

Sotsiaalkindlustusamet infoturbe reeglid

1. Üldsätted

- 1.1. Käesolevad Sotsiaalkindlustusameti (edasipidi SKA) infoturbe reeglid on kohustuslikud järgimiseks SKA-ga lepingulistes suhetes olevatele isikutele (edasipidi kasutaja):
 - 1.1.1. kes omavad iseseisvat ligipääsu SKA tööruumidele;
 - 1.1.2. kes kasutavad lepingu täitmiseks isiklikku arvutit ja omavad ligipääsu SKA arvutivõrgule;
- 1.2. Kasutaja on kohustatud järgima SKA infoturbe reegleid ulatuses, mis vastab tema ligipääsuõigustele, kasutatavale varale ja teenustele vastavalt punktides 1.1.1.-1.1.2. kirjeldatule.
- 1.3. Käesolevate reeglite kasutajale kohalduva mistahes punkti rikkumine võib kaasa tuua lepingu lõpetamise.

2. Infoturbealased koolitused

- 2.1. Kasutajad on kohustatud esmakordsel arvutivõrgule ligipääsu saamisel läbima SKA poolt kasutatavas e- õppe keskkonnas koolituse SKA määratud tähtaja jooksul. Edaspidi tuleb koolitus läbida vähemalt üks kord aastas hiljemalt 30. novembril.
- 2.2. Kasutajatel, kes ei ole koolitust tähtjaks läbinud, peatatakse kaugtöö võimalus VPN sulgemisega.

3. Infoturbe nõuded arvutiga töötamisel

- 3.1. Kasutaja peab:
 - 3.1.1. täitma kõiki SKA infoturbe nõudeid nii SKA territooriumil ja arvutivõrgus kui neist väljaspool SKA-le teenust osutades;
 - 3.1.2. järgima ITabi, SKAtoe ja lepingu kontaktisiku saadetud korraldusi rakenduste kasutamiseks;
 - 3.1.3. esimesel võimalusel teavitama e-kirja või telefoni teel lepingu kontaktisikut, itabi@tehik.ee ja skatugi@sotsiaalkindlustusamet.ee rikestest ja muudest infotehnoloogiliste teenuste kasutamist takistavatest asjaoludest, sh IT vara vargusest, kaotamisest või hävimisest;
 - 3.1.4. kasutama isiklikus arvutis lepingu täitmisega seotud tegevusteks eraldi isiklikku kasutajakontot, millele ligipääs on ainult temal endal ja mitte kasutama selleks vaikimisi administraatori kontot.
 - 3.1.5. teenuse osutamise välisel ajal hoidma arvuti suletuna, kasutajakontolt välja logituna või kasutama talveune funktsiooni; arvutist ajutiselt eemaldudes lukustama selle (vajutades näiteks üheaegselt Windows logo klahv + L või klahvikombinatsiooni Ctrl+Alt+Del), eemaldama ID kaardi;
 - 3.1.6. sisestama parooli ja PIN koodid kolmandatele isikutele varjatult;

- 3.1.7. tagama, et arvutiekraanil (sh lisamonitoril) kuvatav teave ei oleks nähtav kõrvalistele isikutele ning vajadusel muutma arvuti või monitori asendit ning kasutama ekraani andmekaitsefiltrit;
- 3.1.8. tagama, et telefoni- ja videokonverentsid, mis sisaldavad konfidentsiaalset teavet, ei oleks kuuldavad kõrvalistele isikutele, ning kasutab vajaduse korral kõrvaklappe, et tagada vestluse privaatsus.
- 3.1.9. looma andmeside üksnes turvaliste kanalite kaudu, kasutades selleks püsiühendust lepingu alusel internetiteenuse pakkujaga, avalikus ruumis viibides mobiilset andmesidet isikliku SIM kaardi abil ja vältima avalike WiFi võrkude kasutamist;
- 3.1.10. vältima juhtmeta ühenduste tarbetut aktiveerimist;
- 3.1.11. isikliku püsiühenduse puhul muutma ruuteri tehase antud nime ja salasõna ning ruuteri WiFi nimetuses mitte kasutama nimesid ja muud endaga seostatavat;
- 3.1.12. tagama, et ruuteril oleks viimased turvapaigad, vananenud seadmed välja vahetama;
- 3.1.13. isikliku püsiühenduse WiFi seadistamisel kasutama vähemalt WPA2 protokollit;
- 3.1.14. vältima paberkandjal dokumentidega töötamist, sh printerite kasutamist. Kui see ei ole võimalik, siis võtma kasutusele meetmed paberdokumentide konfidentsiaalsuse tagamiseks, seal hulgas transpordil, hoiustamisel, hävitamisel.
- 3.1.15. Enne isikliku arvuti hooldusesse andmist veenduma, et arvutis ei sisalduks lepingu täitmisega seotud isikuandmeid või muid konfidentsiaalseid dokumente ja et oleks blokeeritud ligipääs SKA e-posti aadressile.
- 3.2. Kasutajal on keelatud:
 - 3.2.1. salvestada isikuandmeid arvuti töölauale;
 - 3.2.2. sisestada tehisintellektil põhinevatesse vestlusassistentidesse isikuandmeid ja muud konfidentsiaalset teavet;
 - 3.2.3. edastada interneti kaudu (ka läbi sotsiaalmeedia, sõnumivahetusrakenduste, foorumite, blogide, kommentaaride jne) salastamata (krüpteerimata) teavet, mis ei ole mõeldud avalikuks kasutamiseks või mis võib kahjustada SKA mainet;
 - 3.2.4. kasutada arvutivõrgu skaneerimist, võrguliikluse pealtkuulamist või muid võrguliiklust jälgivaid või segavaid rakendusi või seadmeid;
 - 3.2.5. lepingu täitmiseks vajaliku või lepingu täitmisel saadud informatsiooni edastamine isiklike kontaktandmete kaudu (nt e-post, suhtlusrakendused), kui lepingus ei ole kokku lepitud teisiti;
 - 3.2.6. väljastada juurdepääsupiiranguga informatsiooni lepinguga mitte seotud eesmärkidel;
 - 3.2.7. hoida ja töödelda isikuandmeid ja muud konfidentsiaalset teavet eraelus kasutatavates avalikes pilveteenustes;
 - 3.2.8. lepingu täitmiseks kasutatavas IT-varas laadida internetist alla mittelegaalset tarkvara, kasutada kaheldavate kasutustingimustega rakendusi nt DeepSeek;

4. Isiklike sülearvutite ja mobiilsideseadmete kasutamine

- 4.1. Kasutaja peab arvestama, et seadet on võimalik kasutada väljaspool SKA turvatud arvutivõrku ja territooriumi, mistõttu see teeb seadmest kõrgendatud ohu allika ning paneb selle kasutajale lisavastutuse.
- 4.2. Sülearvuti kasutaja kohustub:
 - 4.2.1. mitte jätta sülearvutit magnetvälja (näiteks varjestamata kõlarite lähedusse), otsese päikesekiirguse või kõrge temperatuuri kätte, samuti tolmusesse või niiskesse keskkonda;

- 4.2.2. transportima sülearvutit vaid selleks ettenähtud kotis ning reisimisel kandma sülearvutit käsipagasina; transportimisel lülitama sülearvuti välja või kasutama talveune funktsiooni;
- 4.2.3. võimaluse korral lennujaamade jms turvakontrollis laskma sülearvutile (koos kotiga) teha läbivalgustuse asemel käsitsi läbivaatus;
- 4.2.4. transportimisel eemaldama ID-kaardi sülearvutist ja mitte hoidma seda sülearvuti kotis, et vähendada kaotamise korral riski volitamatuks autentimiseks.
- 4.3. Mobiilsideseadmes töölase e-kirjavahetuse, kalendri ja MS Teams kasutamisel peab kasutaja:
 - 4.3.1. seadistama mobiilsideseadmes automaatse vähemalt kuuekohalise PIN koodiga ekraaniluku, mis lukustub hiljemalt ühe minuti möödumisel jõudeolekust. PIN koodis on keelatud kasutada lihtsasti arvatavaid või järjestikuseid kombinatsioone. Lubatud on biomeetria kasutamine;
 - 4.3.2. tagama, et tema kasutataval mobiilsideseadmel on Android või IOS operatsioonisüsteemisüsteemi versioon, millel on kehtiv tootjapoolne tarkvarauuenduste tugi, soovitatavlt viimane operatsioonisüsteemi versioon;
 - 4.3.3. hoidma seadme turvauuendused viimases seisus, paigaldades seadme- või operatsioonisüsteemi tootja väljastatud tarkvara turvauuendusi vähemalt ühe kalendrikuu jooksul alates nende uuenduste väljastamisest ja kontrollima regulaarselt turvauuenduste installeerumist;
 - 4.3.4. paigaldama mobiilirakendusi ainult usaldusväärsetest ametlike tootjate tarkvaravaramutest (Google Play, App Store, AppGallery);
 - 4.3.5. WiFi, infrapuna-, bluetooth- ja NFC liidesed välja lülitama ajal, kui neid ei kasutata;
 - 4.3.6. mobiilsideseadme ühendamisel väliste seadmetega bluetooth kaudu kasutama turvalist ühendamist paariskoodiga, kasutama krüpteeritud ühendust;
 - 4.3.7. omama ülevaadet, kuhu salvestatakse mobiilsideseadme varundamise käigus andmed ja veenduma, et ei salvestataks eraelus kasutatavatesse avalikesse pilveteenustesse AK informatsiooni sisaldavaid faile;
 - 4.3.8. mobiilsideseadme kaotamise või varastamise korral koheselt teavitama sellest ITabi ja paluma kaughalduse teel tühjendada seade. Teavitama intsidendist SKAtuge ja lepingu kontaktisikut;
 - 4.3.9. enne isikliku mobiilsideseadme müümist, utiliseerimist, edasikinkimist, väljavahetamist, parandusse või garantiisse viimist kustutama seadme mälu sisu ja sätted nii, et poleks võimalik asutuse andmetele juurdepääsu saada (factory reset). Kui mobiilsideseadmes oli ligipääs töölasele kirjavahetusele ja kalendrile, teavitama ITabi vajadusest eemaldada seade SKA mailiteenust kasutavate seadmete nimekirjast;
- 4.4. Kasutajal on keelatud:
 - 4.4.1. salvestada vestlusi ilma kõigi osapoolte nõusolekuta;
 - 4.4.2. kasutada isiklikke mobiilsideseadmeid kliendiandmeid sisaldavate fotode ja videoklippide tegemiseks;
 - 4.4.3. anda oma mobiilsideseadet kasutamiseks kolmandatele isikutele ja avaldada neile oma mobiilsideseadme PIN koodi;
 - 4.4.4. ühendada mobiilsideseadet andmeedastusvõimekusega kaabliga võõra arvuti külge, sh aku laadimiseks ja kasutada mobiilsideseadme laadimiseks avalikus ruumis olevaid ja tundmatuid USB pesasid;
 - 4.4.5. kasutada mobiilsideseadet, millele enam turvauuendusi ei väljastata.

5. Autentimine ja salasõnad

- 5.1. Kasutajal peab olema ID-kaart, nutiseade ja sellesse installeeritud autentimiskirjend Microsoft Authenticator.
- 5.2. Kasutaja peab sisenema arvutivõrku ja infosüsteemidesse ainult temaga isikustatud e-ID vahenditega, sh isiklikult talle antud kasutajatunnuse ja salasõnaga.

- 5.3. Kasutaja vastutab salasõna saladuses hoidmise eest ja peab tagama, et tema autentimisvahendite abil ei pääse arvutivõrku ja rakendustesse kolmandad isikud. Vajadusel tuleb kasutada paroolihaldurit KeePass.
- 5.4. Salasõna peab:
 - 5.4.1. koosnema suur- ja väiketähtede ning numbrite ja sümbolite kombinatsioonist;
 - 5.4.2. olema vähemalt 16 tähemärki pikk;
 - 5.4.3. olema valitud selliselt, et seda on võimalik meelde jätta, kuid pole lihtne ära arvata.
- 5.5. Salasõna ei tohi olla:
 - 5.5.1. koostatud vaid ühesugusustest sümbolitest ega klaviatuurijärjestuses tähtedest või numbritest;
 - 5.5.2. tuletatud isiklikust informatsioonist, mida keegi võib hõlpsasti ära arvata, näiteks nimi, kasutajanimi, oma telefoninumber, isikukood vms;
 - 5.5.3. lihtsasti tuletatav eelnevalt kasutatud salasõnadest;
 - 5.5.4. koostatud üksnes sõnaraamatus sisalduvatest sõnadest;
 - 5.5.5. kasutuses korduvalt erinevates rakendustes, sealhulgas kolmandate osapoolte veebisaitidel ja teenustes.
- 5.6. Kui kasutaja kahtlustab, et salasõna on saanud teatavaks kolmandatele isikutele, peab ta kohe selle muutma salasõna või paluma IT-abi või vastutavat infosüsteemi kasutuse haldurit salasõnaga seotud kasutajaõigused tühistada.

6. SKA e- posti kasutamine

- 6.1. SKA e-posti aadressi kasutatakse ainult lepingu täitmisega seotud kirjavahetuseks. SKA e- posti kasutamine on keelatud:
 - 6.1.1. suhtlemiseks eraelulistel ja ärilistel eesmärkidel, seoses kolmandale isikule teenuse osutamisega või ametiasutustega, mis ei ole seotud SKA teenuse osutamisega;
 - 6.1.2. tarbijamängude mängimiseks;
 - 6.1.3. isiklike kommertsteadete tellimiseks;
 - 6.1.4. eraelus kasutatavates veebikeskkondades registreerumiseks;
 - 6.1.5. tegevusteks, mis võivad põhjustada hulgalise kommertsteadete ja rämpsposti saatmise SKA e-posti aadressile;
 - 6.1.6. lepingu täitmisel saadud info, sh isikuandmete ja kirjade edasi saatmiseks enda isiklikule e-posti aadressile (seal hulgas suunamine), muudesse isiklikesse suhtluskanalitesse või lepingu täitmisega mitte seotud kolmandatele isikutele, samuti salvestada kirju eraelus kasutatavatesse avalikesse pilveteenusesse;
- 6.2. Kasutajal on keelatud klikkida kahtlusi tekitava pealkirjaga või kahtlustäratavalt e-posti aadressilt saabunud e-kirjas olevatel linkidel ning avada manuseid, kui pole veendunud nende turvalisuses. Kahtlaste e-kirjade kontrollimiseks tuleb edastada need otse ITAbile itabi@tehik.ee kas kontrollimiseks või rämpspostifiltrisse lisamiseks ja enda e-postkastist kustutada.
- 6.3. E-kirjade saatmisel tuleb jälgida, et e-kirja teemariida ei sisaldaks isikuandmeid ning kirjad ei sisaldaks isikuandmeid ebavajalikul hulgal.

7. Suhtlusteenuste kasutamine

- 7.1. Avalike suhtlusrakenduste, suhtluskanalite, koostööplatvormide ja eraelus kasutatavate pilveteenuste kasutamine isikuandmete töötlemiseks krüpteerimata kujul on keelatud.
- 7.2. Kasutajad on kohustatud järgima sotsiaalmeedia kasutamisel SKA kommunikatsioonipõhimõtteid ja sotsiaalmeedia kasutamise head tava ning jälgima, et nende loodud sotsiaalmeediagruppides ei käsitletaks teemasid, mis võivad kahjustada SKA mainet. Vajadusel palub kasutaja lepingu kontaktisikul neid põhimõtteid ja tavaid tutvustada.

- 7.3. Kui kasutaja osalusega sotsiaalmeedia grupis jagatakse SKAd või riiki kahjustavaid soovitusi või arutatakse tegevusi, mis võivad olla süüteo tunnustega, on kasutaja kohustatud sellest teavitama viivitamatult SKAtuge ja lepingu kontaktisikut.

8. SKA ruumide kasutamine ja füüsiline turve

- 8.1. SKA kontorites kasutatavad ruumid on jagatud tinglikult klienditsooniks ja töötsooniks. Klienditsoon on ala, kuhu võivad hoone lahtioleku aegadel siseneda kõik isikud. Töötsooni kuuluvad ainult kasutajatele mõeldud tööruumid, sh vestlustoad, kus on kolmandatel isikutel lubatud viibida ainult kasutajate vastutusel.
- 8.2. Kasutajatele väljastatud pääsuvahenditele on keelatud lisada informatsiooni, millest saavad nende kaotamise korral kolmandad isikud tuletada hoonet või ruume, millesse pääsuvahendiga on ligipääs.
- 8.3. Kasutaja on kohustatud talle SKA lepingu täitmiseks väljastatud pääsuvahendit kasutama ainult isiklikult. Pääsuvahendi edastamine kolmandatele isikutele on keelatud, sõltumata sellest, kas pääsuvahendi on kasutajale väljastanud SKA või SKA partnerasutus.
- 8.4. Pääsuvahendi kaotamise korral peab kasutaja sellest teavitama viivitamatult SKAtoe kaudu kinnisvara- ja haldustalitust, lisades teatele info, millal ja kus viimati pääsuvahendit kasutas.
- 8.5. Tööruumist viimasena lahkuv kasutaja vastutab selle eest, et ruumi aknad oleks suletud ja tööruumi ning klienditsooni vaheline uks oleks lukustatud.
- 8.6. Kasutaja kohustus on jälgida töötsooni sisenemisel või sealt lahkumisel, et temaga koos ei siseneks töötsooni kolmandad isikud.
- 8.7. Kasutaja kohustus on tagada, et tema poolt töötsooni lubatud külalised ei jääks ilma järelevalveta.

9. Turvateadlikkuse kontroll ja monitooring

- 9.1. IT vara ja andmete sihipärase kasutamise kontrollimiseks või intsidendi lahendamise eesmärgil on SKA nõunikul sisekontrolli valdkonnas ja infoturbspetsialistidel õigus tutvuda kasutaja teadmisel tema tööalase e-postkasti sisuga. Kasutaja nõusolekut küsitakse e-posti kausta „isiklik“ sisuga tutvumiseks.
- 9.2. Turvanõuete täitmist kontrollib SKA infoturbspetsialist, kelle nõudmisel tuleb kasutajal tõendada kohustuslike turvameetmete rakendatust.
- 9.3. SKA infoturbe reeglite rikkumise või infosüsteemide väärkasutuse kahtluse tekkimisel peatatakse kasutusõigused koheselt kuni asjaolude selgitamiseni.
- 9.4. Lepingu kontaktisiku, SKA infoturbspetsialisti või andmekaitsespetsialisti nõudmisel tuleb lõpetada ebaseaduslik andmetöötlus või muu infoturbe nõuetele mittevastav tegevus.
- 9.5. SKA-l on õigus ilma eelneva hoiatuseta peatada kasutaja juurdepääs teenustele, kui ilmneb või on tekkinud põhjendatud kahtlus, et kasutaja tegevus on ohuks arvutivõrgule ja infosüsteemidele.
- 9.6. Õiguste peatamisest või piiramisest teavitatakse kasutajat ja lepingu kontaktisikut.

10. Konfidentsiaalsuskohustus

- 10.1. Kasutaja peab lähtuma põhimõttest, et lepingu täitmisega saadud isikuandmed ja muu info on konfidentsiaalne ja kasutatav ainult lepingu täitmiseks.
- 10.2. Konfidentsiaalsena on käsitletav ka SKA siseinfot sisaldav SKA sisene kirjavahetus, sh teave, mis puudutab SKA töökorralduslikke küsimusi.
- 10.3. Konfidentsiaalsuskohustus on tähtajatu, st kehtib ka peale SKA-ga lepingulise suhte lõppemist.