavalt keerukas, et vältida ära arvamist;

3.6.3 ei tohi olla leitav sõnastikest ega omada otsest või kaudset seost kasutajaga;

3.6.4 peab koosnema minimaalselt neljast sümbolite grupist – suurtähed, väiketähed, numbrid, kirjavahemärgid.

3.7 Infosüsteemist tingitud juhtudel võib parool eelpool sätestatust erineda.

3.8 Kasutaja vastutab personaalselt talle antud ja tema poolt seatud paroolide saladuses hoidmise eest.

3.9 TTJA töövahendites kasutatavaid paroole ei tohi kasutada teiste asutuste või teenuste rakenduses (Gmail, Hotmail või muud e-posti teenused, Facebook või muud suhtlusportaalid, Dropbox või muud failijagamisteenused jne) ja vastupidi.

3.10 Paroole on lubatud hallata vaid selleks ettenähtud keskkondades (nt KeePass).

3.11 Pärast töö lõpetamist tuleb kasutatud süsteemist alati välja logida.

3.12 Kasutajakonto lukustub parooli viiekordsel valesti sisestamisel.

3.12.1 Konto lukustumise korral peab kasutaja ühendust võtma IT-abiga (vt. lisas 2 toodud kontaktid).

3.13 Teenistuja töösuhte lõppemisel suletakse personalitöötaja poolt algatatud töövoo põhjal kõik kasutajaga seotud kontod tema viimase tööpäeva lõpul, kui ei ole kokku lepitud teisiti.

3.14 Teenistuja töösuhte lõppemisel säilitatakse teenistuja valduses olnud informatsioon (e-post, kodukataloog) 6 kuud. Juurdepääs eelnimetatud informatsioonile võimaldatakse põhjendatud juhtudel teenistuja vahetule juhile või tema poolt nimetatud isikutele pöördumise alusel. E-posti ümber ei suunata.

4. Tööjaam (paiksed ja/või mobiilsed kohtvõrku ühendatud arvutid)

4.1 Tööjaama tarnib, häälestab ja paigaldab IT-teenuseosutaja, TTJA personalitöötaja või vahetu juhi poolt algatatud pöördumise (töövoo) alusel.

4.2 Kasutaja vastutab tema kasutusse antud tööjaama ja selle lisaseadmete nõuetekohase kasutamise eest alljärgnevalt:

4.2.1 kuvariekraan ei asu kõrvaliste isikute nägemisväljas, vajadusel kasutatakse ekraanifiltrit;

4.2.2 tööjaama juurest lahkudes tuleb tööjaama ekraan sulgeda või lukustada (nt käsuga Windowsi logo klahv + L);

4.2.3 tööjaam ja selle lisaseadmed on alaliselt kaitstud varguse eest.

4.3 Tööjaamas on lubatud kasutada ainult eelpaigaldatud või tarkvarakeskuses (*Software Center*) kättesaadavaks tehtud tarkvara.

4.3.1 Kui kasutaja soovib ametialaseks tegevuseks kasutada TTJA või IT-teenuseosutajale mittekuuluvat IT-vara või paigaldada tööjaama tarkvarakeskuses puuduvat tarkvara, tuleb selleks vastavalt korra p-le 15 esitada taotlus IT-abisse.

4.4 Bluetooth, kaamera ja mikrofon lülitatakse tööjaamal sisse vaid nende kasutamisel. Muul ajal on need deaktiveeritud (kasutades tööjaama füüsilist kaamerakatikut ja mikrofoni vaigistamise nuppu).

4.5 Tööjaama sisselogimiseks võidakse kasutada kaheastmelist autentimist, kus rakendatakse nt ID-kaardi, digi-ID, Windows Hello for Business või Yubikey'ga autentimist.

4.6 Tööjaama kasutajale on infosüsteemide kasutamiseks ja juurdepääsuks antud kasutus- ja pääsuõigused vastavalt kasutaja ametijuhendis toodud teenistusülesannete ning volituste täitmiseks. Täiendavate õiguste taotlemiseks tuleb vastavalt korra p-le 15.2.6 pöörduda IT-abi poole.

4.7 Enne uue tarkvara kasutuselevõttu on vajalik selle kooskõlastus IT-abi poolt. Ilma eelneva kooskõlastuseta on kasutajatel keelatud tarkvara tööarvutitesse lisada.

5. Failiruum ja failide edastamine

5.1 Igale kasutajale on tagatud temale antud tööjaamas personaalne failiruum, kaustades Dokumendid (*My documents*) ja Töölaud (*desktop*), mis on mõeldud tööalaste failide hoiustamiseks. Personaalsetes failiruumides hoiustatavaid faile varundatakse. Personaalsel failiruumil on mahupiirang. Teisi asukohtasid kohalikus arvutis ei varundata.

5.2 Failiserveril on kasutajale saadaval Z ketas ainult TTJA kasutajatele ja Y ketas, kuhu saab tellida eriõigustega kettapinda.

5.3 Ühise failiruumi kaudu tööalaste failide jagamisel tuleb kasutada selleks vastavale kasutajagrupile eraldatud ühist kausta ning veenduda, et kasutajagruppi kuuluvad kasutajad tohivad vastavale infole juurde pääseda. Info haldamise eest vastutab vastava info omanik.

5.4 Teadmispiiranguga (nt isikuandmed) failid, mida hoitakse teadmisvajadust mitteomavate isikutega ühises failiruumis, peavad olema krüpteeritud.

5.5 Ühistes failiruumides hoiustatavad failid varundatakse ning vajadusel saab neid taastada kuni 6 kuu tagusesse perioodi.

5.6 Ühistes failiruumides asuvad failid on vastava info looja vastutusel. Kui info on vananenud ja ei leia enam kasutust, siis tuleb see ühisest failiruumist eemaldada.

5.7 AK teabe edastamine on lubatud alljärgnevatel viisidel:

5.7.1 riigiasutuste adressaatidele krüpteerimata kujul, kasutades selleks tööjaamas seadistatud infovahetuse tarkvara (nt Outlook) ja/või TTJA dokumendihalduse korras sätestatud edastusvahendeid;

5.7.2 riigiasutuste välistele adressaatidele krüpteeritud (nt krüpteerides ID-kaardiga või TTJA krüptovõtmega) või krüpteerimata kujul vastavalt õigusaktides reguleeritud juurdepääsutingimustele ning kasutaja tööandja kehtestatud nõuetele;

5.7.3 asutusevälisele või -sisesele osapoolele krüpteerimata kujul, kasutades selleks IT-teenuseosutaja poolt võimaldatud failivahetuskeskkonda (https://transit.envir.ee)

või samaväärset turvalist infovahetuskeskkonda (nt SharePoint). Eeltooduid eelistatakse mahukamate andmete edastamisel.

5.8 Kasutaja on kohustatud jälgima, et kõrvalistele isikutele ei esitata jääkteavet. Kasutaja peab:

5.8.1 kontrollima enne failide edastamist, ega failid ei sisalda avaldamisele mittekuuluvat jääkteavet nagu kommentaarid, muudatuste ajalugu või liigsed metaandmed;

5.8.2 eemaldama tuvastatud jääkteabe, vajadusel muutma selleks failivormingut.

5.9 Jääkteabe eemaldamise kohustuse täitmist kontrollitakse pisteliselt.

5.10 Failide edastamisel välistel andmekandjatel tuleb lähtuda käesoleva korra p-st 11 **(**Irdkandjate käsitsemine**).**

6. Pilvteenuste kasutamine

6.1 Pilvteenuste (nt Teams, OneDrive, SharePoint) kasutamine peab toimuma vastavalt TTJA infoturvapoliitikale ja andmekaitse juhendile.

6.2 Pilvteenuseid kasutatakse ainult IT-teenuseosutaja poolt lubatud platvormidel.

6.3 IT-teenuseosutaja infoturbevaldkond võib pilvteenuste kasutamisele seada tehnilisi piiranguid, mis on vajalikud infoturbenõuete täitmiseks.

6.4 Pilvteenuses hoitavate andmete eest vastutab lõppkasutaja (andmete omanik). Kui andmete omanik teab, et tema andmed ei tohi Eestist väljuda või peab seda liiga suureks riskiks, tuleb kasutada alternatiivseid grupitöö lahendusi (nt võrgukettad Z ja Y).

6.5 Tundlike andmete (isikuandmed, AK teave jne) juhusliku lekkimise vältimiseks, tuleb pilvteenuses rakendada krüpteerimist (nt ID-kaart, 7-zip).

6.6 Andmete omanik tagab, et pilvteenuse rikke või kompromiteerimise korral ei kaasneks andmete hävimist. Selle vältimiseks tuleks teha turvakoopiaid ühistöö võrguketastele Z ja Y.

6.7 Pilvteenustes tohib hoida ainult andmeid, mis on koostööks tarvilikud ning mille säilitusvajadus on lühike. Pilvteenustest tuleb kustutada andmed, mida seal ei ole enam vaja.

7. Grupitöö- ja konverentsitarkvara

7.1 Kasutajal on lubatud vaikimisi kasutada ainult IT-teenuseosutaja poolt lubatud ja toetatud grupitöö- ja konverentsitarkvara rakendust MS-Teams.

7.1.1 Muude rakenduste (Zoom, Webex, Signal, Slack jm) kasutamine on lubatud, kui on tagatud infoturbe üldnõuded ning rakendus on vältimatult vajalik ja koosoleku korraldaja poolt valitud.

7.2 Kasutajad on teadlikud, kuidas grupitöö- ja konverentsitarkvara turvaliselt kasutada, seda ka välise osapoole algatatud vestluste või videokonverentside puhul.

7.3 Videokonverentsi või veebikoosoleku algatamisel:

7.3.1 toimub osalejate valik vastavalt vestluse sisule ja eesmärkidele;

7.3.2 toimub kõigi osalejate tuvastamine;

7.3.3 toimub modereerimisõiguste määramine ainult valitud kasutajatele;

7.3.4 lepitakse kokku videokonverentsi või vestluse salvestamise korras;

7.3.5 lepitakse kokku konverentsiseadmete kasutamise korras.

7.4 Konverentsi- ja grupitöötarkvarasse tuleb siseneda ametlike töökoha kontodega. Isikliku tarkvara või kontode kasutamine ametlikel koosolekutel ei ole lubatud, kui see ei ole erandjuhul eelnevalt kokku lepitud.

7.5 Koosolekute ja töögruppide andmeid (sh salvestusi, dokumente, vestlusi) tuleb käsitleda vastavalt TTJA andmekaitse reeglitele ja põhimõtetele.

7.6 Salvestuste tegemine on lubatud ainult põhjendatud juhtudel ja peab olema eelnevalt osalejatega kooskõlastatud.

7.7 Koosolekutele ja grupitööruumidesse ei tohi kutsuda volitamata osalejaid ega jagada konfidentsiaalset teavet väljapoole asutust.

7.8 Osalejad peavad kasutama turvalisi ühendusi ja vältima tundliku teabe jagamist avalikus või ebaturvalises keskkonnas.

7.9 Konverentsikõne või muu vestluse raames on keelatud edastada/jagada isikuandmeid või muid AK märkega informatsiooni ja/või andmeid, samuti teavet, millel AK märge puudub, kuid mille sisu on mõeldud üksnes asutusesiseseks kasutamiseks.

7.10 Kasutajatel on kohustus vestluse alguses tehisintellekti (edaspidi **TI**) funktsioonid välja lülitada (juhul, kui TI funktsioonid on aktiveeritud).

7.11 Kasutajal on keelatud üle anda oma seadme juhtimine teisele osapoolele, välja arvatud IT-abi teenuse osutamisel IT-probleemide lahendamiseks vajaliku seansi puhul.

7.12 Virtuaalse koosoleku puhul kaugtööl olles (näiteks kodukontor) tuleb tagada, et:

7.12.1 taustal olevad esemed, isikud ning helid ei ole tuvastatavad;

7.12.2 kõrvalistele isikutele ei ole tuvastatavad virtuaalsel koosolekul osalevad isikud ja nad ei näe ega kuule koosolekul esitatud konfidentsiaalset teavet.

8. E-post ja meililistid

8.1 Igal kasutajal on tööalaseks kasutamiseks e-posti aadress kalendri kasutamise võimalusega.

8.2 Tööalast e-posti aadressi kasutatakse moel, mis ei kahjusta tööandja usaldusväärsust ja mainet ning mis ei põhjusta töövälise infovoo algatamist (nt kommertsteated või rämpspost).

8.3 Tööalaseid e-posti aadresse ei tohi kasutada isiklikuks otstarbeks.

8.4 Tööalaseid e-kirju ei ole lubatud suunata TTJA-välisele e-posti aadressile (nt isiklikule Gmaili e-posti aadressile).

8.5 Nii e-postkastile kui ka ühekordse e-kirja suurusele on kehtestatud vaikimisi mahupiirangud, millega saab tutvuda IT-Teenuseosutaja teenusveebis.

8.6 Kasutaja e-posti sisu (kirjade mustandid, saadetud ja saadud kirjad, manused, kalendrikanded) on varukoopiatelt taastatavad 6 kuu jooksul alates salvestamisest, saatmisest või saamisest.

8.7 Kasutajad lisatakse meililistidesse arvuti kasutajakonto loomisel vastavalt ametikoha struktuursele paiknemisele.

8.8 Täiendavate meililistide või ühise e-posti aadressi loomiseks teeb TTJA teabehalduse nõunik vastavalt korra p-le 15.2.7 (meililistide loomine või muutmine;) vastavasisulise pöördumise IT-abisse vastavalt TTJA dokumendihalduse korrale.

9. Nutiseade

9.1 Kui tööandja on väljastanud tööalaseks kasutamiseks nutiseadme (mobiiltelefon, tahvelarvuti vms), eelistab kasutaja tööalaseks kasutamiseks turvakaalutlusel väljastatud nutiseadme kasutamist isiklikule seadmele.

9.2 Kasutajale võimaldatakse juurdepääs tööalastele rakendustele (Teams, Outlook) läbi nutiseadme, juhul kui on täidetud vastavad eeldused:

9.2.1 kasutajal on App Store'i või Google Play konto.

9.2.2 Grupitöö- ja suhtlustarkvara kasutamiseks nutiseadmes tuleb läbi App Store'i või Google Play keskkonna paigaldada rakendus MS Teams.

9.2.3 E-posti kontole ligipääsuks tuleb seadistada telefon vastavalt IT-teenuseosutaja iseteeninduspportaalis asuvale juhendile.

9.3 Nõuded nutiseadme ja rakenduste tööalaseks kasutamiseks:

9.3.1 kasutaja peab tundma ja kasutama nutiseadme (sh ka isikliku) turvafunktsionaalsust;

9.3.2 seadmel ei tohi olla eemaldatud tootja kehtestatud piirangud, näiteks lahtimurdmise (*jailbreak)* või juurkasutaja õiguste ülevõtmise (*rooting*) teel;

9.3.3 rakenduste kasutamine eeldab vähemalt kuuekohalist PIN-koodi seadme ekraaniluku avamiseks;

9.3.4 lisaks PIN-koodile võib kasutaja rakendada täiendavalt seadme toetatud autentimise lahendusi (nt sõrmejäljelukk, näotuvastus, YubiKey), tagades seeläbi mitmeastmelise autentimise;

9.3.5 seadmes tuleb vältida Bluetoothi, traadita kohtvõrgu liidese (WiFi), globaalse asukoha süsteemi (GPS) ja teiste taoliste funktsioonide tarbetut aktiveerimist;

9.3.6 Bluetooth ühenduse loomisel teise seadmega rakendab kasutaja turvalist sidumiskoodi;

9.3.7 andmevahetuse eelistatuim viis on mobiilsideoperaatori andmeside;

9.3.8 uusi rakendusi, sh personaalseks kasutamiseks mõeldud rakendusi, on lubatud paigaldada ainult usaldusväärsetest allikatest, nagu App Store või Google Play;

9.3.9 kasutaja paigaldab kõik seadme- või operatsioonisüsteemi tootja väljastatud tarkvara turvauuendused;

9.3.10 kasutaja piirab virtuaalsete assistentide kasutamise;

9.3.11 tuleb vältida konfidentsiaalse informatsiooni ja AK teabe käitlemist isiklikus nutiseadmes;

9.3.12 kasutaja vastutab kahjurvaratõrje rakenduse kasutamise eest.

9.4 Nutiseadet (sh mobiilset tööjaama) on keelatud kaasa võtta konfidentsiaalsetele koosolekutele, kui koosoleku korraldaja on nii sätestanud.

9.5 Enne tööalaselt kasutatud nutiseadme (sh isikliku seadme) mistahes moel kasutuselt kõrvaldamist (sh ajutiselt kasutuselt kõrvaldamisel seadme hooldusesse viimisel) eemaldab kasutaja seadmest tööga seotud kontod, rakendused ja juurdepääsud:

9.5.1 taastab seadme tehaseseaded (mis ühtlasi kustutab telefonist ka kasutaja andmed) ja kontrollib, kas kõik andmed on telefonist kustutatud;

9.5.2 kui andmeid ei õnnestu seadmest kustutada, annab kasutaja seadme andmete kustutamiseks IT-teenuseosutajale;

9.5.3 seadme kasutuselt kõrvaldamisel võtab seadmest välja ja kustutab turvaliselt või hävitab seadmes olnud mälukaardi ja/või SIM-kaardi.

9.6 Tööalaselt kasutatud nutiseadme (sh isikliku nutiseadme, kui sellel on aktiveeritud juurdepääs tööalastele rakendustele) kaotamise, hävimise või varguse korral tuleb sellest vastavalt korra punktile 15.2.5. viivitamatult teavitada IT-abi;

9.7 Kadunud nutiseadme ülesleidmisel tuleb kontrollida, kas seadet pole vahepeal manipuleeritud. Kahtluste korral tuleb seade kõrvaldada kasutuselt või teha seadmele uuesti tehase algseadistus.

9.8 Teiste nutifunktsioone omavate seadmete (esemevõrgu- ehk IoT-seadmete) kasutamisel tuleb lähtuda korrast „TTJA esemevõrgu (IoT) seadmete kasutamise kord“.

9.9 Nutiseadmete toite tagamiseks hoitakse telefoni aku piisavalt laetuna. Pikemaajalisel mobiiltelefoni kasutusel kantakse kaasas laadijat ja/või akupanka.

9.9.1 Aku säästmiseks ja nutiseadme kasutusohutuse tagamiseks (nt isesüttimine) välditakse äärmuslikke temperatuure.

9.9.2 Võimalusel välditakse avalikke USB-laadimispesasid (lennujaamad, ühistransport, kaubanduskeskused, meelelahutusasutused jms) ning eelistatakse vooluvõrku ühendatavat laadijat.

9.10 Kui tööalaseks tegevuseks kasutatakse isiklikku seadet, siis:

9.10.1 peavad olema täidetud kõik käesolevas korras toodud nõuded seadmele;

9.10.2 seadmega ümberkäimisel ja AK teabe seadmes töötlemisel lähtutakse käesolevas korras esitatud nõuetest;

9.10.3 tööalaseks kasutamiseks on lubatud ainult IT-teenuseosutaja poolt heaks kiidetud rakendused (nt MS Teams, Outlook).

10. Tehisintellekt (TI)

10.1 Kasutajal on keelatud TI kasutamine mistahes viisil, mis põhjustab märkimisväärseid riske inimeste tervisele, ohutusele või põhiõigustele (manipuleerivad, ekspluateerivad TI-süsteemid, nn „*sotsiaalsed hindamissüsteemid*“).

10.2 Kasutajal on keelatud TI kasutamisel asutusesiseseks kasutamiseks mõeldud (mh AK-märkega) ning isikuandmeid sisaldava info kasutamine.

10.3 TI-mudelite treenimiseks kasutatakse ainult pseudonüümitud või anonüümitud isikuandmeid.

10.4 Kui TI sisendis on vajalik täielikult või osaliselt kasutada kolmandate isikute intellektuaalomandit, siis selliste andmete kasutamiseks on eelnevalt vajalik hankida omaniku luba.

10.5 Kasutajal on keelatud generatiivse TI poolt loodud, teadaolevalt kunstnike või kirjanike stiili matkivate teoste kasutamine, välja arvatud juhul, kui see on vajalik otseste tööülesannete täitmiseks.

10.6 Kõik TI poolt tehtud (sh esialgsed) otsused peab valideerima kasutaja.

11. Irdkandjate käsitsemine

11.1 Irdkandjate (ehk hõlpsalt vahetatavate andmekandjate, näiteks BD, CD, DVD, lindikassett, mälupulk, väline kõvaketas, mälukaart jne) tööalane kasutamine on vaikimisi keelatud. Põhjendatud kasutusvajaduse korral tuleb esitada pöördumine IT-abisse.

11.2 AK või muu tööalase teabe salvestamine irdkandjale toimub vaid otseste tööülesannete täitmiseks.

11.3 Kasutatakse vaid IT-teenuseosutaja poolt heaks kiidetud või kontrollitud irdkandjaid. Vastavuse kontrollimiseks tuleb teha taotlus IT-abisse.

11.4 Irdkandja ei ole ette nähtud andmete pikaajaliseks säilitamiseks. Kui informatsiooni hoidmine irdkandjal ei ole enam tööülesannete täitmiseks vajalik, tuleb informatsioon irdkandjalt kustutada.

11.5 Juhul, kui irdkandja ei ole krüptograafilise funktsionaalsusega (nt krüpteeritud mälupulk või kõvaketas), on soovituslik andmekandjal olev teave krüpteerida ID-kaardiga.

11.6 IT-teenuseosutaja poolt väljastatud irdkandja on kasutajapõhine ning mõeldud kasutamiseks vaid taotluses esitatud töökohustuste täitmiseks.

11.7 Irdkandjaid transporditakse üldjuhul isikliku järelevalve all.

11.8 Kui põhjendatud juhtudel kasutatakse transportimiseks posti- või kullerteenust, tuleb irdkandja pakkida turvalisse ja pakendi korduvat avamist-sulgemist mittevõimaldavasse pakendisse (eelistatult turvaümbrikku). Lahtikrüpteerimise võti või parool saadetakse alternatiivset kanalit kasutades. Pakend ega irdkandjal olev märgistus ei tohi sisaldada vihjeid pakendis oleva info sisu kohta.

11.9 Kui kasutaja saab irdkandja posti- või kullerteenuse kaudu, peab ta veenduma, et:

11.9.1 saatja on tuvastatav ja ta on irdkandja reaalselt adressaadile saatnud,

11.9.2 saadud pakend on terve ja kahjustamata.

11.10 Kui pakend on kahjustatud või esineb kahtlus pakendis sisalduva irdkandja manipuleerimise kohta, siis on seda lubatud kasutada vaid pärast selle verifitseerimist IT-teenuseosutaja poolt.

11.11 Kasutaja on kohustatud irdkandja vargusest, kaotusest või manipuleerimiskahtlusest vastavalt käesoleva korra punktile 15 (IT-abi ja pöördumised) koheselt IT-abi teavitama.

11.11.1 Kasutaja täpsustab eelnimetatud teates, millist teavet irdkandjal talletati.

11.12 Pärast kaotamist üles leitud või taasloodud irdkandjat tuleb kontrollida võimaliku andmemanipulatsiooni ja kahjurvara leidumise suhtes.

11.13 Kõrgema kaitsetarbe korral tohib iga irdkandjat kasutada vaid ühe korra.

11.14 Enne korduvkirjutatavate irdkandjate edasiandmist, taaskasutamist või kasutuselt kõrvaldamist on irdkandjatelt andmed ettenähtud viisil (näiteks irdkandja turvaline formaatimine) kustutatud.

11.15 Irdkandjaid sisaldavaid kingitusi on lubatud kasutada vaid pärast nende verifitseerimist IT-teenuseosutaja poolt.

12. Printimine ja skaneerimine

12.1 Tööalase teabe printimine, paljundamine ja skaneerimine on lubatud ainult IT-teenuseosutaja poolt või kasutaja enda poolt hallatavast seadmest.

12.2 Teabe printimisel või paljundamisel tuleb vastav materjal koheselt printerist eemaldada.

12.3 Printerist või koopiamasinast leitud materjal tuleb koheselt toimetada selle omanikule või omaniku tuvastamatuse korral hävitada paberihunti kasutades või viia see 0-korrusel asuvasse kinnisesse paberikonteinerisse (v.a juhul kui tööandja TTJA on reguleerinud teisiti).

12.4 Ekslikult prinditud tarbetu dokument hävitatakse kohe, ekslikult skaneeritud dokument kustutatakse.

13. Kaugtöö

13.1 Kaugtöö (töötamine väljaspool TTJA ruume) korraldamine lähtub TTJA töökorralduse reeglitest.

13.2 Muud olulised kaugtöö aspektid (töötaja vastutus, kulude hüvitamine jne) on reguleeritud telefoniside korralduspõhimõtete ja kulude piirmäärade kehtestamise korraga ja muude kaugtööd puudutavate lisakokkulepetega.

13.3 Tööandja tööruumidest väljaspool töötamiseks kasutatakse usaldusväärseid parooliga kaitstud võrguühendusi (nt kodune Wi-Fi). Avalike võrkudega (nt kohvikute, hotellide jms võrkudega) ühenduse loomisele eelistab kasutaja esimese valikuna sülearvuti sisseehitatud modemiga andmeside loomist. Selle puudumisel mobiilse andmeside kasutamist (*hotspot*), mis on kaitstud parooliga (minimaalselt WPA2-AES). Piisava kvaliteediga võrguühenduse olemasolu eest väljaspool tööruume vastutab arvuti kasutaja.

13.4 Kõikides arvutites on eelseadistatud VPN tarkvara, mis rakendub automaatselt väljaspool kontori võrku. Avalikus võrgus ei ole lubatud VPNi välja lülitada.

13.5 Kaugtööks valitud asukoht peab välistama kõrvaliste isikute tööjaama ekraani ja tööprotseduuride ning igasugusel kujul tööalase teabe jälgimise. Avalikes kohtades tuleb eelistada ekraanifiltri kasutamist.

13.6 Video- või telefonikõne ajal tagab kasutaja, et seda ei oleks võimalik pealt kuulata. Lisaks tuleb jälgida, et videokõne ajal ei oleks taustal nähtaval tööalast informatsiooni.

13.7 Avalikest arvutitest (internetikohvikud, raamatukogud jne) ei ole tööalase e-posti lugemine ning varadele juurdepääs lubatud.

13.8 Kaugtööl olles peab kasutaja:

13.8.1 järgima asutuse kehtivat andmekandjate turvalise kõrvaldamise korda;

13.8.2 tagama enne kasutatud andmekandjate ja dokumentide kõrvaldamist tundlike andmete eemaldamise;

13.8.3 mitte hävitama konfidentsiaalsete andmetega andmekandjaid, vaid tooma need tagasi asutusse, kus on olemas vahendid andmekandjate turvaliseks kõrvaldamiseks.

14. Infoturve töötamisel välisriigis (sh välislähetuses)

14.1 Välislähetuses või välisriigis töötamiseks loetakse igasugust tööalase informatsiooni käsitlemist kasutajale väljastatud seadmega väljaspool Eesti Vabariigi territooriumi.

14.2 Välislähetuses või välisriigis viibivad kasutajad lähtuvad tööülesannete turvalisuse tagamisel käesolevast korrast ja ennekõike korra punktis 13 (Kaugtöö) esitatud nõuetest.

14.3 Kasutaja teavitab IT-abi enne välislähetuses või välisriigis töötamise alustamist, kui välisriigis töötamise aeg on 3 kuud või pikem.

14.4 Kasutaja teavitab IT-abi seadme kaasavõtmisest välisriiki, kui reisitakse väljaspoole OECD, EL või NATO liikmesriike.

14.5 Riskiriikidesse reisides ei tohi kaasa võtta seadmeid, milles on seadistatud tööga seotud kontod (sh isiklikud seadmed). Riskiriikide nimekiri on kättesaadav https://kapo.ee/et/content/riigisaladuse-kaitse/ kodulehel.

14.6 Vastav pöördumine tuleb teha IT-abisse esimesel võimalusel, aga mitte hiljem kui 5 tööpäeva enne välisriiki siirdumist.

14.6.1 IT-teenuseosutaja hindab pöördumise alusel riigispetsiifiliste õigusaktide, reisi- ja keskkonnatingimuste täiendavat käsitlusvajadust või täiendavate turbemeetmete rakendamist (sh pääsuõiguste kitsendamist) seadme ja teabe kaitseks.

14.6.2 IT-teenuseosutaja vastab taotlusele hiljemalt 5 tööpäeva jooksul.

14.7 Kasutaja on valmis IT-teenuseosutaja infoturbe seisukohast tulenevalt välisriigis viibimise ajaks ajutiselt asendama igapäevase seadme IT-teenuseosutaja väljastatud eelseadistatud seadmega.

14.8 Seadmeid transporditakse kõikide transpordiviiside puhul käsipagasis, tagades alalise teadmise seadmete hetkeasukohast.

14.9 Seadmete, irdkandjate ja dokumenteeritud teabe kaasavõtmisel välisriiki lähtutakse minimaalsuse printsiibist, mispuhul on kõikide eelloetletud elementide kaasavõtmine töökohustuste täitmiseks vältimatu.

14.10 Kasutaja peab välislähetuses kasutama välisseadmete (nt hiir, klaviatuur, kõrvaklapid jms) kasutamisel juhtmega ühendatavaid välisseadmeid.

14.11 Kui sihtkohariigis ei ole võimalik tagada irdkandjate hävitamist ettenähtud viisil, hoitakse need tagasipöördumiseni alles ning hävitatakse või utiliseeritakse vastavalt ettenähtud turvanõuetele.

14.12 Seadmete ja teabe kaotamise, varguse või mistahes muu kontrolli kaotamise juhtumi korral lähtub kasutaja käesoleva korra punkti 16 (Infoturvaintsidendid) nõuetest, kuid teavitab ühtlasi kohalikku õiguskaitseorganit.

15. IT-abi ja pöördumised

15.1 IT-abi ning pöördumiste kontaktid on toodud lisas 2.

15.2 IT-abi poole pöördutakse taotluse või pöördumisega alljärgnevatel juhtudel:

15.2.1 vahejuhtumid või kahtlused, mis viitavad kindlale või võimalikule soovimatule IT-sündmusele;

15.2.2 probleemid infosüsteemi või IT-varaga;

15.2.3 probleemid seoses õigustega (infosüsteemide juurdepääsu-, lugemis- või muutmisõigused);

15.2.4 AK-teabe kaotsiminek või väärkasutus infosüsteemides.

15.2.5 IT-vara kaotamine, hävimine või vargus (sh isiklik nutiseade, kui sellel on aktiveeritud juurdepääs tööalastele rakendustele);

15.2.6 soov luua või laiendada juurdepääsu tööks vajalikule keskkonnale;

15.2.7 meililistide loomine või muutmine;

15.2.8 vajadus uue või lisafunktsionaalsusega riist- või tarkvara järele;

15.2.9 TTJA-välise (sh isikliku) seadme kasutamine igasuguseks ametialaseks tegevuseks;

15.2.10 vajadus muuta arvutitöökoha (võrgu- ja elektriühenduste valmidus) füüsilist asukohta;

15.2.11 vajadus tellida käesolevas korras toodud turvanõuete täitmiseks vajalikke vahendeid (ekraanifilter, tööjaama kaamera katik jms).

15.3 Eeltoodud loetelu ei ole ammendav ning teavitamisel lähtub kasutaja kahtluse printsiibist (st teavitab esmaste ilmingute ja viidete põhjal ning ei oota kahtluste realiseerumist või kinnituse saamist).

15.4 IT-abi registreerib kõik pöördumised ning suunab olukorra lahendamiseks.

15.5 Pöördumiste ja taotluste lahenduse kulgu saab jälgida, muuta, taasavada või sulgeda IT-abi iseteeninduskeskkonnas.

15.6 Kasutaja aitab igakülgselt kaasa probleemi uurimisele ja lahendamisele.

15.7 Kiireloomulistest probleemidest teavitamiseks kasutatakse prioriteetse suhtluskanalina telefoni teel teavitamist.

16. Infoturvaintsidendid

16.1 Infoturvaintsident on sündmus või mitmete sündmuste jada, mis kahjustab või seab ohtu organisatsiooni turvapoliitikad, turvastandardid või turvapraktikad. Seda määratletakse kui edukalt või potentsiaalselt toime pandud katset kahjustada konfidentsiaalsust, terviklust või käideldavust (CIA: *Confidentiality, Integrity, Availability*) teabekogumis, süsteemis või võrgus.

16.2 Infoturvaintsidente registreeritakse IT-abi (vt lisa 2) kaudu.

16.3 Infoturvaintsidendi lahendamisel lähtutakse IT-teenuseosutaja Turvaintsidentide lahendamise raamistikust (kättesaadav IT-teenuseosutaja abiportaali kaudu).

16.4 Infoturvaintsidentideks loetakse muuhulgas:

16.4.1 infosüsteemi toimimise häirimine, pahavara tuvastamine või viitav kahtlus;

16.4.2 õngitsuskiri (*phising*) või muu manipuleerimisründele (*social engineering*) viitav tegevus;

16.4.3 eksimused käesoleva või teiste TTJA infoturbealaste kordade või protseduuride vastu;

16.4.4 katse või õnnestunud volitamata juurdepääs teabele (sh paberkandjal dokumendid) või selle lubamatu kasutus infosüsteemis;

16.4.5 teadmispiiranguga teabe kaotsiminek või väärkasutus infosüsteemides;

16.4.6 andmekandjate (sh irdkandjate ja paberdokumentide) vargust ja/või hävimist;

16.4.7 infoturbereeglite rikkumine, sh:

16.4.7.1 TTJA kehtivate kordade (käesolev kord, Riigisaladuse kaitse juhendi, TTJA infoturvapoliitika jne) rikkumine;

16.4.7.2 tööalaste andmete kasutamine töövälistes keskkondades (meiliaadress, parool jne).

17. IT-välised intsidendid

17.1 Infoturbeintsidendiks ei loeta füüsilise turbega seotud ja IT-süsteemide väliseid juhtumeid ja kahtlusi. Näiteks on IT-välisteks intsidentideks alljärgnevad:

17.1.1 sellise vara kahjustamine või kaotamine, mida ei käsitleta IT-varana (nt kasutaja läbipääsukaart);

17.1.2 vargus;

17.1.3 volitamata sissepääs TTJA territooriumile, vandalism;

17.1.4 töötajate sihilik füüsilist või teabelist turvalisust kahjustav käitumine;

17.1.5 eksimused või sellealased kahtlused asutusesisese teabega ümberkäimisel asutusevälistes keskkondades.

17.2 Eelloetletud juhtumite korral käitub kasutaja vastavalt TTJA töökorralduse reeglitele ning pöördub lahendamiseks reeglites määratud vastutava isiku või üksuse poole.

18. Teenistussuhete lõppemine või peatamine

18.1 Võimaldamaks seadme tagastamist ja/või infosüsteemidega seotud juurdepääsude muutmist, algatab TTJA personalitöötaja töövoo alljärgnevatel juhtudel:

18.1.1 teenistussuhte lõppemine;

18.1.2 teenistussuhte ajutine peatamine kestusega 90 päeva või kauem;

18.1.3 seadme kasutusvajaduse äralangemine või muu infosüsteemide juurdepääsuõiguste peatamise vajadus.

18.2 Töövoo alusel peatab IT-teenuseosutaja kasutaja konto ja juurdepääsuõigused teenistussuhte lõppemise või peatumise päevast.

18.3 Seadme(te) vahetu tagastamine toimub pöördumisele vastatud IT-abi juhiste alusel.

Lisa 1
TTJA infovahendite kasutamise ja
andmete töötlemise korra juurde

Lisa 1 Kasutatud terminid

- **AK**: „Asutusesiseseks kasutamiseks“. Informatsioon, mis on mõeldud ainult TTJA sisemiseks kasutamiseks ja ei ole avalik.
- **IT-vara**: Infotehnoloogia vara. Igasugune artikkel, ese või olem, mida saab kasutada digitaalteabe hankimiseks, töötluseks, talletuseks ja jaotamiseks. IT-varade hulka kuuluvad: tarkvara, infosüsteemid, infokandjad (füüsilised ja digitaalsed), arvutivõrk, IT-seadmed (füüsilised ja virtuaalsed), litsentsid (ja litsentsitõendid), lepingud, IT-varade halduse varad (vahendid, metaandmed), teenused (enamasti väljastpoolt saadavad), mis on vajalikud IT-varade halduse nõuete täitmiseks, näiteks tarkvara teenusena, riistvara hoolduse, tarkvara toe ja koolituse, failid või muud infosisuga olemid (nn digitaalsed infosisuvarad, näiteks digitaalkujul standardikogud, meediumikogud), teave iseendast, sõltumatult IT riistvara- ja tarkvaravaradest.
- **IT-teenuseosutaja**: Infotehnoloogia teenuseosutaja. Asutuseväline teenusepakkuja, kes tagab IT kasutajatoe, arvutitöökohtade halduse, äritarkvara kasutajatoe ning süsteemihalduse teenused.
- **Kasutaja** on igasugust IT-vara kasutav isik: teenistuja, töötaja, allettevõtja, kolmas pool vms, kes on oma tööülesannete täitmiseks õigustatud kasutama TTJA-le, ja/või IT-teenuseosutajale kuuluvat ja/või renditud IT-vara.
- **Seade või töövahend** on käesoleva korra mõistes igasugune füüsiline IT-vahend, arvuti (koos tarkvaraga), võrguseade, salvestusseade, perifeerseade (klaviatuur, printer, monitor, hiir jms), kommunikatsioonivahend (telefon, peakomplekt, konverentsiseadmed jms) ja turvaseade (näiteks ID-kaardi lugeja või sõrmejäljelugeja), mida kasutatakse tööülesannete täitmiseks.
- **Pääs või ligipääs** on kasutaja või programmi võime olla interaktsioonis varaga, näiteks lugeda või kirjutada andmeid, saata võrgu kaudu sõnumeid, siseneda teatud hoonesse või ruumi, avada teatud kappi.
- **VPN**: Virtuaalne privaatvõrk. Turvaline võrgutehnoloogia, mis võimaldab luua krüpteeritud ühenduse avaliku võrgu kaudu.
- **CIA**: *Confidentiality, Integrity, Availability*. Kolm peamist infoturbe põhimõtet: konfidentsiaalsus, terviklus ja käideldavus.
- **TI**: Tehisintellekt. Arvutisüsteemid, mis suudavad täita ülesandeid, mis tavaliselt nõuavad inimintellekti, nagu visuaalne tajumine, kõnetuvastus, otsuste tegemine ja keele tõlkimine.
- **Yubikey**: Turvavõti, mida kasutatakse kaheastmeliseks autentimiseks. Väike seade, mis pakub tugevat autentimist, ühendades füüsilise turvavõtme ja krüptograafia.
- **Software Center**: Tarkvarakeskus. Keskkond, kus kasutajad saavad paigaldada ja hallata tarkvara, mis on TTJA poolt heaks kiidetud.
- **Bluetooth**: Traadita tehnoloogia andmete edastamiseks lühikeste vahemaade puhul. Kasutatakse seadmete ühendamiseks ja andmete edastamiseks.

- **ID-kaart**: Eesti kodanike isikut tõendav dokument, mida saab kasutada ka digitaalseks autentimiseks ja allkirjastamiseks.
- **DigiDoc**: Krüptokonteiner, mida kasutatakse turvaliseks andmete edastamiseks. Tarkvara, mis võimaldab dokumentide krüpteerimist ja turvalist edastamist.
- ***KeePass***: Paroolihaldustarkvara. Tarkvara, mis võimaldab paroolide turvalist haldamist ja salvestamist.
- ***Phishing***: Õngitsuskiri, manipuleerimisründe vorm. Küberkuritegevuse vorm, kus ründaja üritab petta kasutajat, et saada kätte tundlikku informatsiooni, nagu paroolid ja krediitkaardi andmed.
- ***Social engineering***: Manipuleerimisründe vorm. Meetod, kus ründaja manipuleerib inimesi, et saada kätte tundlikku informatsiooni või panna neid tegema teatud tegevusi.
- **7-zip**: Failipakkija tarkvara, mida kasutatakse failide krüpteerimiseks. Tarkvara, mis võimaldab failide pakkimist ja krüpteerimist turvaliseks edastamiseks.

Lisa 2
TTJA infovahendite kasutamise ja
andmete töötlemise korra juurde

Lisa 2: IT-teenuseosutaja kontaktid

TTJA IT-teenuseosutaja on Keskkonnaministeeriumi Infotehnoloogiakeskus (edaspidi KeMIT).

IT-abi teenus on kättesaadav **tööpäeviti 08:00-17:00**.

IT-abi üldkontaktid:

KEMITi iseteeninduspordaal**: https://help.kemit.ee**

Telefon: **626 5000**

E-posti aadress: **help@kemit.ee**