KINNITATUD
rektori 02.06.2020
käskkirjaga nr 1.1-2/354

ISIKUANDMETE TÖÖTLEMISE KORD

I ÜLDSÄTTED

1.1. Isikuandmete töötlemise kord (edaspidi kord) sätestab isikuandmete töötlemise põhimõtted Sisekaitseakadeemias (edaspidi akadeemia), andmesubjekti õigused ja akadeemia kohustused isikuandmete töötlemisel.

1.2. Akadeemia töötleb isikuandmeid lähtudes Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmäärusest (Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) ja isikuandmete kaitse seadusest, korrast, Sisekaitseakadeemia teabehalduskorrast, dokumentide loetelust ning muudest asjakohastest õigusaktidest.

1.3. Kord avaldatakse akadeemia veebilehel. Lisaks avaldatakse veebilehel korral põhinev Sisekaitseakadeemia privaatsuspoliitika, kus selgitatakse isikuandmete töötlemise tingimusi.

1.4. Akadeemia tegevus on avalik, välja arvatud juhul, kui õigusaktidega on sätestatud teisiti.

1.5. Isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest.

1.6. Korras kasutatakse mõisteid eelkõige alljärgnevas tähenduses:

1.6.1. isikuandmete töötleja/vastutav töötleja – akadeemia ja tema töötaja, kes töötleb isikuandmeid akadeemia ülesandel;

1.6.2. andmesubjekt – tuvastatud või tuvastatav füüsiline isik, kelle isikuandmeid akadeemia töötleb, sh taseme- ja täiendusõppes õppija, konverentsil osaleja, töötaja, teenuse osutaja, kodulehe külastaja, avalduse esitaja;

1.6.3. isikuandmed – akadeemia ülesannete täitmise ja kaasnevate tegevustega tegelemise käigus tekkivad andmed tuvastatud või tuvastatava andmesubjekti kohta. Isikuandmeteks on mis tahes andmed, mis akadeemial andmesubjekti kohta teada on, sõltumata sellest, millisel kujul või millises vormis need andmed on, sealhulgas ees- ja perekonnanimi, isikukood, telefoni- või mobiiltelefoninumber ning postiaadress, arvuti IP aadress jt andmed;

1.6.4. eriliiki isikuandmed – poliitilised vaated, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed; etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed; andmed terviseseisundi või puude kohta; andmed pärilikkuse informatsiooni kohta; biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geeniandmed); andmed seksuaalelu kohta; andmed ametiühingu liikmelisuse kohta; andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist;

1.6.5. kolmas isik – iga füüsiline või juriidiline isik, kes ei ole andmesubjekt, vastutav töötleja, volitatud töötleja ega nimetatud isikute töötaja;

1.6.6. volitatud töötleja – isik, kes töötleb isikuandmeid akadeemia ülesandel seaduse, seaduse alusel antud õigusakti või kirjaliku lepingu alusel.

II ISIKUANDMETE TÖÖTLEMISE EESMÄRK

2.1. Akadeemia töötleb isikuandmeid üksnes õiguspäraste eesmärkide saavutamiseks ning ulatuses, mis on vajalik akadeemia põhimäärusest tulenevate ülesannete ja tegevuste ning kaasnevate tegevuste elluviimiseks.

III ISIKUANDMETE TÖÖTLEMINE

3.1. Isikud, kelle isikuandmeid akadeemias töödeldakse on peamiselt:

3.1.1. andmesubjekt, kelle andmeid on vaja töödelda tulenevalt akadeemia põhimääruses sätestatud ülesannete ja tegevuste ning põhitegevusega kaasnevate tegevuste elluviimiseks;
3.1.2. kolmandad isikud, kes on andmesubjekti poolt määratud kontaktisikuks või kelle kohta avaldab andmesubjekt teavet seoses korra punktis 3.1.1 nimetatuga.

3.2. Akadeemias töödeldavate isikuandmete, sh eriliigiliste isikuandmete koosseisu kuuluvad peamiselt:

3.2.1. isikut tuvastavad andmed, s.h nimi, isikukood, rahvus, emakeel;
3.2.2. kontaktandmed (mobiiltelefoni või telefoninumber, aadress);
3.2.3. andmesubjekti poolt määratud kontaktisiku andmed (mobiiltelefoni või telefoninumber, aadress);
3.2.4. teave isiku perekonna ning sotsiaalse tugivõrgustiku kohta (perekonnaseis, laste arv);
3.2.5. andmed hariduse, harrastuste, sõiduki ja eluviiside ning tööalase tegevuse kohta.
3.2.6. töövõime kaotuse protsent ja puude raskusaste arstliku ekspertiisi otsuse alusel;
3.2.7. teave isiku terviseseisundi kohta;
3.2.8. õigusaktides nimetatud teenistusse sobimise otsustamiseks vajalik teave;
3.2.9. õpisooritused ja neile antud hinnangud;
3.2.10. sisseastumiseks tehtud sooritused ja neile antud hinnangud;
3.2.11. õppearendus-, teadus-, arendus- ja innovatsioonitegevuse elluviimiseks vajalik teave;
3.2.12. muu akadeemia põhimäärusest tulenevate ülesannete ja tegevuste ning põhitegevustega kaasnevate tegevuste elluviimiseks vajalik teave.

3.3. Isikuandmete töötlemisel lähtub akadeemia järgmistest põhimõtetest:

3.3.1. seaduslikkuse põhimõte – isikuandmeid võib koguda vaid ausal ja seaduslikul teel ning igasuguseks isikuandmete töötlemiseks peab olema alus;
3.3.2. eesmärgipärasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas;
3.3.3. minimaalsuse põhimõte – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks;
3.3.4. kasutuse (säilitamise) piiramise põhimõte – isikuandmeid võib kasutada üksnes eesmärgipäraselt ja eesmärgi saavutamiseni, eesmärgist tuleneb ka säilitamistähtaeg. Isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;
3.3.5. õigsuse ja andmete kvaliteedi põhimõte – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks;
3.3.6. turvalisuse põhimõte – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest;
3.3.7. vastutuse ja läbipaistvuse põhimõte – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist.

3.4. Lähtudes korras toodud isikuandmete töötlemise põhimõtetest akadeemia:

3.4.1. töötleb isikuandmeid, sh edastab neid kolmandale isikule ja/või kolmandasse riiki, ainult seaduse, lepingu, nõusoleku või õigustatud huviga määratud eesmärgil ja ulatuses järgides kõiki andmekaitset reguleerivaid õigusakte;

3.4.2. tagab isikuandmete kaitse läbi tõhusate organisatsiooniliste, füüsiliste ja infotehnoloogiliste turvameetmete (nt edastab kolmandale isikule andmeid krüpteeritult) ning range konfidentsiaalsus- ja turvalisusreeglistiku, kaitstes isikuandmeid igasuguse õigustamatu kasutamise eest;

3.4.3. töötleb teadusuuringu tegemise käigus eriliigilisi isikuandmeid üksnes siis, kui uuringu isikuandmete töötlemise tingimuste täitmist on eelnevalt kontrollinud asjaomase valdkonna eetikakomitee või kui teadusvaldkonnas puudub eetikakomitee, siis Andmekaitse Inspektsioon;

3.4.4. tunnistab isikuandmeid sisaldava teabe asutusesiseseks kasutamiseks mõeldud teabeks ja kehtestab sellele juurdepääsupiirangu;

3.4.5. töötleb isikuandmeid paberkandjal või infosüsteemis. Infosüsteem, milles isikuandmeid töödeldakse ning dokumentidele kehtestatud asukohad, juurdepääsupiirangud ja säilitustähtajad on nimetatud akadeemia teabehalduskorras ja dokumentide loetelus;

3.4.6. kustutab või hävitab viivitamata isikuandmeid, mida akadeemia enam ei vaja, sh säilitustähtaja möödumise tõttu;

3.4.7. võimaldab ligipääsu isikuandmetele ainult vastava juhendamise saanud töötajatele ja võlaõigusliku lepingu alusel külalisõppejõududele ning muudele volitatud isikutele, kellel on õigus isikuandmeid töödelda vaid ulatuses, mis on vajalikud isikuandmete töötlemise eesmärkide saavutamiseks;

3.4.8. ei väljasta isikuandmeid kolmandatele isikutele, välja arvatud juhul kui andmete väljastamise kohustus tuleneb seadusest või andmesubjekt on andnud selleks loa. Isikuandmete edastamine või nendele juurdepääsu võimaldamine andmete töötlemiseks kolmandale isikule on lubatud andmesubjekti nõusolekuta juhul, kui:

3.4.8.1. isikuandmed laekuvad ja neid töödeldakse isikustamata kujul (nt anonüümsed küsitlused);

3.4.8.2. üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada;

3.4.8.3. isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks.

3.4.9. avalikustab avaliku teabe seaduse alusel teabe ja dokumendid oma kodulehel või edastab isikule teabe ja/või dokumendi teabenõude alusel. Juurdepääsu piiramisel lähtub avaliku teabe seaduse §-st 35. Andmesubjektiga seotud dokumendid on valdavalt juurdepääsupiiranguga, avalikus dokumendiregistris kasutatakse andmesubjekti nime asemel initsiaale, dokumendi pealkiri näidatakse kujul, mis ei võimalda aimata selle täpsemat sisu ja seal ei kuvata juurdepääsupiiranguga dokumendi sisu. Juurdepääsupiirangutega on võimalik tutvuda dokumentide loetelus. Kui esineb ilmne avalik huvi, siis võib avalikustada eraisikuga peetava kirjavahetuse ja muude teabe või dokumentide asjaolusid (avaliku teabe seaduse § 30 lg 4, § 38 lg 1). Muuhulgas jätame endale õiguse, kui isik viib ise info avalikkuse ette, anda vajadusel avalikkusele oma tegevuse kohta selgitusi;

3.4.10. avalikkuse teadlikkuse suurendamiseks kajastab akadeemia uudiseid ja fotosid oma ülesannete täitmisest oma veebilehel, siseveebis ning muudes meediakanalites. Uudiseid koostades hoidutakse asjaosaliste eraelu ülemääraselt riivamast;

3.4.11. edastab isikuandmeid andmesubjektile või kolmanda isikule avalduse, lepingu, seaduse või seaduse alusel antud õigusakti alusel. Isikuandmeid sooviv isik peab suutma tõendada oma isikusamasust ja andmete saamise õigust. Avaldus ja leping isikuandmete edastamiseks peavad olema kirjalikus vormis. Kui akadeemia ei ole veendunud, et andmete edastamine on õigustatud, andmeid ei väljastata. Avaldus rahuldatakse või sellele esitatakse põhjendatud keeldumine seadusega ettenähtud tähtaja jooksul. Kui avaldust on vaja täpsustada või kui

isikuandmete töötlus on aeganõudev, võib akadeemia avalduse täitmise tähtaega pikendada informeerides sellest avalduse esitajat. Akadeemia võib keelduda teabe edastamisest, kui see võib:

3.4.11.1. takistada või kahjustada süüteo tõkestamist, avastamist või menetlemist või karistuse täideviimist;
3.4.11.2. kahjustada teise isiku õigusi ja vabadusi;
3.4.11.3. ohustada riigi julgeolekut;
3.4.11.4. ohustada avaliku korra kaitset;
3.4.11.5. takistada ametlikku uurimist või menetlust.

3.4.12. tagab andmesubjektilt isikuandmete saamisel talle järgmise teabe esitamise:

3.4.12.1. andmed teabe vastutava töötleja kohta, selle esindaja nimi ja kontaktandmed, vajadusel andmekaitsespetsialisti kontaktandmed;
3.4.12.2. isikuandmete töötlemise eesmärk ja õiguslik alus;
3.4.12.3. vajadusel teave kavatsusest edastada isikuandmed kolmandale isikule ja/või kolmandasse riiki ning teave kaitse piisavuse või kaitsemeetmete sobivuse kohta;
3.4.12.4. andmete säilitamise tähtajad või nende määramise kriteeriumid;
3.4.12.5. teave andmesubjekti õigusest nõuda isikuandmete parandamist, kustutamist, töötlemise piiramist, andmete ülekandmist, õigusest nõusolek igal ajal tagasi võtta ning õigusest esitada kaebus Andmekaitse Inspektsioonile;
3.4.12.6. kui isikuandmeid saadakse mujalt kui andmesubjektilt, teave isikuandmete päritoluallikast.

3.5. Isikuandmete töötlemisega seoses andmesubjekt:

3.5.1. võib isikuandmete töötluseks antud nõusoleku igal ajal tagasi võtta, esitades vastavasisulise avalduse punktis 3.5.9 näidatud e-posti aadressile, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud isikuandmete töötlemise seaduslikkust;
3.5.2. võib saada akadeemialt kinnitust selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse. Kui töödeldakse, siis saada teavet töödeldud isikuandmete, nende töötlemise eesmärkide ja liikide kohta. Kui teavet edastati kolmandatele isikutele ja/või kolmandatesse riikidesse, siis informatsiooni ka selle kohta;
3.5.3. võib nõuda tema ebaõigete isikuandmete parandamist, mittetäielike andmete täiendamist, isikuandmete töötlemise piiramist vastavalt õigusaktidele;
3.5.4. võib nõuda teda käsitlevate isikuandmete kustutamist, väljaarvatud juhul, kui akadeemial või kolmandal isikul on õiguslik alus nende isikuandmete töötlemiseks;
3.5.5. võib nõuda isikuandmete ülekandmist vaid siis, kui see on tehniliselt teostatav, st kui kaks süsteemi suudavad omavahel turvaliselt suhelda ja vastuvõttev süsteem on tehniliselt suuteline sissetulevaid andmeid vastu võtma;
3.5.6. võib esitada vastuväiteid isikuandmete töötlemise suhtes kui see toimub akadeemia või kolmanda isiku õigustatud huvi alusel. Välja arvatud juhul, kui on tõendatud, et andmeid töödeldakse mõjuval õiguspärasel põhjusel, mis kaalub üles andmesubjekti huvid, õigused ja vabadused, või kui andmeid töödeldakse õigusnõuete koostamise, esitamise või kaitsmise eesmärgil;
3.5.7. võib keelata isikuandmete töötlemise otseturunduse eesmärgil, sealhulgas profiilianalüüsi suhtes sel määral, mil see on seotud kõnealuse otseturundusega;
3.5.8. võib saada teavet tema isikuandmetega seotud rikkumistest, kui rikkumine kujutab endast tõenäoliselt suurt ohtu tema õigustele ja vabadustele. Akadeemia peab vastavas teates selges ja lihtsas keeles kirjeldama rikkumise laadi ning esitama andmekaitsespetsialisti või muu pädeva isiku nime ja kontaktandmed või kirjeldama rikkumise võimalikke tagajärgi või informeerima võimaliku kahjuliku mõju leevendamiseks rakendatud/kavandatud meetmetest;

3.5.9. võib isikuandmete töötlemisega seonduvate küsimuste tekkimisel või kaebuse esitamiseks pöörduda akadeemia poole kirjalikult teel alljärgnevatel kontaktidel Kase 61, Tallinn 12012 või e-posti aadressil andmekaitsespetsialist@sisekaitse.ee.

IV ISIKUANDMETE TURVAMEETMED

4.1. Isikuandmete kaitseks rakendatavate turvameetmete eesmärk on kaitsta:

4.1.1. juhusliku või tahtliku volitamata muutmise eest;
4.1.2. juhusliku hävimise ja tahtliku hävitamise eest ning õigustatud isikule andmete kättesaadavuse takistamise eest;
4.1.3. volitamata töötlemise eest.

4.2. Akadeemia poolt töödeldavad isikuandmed on peamiselt paberkandjal dokumentidena, digitaalkujul andmekandjatel või akadeemia teabehalduskorras nimetatud infosüsteemis sh akadeemia dokumendihaldussüsteemis, riigihangete registris, täienduskoolituse infosüsteemis, õppeinfosüsteemis, riigi personali- ja palgaarvestuse andmekogus, millele ligipääsemiseks kasutatakse unikaalseid kasutajatunnuseid ja paroole ning on tagatud, et vastava infosüsteemi kasutajal (akadeemia töötajal) on ligipääs üksnes tema tööks vajalikele andmetele.

4.3. Eriliigilisi isikuandmeid sisaldavaid paberdokumente või teisaldatavaid andmekandjaid hoitakse ja säilitatakse akadeemias lukustatavates kappides või akadeemia arhiivis.

4.4. Paberkandjal olevate eriliigiliste isikuandmete töötlemise ja kasutamise kohta peetakse logi või registrit. Isikud, kellele on lubatud eriliigiliste isikuandmete töötlemine, peavad tagama, et iga eriliigiliste isikuandmete kasutamine oleks vastavas logis või registris registreeritud. Nimetatud registrisse kantakse järgmised andmed:

4.4.1. akadeemia töötaja, kes eriliigilisi isikuandmeid töötleb;
4.4.2. info kasutatud eriliigiliste isikuandmete kohta;
4.4.3. kuupäev, millal eriliigilisi isikuandmeid sisaldavad dokumendid võeti või töödeldi ning töötaja allkiri selle kohta;
4.4.4. dokumentide tagastamise kuupäev ja töötaja allkiri tagastamise kohta.

4.5. Eriliigilisi isikuandmeid sisaldavaid paberdokumente või teisaldatavaid andmekandjaid utiliseeritakse, kui akadeemia neid enam ei vaja, sh dokumentide säilitustähtaja möödumisel.

V ANDMEKAITSEGA SEOTUD RIKKUMISTE LAHENDAMINE

5.1. Isikuandmetega seotud rikkumine on mistahes turvanõuetega seotud rikkumine, mis põhjustab isikuandmete:

5.1.1. lubamatu hävimise, kaotsimineku või muutmise;
5.1.2. lubamatu avalikustamise või lubamatu juurdepääsu võimaldamise selleks volitamata isikutele.

5.2. Isikuandmetega seotud rikkumise korral kohustub akadeemia:

5.2.1. rikkumise dokumenteerima (millised on rikkumise asjaolud, rikkumise mõju isikutele, parandusmeetmed (nt tehnilised, korralduslikud), mida akadeemia koheselt rakendab kahjustatud isikuandmete suhtes);
5.2.2. kui rikkumine põhjustas või tõenäoliselt põhjustab andmesubjektide õigustele ja vabadustele kahju, kohustub akadeemia esitama hiljemalt 72 tunni jooksul rikkumisteate Andmekaitse Inspektsioonile;
5.2.3. kui rikkumine põhjustas või tõenäoliselt põhjustab andmesubjektidele suure kahju (oht inimese elule, tervisele, varale ja mainele), kohustub akadeemia sellest teavitama ka andmesubjekti;

5.2.4. juhul, kui akadeemia näol on rikkumise tuvastajana tegemist andmete volitatud töötlejaga, kohustub akadeemia rikkumisest koheselt teavitama vastutavat töötlejat.

5.3. Andmekaitse Inspektsioonile esitatav rikkumisteade peab sisaldama vähemalt alljärgnevat informatsiooni:

5.3.1. isikuandmetega seotud rikkumise laadi kirjeldust. Selleks võib olla näiteks andmete kaotsiminek või hävimine, vargus, koopia tegemine. Samuti volituseta muutmine, lugemine või edastamine;

5.3.2. võimaluse korral puudutatud andmesubjektide kategooriaid ja nende ligikaudne arv ning isikuandmete asjaomaste kirjete liike ja ligikaudset arvu;

5.3.3. andmekaitsespetsialisti või muu kontaktisiku nime ja kontaktandmeid;

5.3.4. isikuandmetega seotud rikkumise võimalike tagajärgede kirjeldust;

5.3.5. meetmete kirjeldust isikuandmetega seotud rikkumise lahendamiseks, sealhulgas vajaduse korral rikkumise võimaliku kahjuliku mõju leevendamiseks.

5.4. Isikule edastatavas teates peavad olema:

5.4.1. selges ja lihtsas keeles selgitatud isikuandmetega seotud rikkumise olemus;

5.4.2. andmekaitseametniku või muu kontaktisiku nimi ja kontaktandmed;

5.4.3. isikuandmetega seotud rikkumise võimalike tagajärgede kirjeldus;

5.4.4. meetmete kirjeldus isikuandmetega seotud rikkumise lahendamiseks.

Lisa 1

SISEKAITSEAKADEEMIA INFOTURBE TAGAMISE ÜLDALUSED
INFOTURBE JUHIS

I ÜLDSÄTTED

1.1. Infoturbe juhise eesmärk on kirjeldada Sisekaitseakadeemia (edaspidi *akadeemia*) üldist lähenemisviisi infoturbe tagamisel.

1.2. Akadeemias koordineerib infoturbe halduse protsessiga seonduvaid tegevusi Siseministeeriumi infotehnoloogia- ja arenduskeskuse (edaspidi SMIT), võttes arvesse kohustuslikke nõudeid ja üldtunnustatud standardeid ning hea tava soovitusi. Tähtsaimateks õigusaktideks, mis reguleerivad andmekaitset automatiseeritud andmetöötlusel või andmekogude pidamisel, on avaliku teabe seadus, isikuandmete kaitse seadus ja riigisaladuse ja salastatud välisteabe seadus ning isikuandmete kaitse üldmäärus.

1.3. Infoturbe valdkonna üldpõhimõtete rakendamise dokumentideks on akadeemias käesolev infoturbe juhis ja teised korrad.

1.4. Korras kasutatakse mõisteid eelkõige alljärgnevas tähenduses:

1.4.1. akadeemia infosüsteemide varad (edaspidi *infovara*) - akadeemias kasutusel olevad infotehnoloogilised vahendid ja viimaste abil töödeldavad andmed, sh isikuandmed. Infotehnoloogilised vahendid on riist-, tarkvara ja andmesideseadmed;

1.4.2. andmed - mis tahes viisil ja mis tahes andmekandjale jäädvustatud või dokumenteeritud teave ning kõikvõimalike (infotehnoloogiliste) vahendite abil edastatav või töödeldav teave;

1.4.3. konfidentsiaalne ehk avaldamisele mitte kuuluv teave - andmed, millele on juurdepääs lepingu või seaduse alusel või mis on mõnel muul alusel kuulutatud mitteavalikuks;

1.4.4. Infoturbeintsident - kõik reaalse või potentsiaalse kahju juhtumid, mis võivad ohustada või halvata infovara turvalisust, põhjustades nende käideldavuse (töökindlus), tervikluse (andmete õigsuse ja muutumatuse) või konfidentsiaalsuse (andmete salastatuse) kao. Infoturbeintsidentideks loetakse muuhulgas ka toimingud, mis ei ole infoturbe valdkonda reguleerivate õigusaktidega kooskõlas.

II INFOTURBE EESMÄRK

1.5. Akadeemia infoturbe eesmärkideks on tagada:

1.5.1. akadeemia igapäevane asjaajamine ja infovahetus, kus põhieesmärgiks on töötaja ootustele vastava, stabiilse, turvalise ja töökindla töökeskkonna tagamine ja talitlusvõime säilitamine;

1.5.2. akadeemia ja isiku vaheline infovahetus, kus eesmärgiks on avaliku info kättesaadavus infovajajale ning avalike teenuste kiire ja tulemuslik osutamine;

1.5.3. akadeemiale töötlemiseks või hoidmiseks antud andmete konfidentsiaalsus ja terviklus;

1.5.4. infosüsteemide kasutamine vastavalt üldistele infoturbenõuetele.

1.6. Infoturbe eesmärkide saavutamiseks tuleb tagada infovarade kolm infoturbe osaeesmärki:

1.6.1. käideldavus – informatsiooni kasutuskõlblikkus ja õigeaegne kättesaadavus üksnes volitatud isikutele;

1.6.2. terviklus – töödeldav informatsioon peab olema usaldatav, vigu peab vältima tarkvara terve elutsükli jooksul ja andmete tõepärasust peab regulaarselt kontrollima. Avaliku teabe seaduse või muu õigusakti alusel töödeldava andmekogu või infosüsteemi täielik kustutamine peab olema välistatud;

1.6.3. konfidentsiaalsus – kriitilistel aladel peab konfidentsiaalse teabe kaitse olema selgelt määratletud ja vastama asjakohastele (seadusest tulenevatele) nõuetele. Tagada tuleb ka üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus ning asutusesiseseks kasutamiseks määratud informatsiooni salastatus. Akadeemia eesmärk on anda juurdepääs informatsioonile ainult tõendatud teadmisvajaduse alusel ja keelata juurdepääs kõigil teistel.

III INFOTURBEINTSIDENT JA KONTROLLJÄLJED

1.7. Infoturbeintsidendist ja selle ohust peab iga töötaja võimalikult kiiresti teavitama SMIT IT abi (kasutajatuge) ja andmekaitsespetsialisti.

1.8. Infoturbeintsidentide lahendamine toimub selleks määratud isiku või isikute koordineerimisel, kes rakendab vastavalt tekkinud olukorrale asjakohast reageerimist. Infoturbeintsidentide avastamise üheks eelduseks on jälitatavuse toimivus.

1.9. Jälitatavuse tagamiseks salvestatakse ja säilitatakse infovarade haldamise ja kasutamisega seotud toimingute teostamise kohta kontrolljälgi (logisid).

1.10. Kontrolljäljed sisaldavad vähemalt toimingu teostaja nime, toimingu liiki ja toimingu teostamise aega.

1.11. Kontrolljälgede salvestamisel ja säilitamisel peab olema tagatud nende vältimatus, käideldavus, terviklus ja konfidentsiaalsus.

IV KONFIDENTSIAALKOHUSTUSE NÕUE

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

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

1.13.1. mitte avalikustama temale teatavaks saanud konfidentsiaalset informatsiooni, välja arvatud kui see on seadusega kohustuslik või vajalik tööülesannete täitmiseks;
1.13.2. järgima kehtivaid andmekaitset puudutavaid õigusakte ja kordasid;
1.13.3. täitma konfidentsiaalkohustuse nõudeid nii töösuhte ajal kui ka peale selle lõppemist.

V ARVUTIVÕRGU KASUTAMINE

1.14. Töötajal peavad olema oma tööülesannete täitmiseks vajalikud arvutikasutamise algteadmised. Viimaste puudumisel on töötaja kohustatud sellest akadeemiat teavitama.

1.15. Töötaja on kohustatud järgima Eesti Vabariigis kehtivaid õigusakte, akadeemias kehtivaid kordasid ning arvutivõrgu kasutamiseks kehtestatud alalisi ja ajutisi piiranguid.

1.16. Kõik arvutivõrgu ja infosüsteemide kasutamisega kaasnevad kasutamisõigused- ja piirangud on personaalsed ning neid ei ole lubatud ühelt isikult teisele edasi anda. Töötaja lahkumisel akadeemiast suletakse tema juurdepääsuõigused arvutivõrgule ja infosüsteemidele.

1.17. Töötajal on õigus töödelda (vaadata, muuta, väljastada) konfidentsiaalset informatsiooni (teave, mis seaduse, lepingu või mõnel muul alusel kuulutatud mitteavalikuks) ainult oma otseste töö- või ametiülesannete täitmiseks. Seda teavet ei tohi edastada kolmandatele isikutele juurdepääsupiirangu kehtestanud asutuse loata.

1.18. Töötaja on kohustatud kasutama võrguressursse optimaalselt ning mitte koormama arvutivõrku mittetööalaste failide ja tegevustega ega segama teiste arvutivõrgu kasutajate tööd.

1.19. Töötajad on kohustatud regulaarselt korrastama endaga seotud elektronposti ja failiserveris asuvaid andmeid, kustutades ebaolulise sisuga kirjad ja failid.

1.20. Töötaja peab järgima head tava ja üldiseid eetika nõudeid ning mitte tekitama teistele töötajatele või akadeemiale oma tegevusega või tegevusetusega kahju ega ohtu arvutivõrgu turvalisusele ja käideldavusele.

VI TÖÖJAAMA, TARKVARA JA LISASEADMETE KASUTAMINE NING KONFIGUREERIMINE

1.21. IT-vahendite (tööjaamad, printerid, skännerid jne) paigutamise planeerimisel tuleb konsulteerida IT-spetsialistidega SMITist ja paigutada IT-vahendid nii, et vastavat õigust mitteomavad inimesed ei omaks juurdepääsu konfidentsiaalsele informatsioonile ning IT-vahendid oleks kaitstud varguse eest.

1.22. Töötajal on keelatud muuta omaalgatuslikult info- ja kommunikatsioonitehnoloogia (edaspidi IKT) vahendite konfiguratsiooni (sh ei paigalda ega eemalda tarkvara; lisa ja eemalda riistvara; lülita välja viirusetõrje tarkvara ega muuda selle seadistusi). Töötaja kohustub hoidma salastatuna talle usaldatud kasutajatunnused, paroolid, koodid jms ning välistama nende sattumise kolmandate isikute kätte. Töökohalt lahkudes lukustab arvuti. Akadeemial on vajadusel õigus rakendada täiendavaid turvameetmeid IKT seadmetes ja süsteemides töödeldava informatsiooni turvalisuse tagamiseks.

1.23. Töötajal on keelatud arvutivõrgu ja operatsioonisüsteemide turvaaukude, ründekoodi, paroolihäkkimise tarkvara või muu sarnase kasutamine täiendavate juurdepääsuõiguste ja privileegide saamiseks või arvutivõrgu töö häirimiseks.