

Järvamaa Rakendusliku Kolledži infosüsteemide halduse ja kasutamise reeglistik

SISUKORD

1.	Eesmärk	2
2.	Üldsätted	2
3.	Turvalisuse tagamine infosüsteemi üldhalduri tasandil	3
4.	Infosüsteemi osade halduri kohustused ja õigused	3
5.	Infosüsteemide kasutaja kohustused ja õigused	3
6.	Salasõnade halduse turvalisuse tagamine halduri tasemel.....	4
7.	Salasõnade halduse turvalisuse tagamine kasutajatasemel	4
8.	Infosüsteemi kasutuskoha turvalisuse tagamine halduri tasemel	4
9.	Infosüsteemi kasutuskoha turvalisuse tagamine kasutajatasemel.....	4
10.	Interneti turvalise kasutamise tagamine halduri tasemel	5
11.	Interneti turvalise kasutamise tagamine kasutajatasemel	5
12.	E-posti kasutamise turvalisuse tagamine halduri tasemel	5
13.	E-posti kasutamise turvalisuse tagamine kasutajatasemel.....	5
14.	Andmekogude kasutamise turvalisuse tagamine halduri tasemel	5
15.	Andmekogude kasutamise turvalisuse tagamine kasutajatasemel.....	6
16.	Turvalisuse tagamine sülearvutite kasutamisel infosüsteemi mobiilsete osadena või väljaspool kolledži infosüsteemi halduri tasemel	6
17.	Turvalisuse tagamine sülearvutite kasutamisel infosüsteemi mobiilsete osadena või väljaspool kolledži infosüsteemi kasutajatasemel	6
18.	Turvalisuse tagamine uue riist- ja tarkvara kasutuselevõtul halduri tasemel	6
19.	Turvalisuse tagamine uue riist- ja tarkvara kasutuselevõtul kasutajatasemel.....	6
20.	Andmete varundamise turvalisuse tagamine halduri tasemel.....	6
21.	Andmete varundamise turvalisuse tagamine kasutajatasemel	6
22.	Vastutus reeglistiku rikkumise korral	7
23.	Infosüsteemi osade haldurid	7

Järvamaa Rakendusliku Kolledži infosüsteemide halduse ja kasutamise reeglistik

Käesolev reeglistik on osa Järvamaa Rakendusliku Kolledži (edaspidi kolledž) infoturbe korraldusest. Arvutikasutaja reeglistik kehtestab elementaarsed sätted, mis aitavad vähendada kolledži infosüsteemi halduskulusid ning tõhustavad selle turvalisust ja efektiivsust.

1. Eesmärk

- 1.1. Reeglistiku eesmärgiks on tekitada organisatsioonisisene turvateadlikkus ning saavutada infosüsteemi kasutajate ja haldajate individuaalset vastutust ja aktiivset osalust turvalisuse tagamisel.

2. Üldsätted

- 2.1. Kolledži infosüsteemi moodustavad avalik ja mitteavalik teave ja andmekogud, statsionaarsed ja mobiilsed arvutid ja nendega seonduvad tarkvarad ning seadmed, arvutivõrk ja selle komponendid ning ressursid (kaasa arvatud interneti ühendus).
- 2.2. Kolledži infosüsteem on kolledži omand, mille kasutamisel tuleb alati lähtuda eelkõige kolledži huvidest.
- 2.3. Kolledži infosüsteemi või selle osa kadumisest või rikkumisest tuleb koheselt teatada kolledži IT-spetsialistile ning kolledži direktorile. IT-spetsialist võtab vajadusel tarvitusele meetmed turvaintsidendi vältimiseks.
- 2.4. Infosüsteemi kasutamisel tuleb juhinduda:
 - 2.4.1. seadusest;
 - 2.4.2. kolledži tegutsemise põhikirjalistest eesmärkidest;
 - 2.4.3. antud reeglistikust;
 - 2.4.4. üldaktsepteeritud käitumisharjumistest infoturbepoliitika kontekstis.
- 2.5. Kolledži infosüsteemi erinevate osade kasutusest tekkivate konfliktide lahendamisel arvestatakse järgnevaid prioriteete:
 - 2.5.1. esimene prioriteet on kolledži põhitegevuse toimimise tagamine;
 - 2.5.2. teine prioriteet on kolledži muude tegevuste toimimise tagamine.
- 2.6. Kolledži infosüsteemide vahendusel kogutud andmed, sh e-kirjad, ja loodud spetsiaalarakendused on kolledži omand.
- 2.7. Kolledži infosüsteemide üldhalduriks ning turvalisuse tagajaks on IT-spetsialist.
- 2.8. Kolledži infosüsteemi, selle osa või nendega seonduvate ruumide eest vastutajad võivad kooskõlastatult IT-spetsialistiga üllatavalt põhimõtetest ja seadmete sihtotstarbest lähtuvalt kehtestada täiendavaid reegleid tingimusel, et need ei vähenda käesoleva reeglistiku nõudeid.
- 2.9. Kolledži infosüsteemi riist- või tarkvaraline muutmine ja ümberehitamine on ilma kolledži infosüsteemide üldhalduri kooskõlastuseta keelatud.
- 2.10. Mistahes kolledži infosüsteemi puudutav suhtlus toimub ITABI süsteemis aadressil <https://itabi.kolledz.ee>

3. Turvalisuse tagamine infosüsteemi üldhalduri tasandil

- 3.1. Kolledži infosüsteemi üldhaldur on IT-spetsialist, kes vastutab reeglistiku täitmise, tagades:
 - 3.1.1. infosüsteemi regulaarse kontrolli;
 - 3.1.2. haldurite ja/või kasutajate piisava juhendamise.

4. Infosüsteemi osade halduri kohustused ja õigused

- 4.1. Infosüsteemi osa võib olla andmekogu või loogiline riist- ja tarkvara kombinatsioon.
- 4.2. Infosüsteemi osade halduriteks määratud isikud on kohustatud:
 - 4.2.1. jälgima infosüsteemide turvalisust, toimimist ja kättesaadavust kasutajatele;
 - 4.2.2. korraldama infosüsteemide kasutajatele asjakohase instruktaaži ja kasutajatoetust;
 - 4.2.3. teavitama infosüsteemide kasutajaid muudatustest ja sündmustest, mis võivad mõjutada infosüsteemi tööd ja/või kasutajate privaatsust ja/või andmete turvalisust;
 - 4.2.4. pidama saladuses oma töökohustuste täitmise käigus neile avalikuks saanud andmeid, mille kohta neil puudub andmete omaniku luba neid edasi anda, v.a. seadusest tulenevatel juhtudel;
 - 4.2.5. vajadusel teostama andmekogude ja failiressursside turvakopeerimist vastavalt kolledži infosüsteemi üldhalduri juhenditele;
 - 4.2.6. hindama uute infosüsteemide kasutuselevõtul nende mõju olemasolevale;
 - 4.2.7. tagama salasõnade turvalisuse kasutajatasemel;
 - 4.2.8. vajadusel osalema turvaintsidentide aruande koostamisel.
- 4.3. Halduril on õigus:
 - 4.3.1. piirata põhjendatud juhtudel infosüsteemi kasutamist.

5. Infosüsteemide kasutaja kohustused ja õigused

- 5.1. Infosüsteemi kasutajad on kolledži töötajad, õpilased või muud isikud, kellele on antud luba infosüsteemi või selle osa kasutada tööülesannete täitmiseks. Kasutusõiguse saamisel omistatakse taotlejale kasutajakonto(d) unikaalse kasutajanime ja esmase salasõnaga. Kasutusõigus kehtib reeglina tööülesannete täitmise ajal.
- 5.2. Infosüsteemi kasutajad on kohustatud:
 - 5.2.1. järgima infosüsteemile kehtestatud reeglistikku ja täitma IT-spetsialisti korraldusi;
 - 5.2.2. mitte kasutama infosüsteemi viisil, mis häirib teiste süsteemi osade või kasutajate tööd;
 - 5.2.3. mitte võimaldama või lubama teistel isikutel kasutada võõraid kasutajaõigusi ning mitte kasutama võõraid kasutajaõigusi;
 - 5.2.4. vältima oma valduses olevate andmete ja informatsiooni lekkimist kõrvalistele isikutele;
 - 5.2.5. mitte kasutama illegaalset või litsentseerimata tarkvara;

- 5.2.6. rakendama viirusetõrjet süsteemivälistele andmetele ja andmekandjatele;
 - 5.2.7. mitte kasutama kolledži infosüsteemi ebaeetilistel või ebamoraalsetel eesmärkidel;
 - 5.2.8. teavitama kolledži ITABI kõikidest infosüsteemi tõrgetest ja turvaintsidentidest ja nende kahtlusest.
- 5.3. Infosüsteemi kasutajal on õigus:
- 5.3.1. kasutada infosüsteeme tööalasel eesmärgil igal ajal, kui see ei ole vastuolus muude kehtestatud reeglitega;
 - 5.3.2. saada informatsiooni kõigist muudatustest ja sündmustest, mis mõjutavad oluliselt infosüsteemide kasutamist või kasutajate privaatsust;
 - 5.3.3. teha haldurile ettepanekuid infosüsteemide töö ja halduse parema korraldamise osas.

6. Salasõnade halduse turvalisuse tagamine halduri tasemel

- 6.1. Salasõnade halduse turvalisuse eest vastutab infosüsteemi või selle osa haldur, tagades:
- 6.1.1. igale kasutajale vastavalt tema kasutajarollile konto avamisel esialgse salasõna;
 - 6.1.2. igale kasutajale piisava toe ja nõustamise.

7. Salasõnade halduse turvalisuse tagamine kasutajatasemel

- 7.1. Salasõnade halduse turvalisuse tagab kasutajatasemel infosüsteemi kasutaja, tagades:
- 7.1.1. salasõna pikkuseks vähemalt 12 tähemärki ja sisaldama väikest, tähte, suurt tähte, sümbolit ja numbrit;
 - 7.1.2. salasõna erinevuse kasutaja isikuga seotud lihtsalt ära arvatava informatsiooniga;
 - 7.1.3. salasõna erinevuse eelmiste salasõnade modifikatsiooniga;
 - 7.1.4. salasõna säilitamise tingimustes, mis välistavad kõrvaliste isikute juurdepääsu;
 - 7.1.5. salasõna vahetuse kasutusõiguse saamisel, halduri korraldusel, turvaintsidenti kahtlusel või juhtumisel;
 - 7.1.6. vajadusel ja võimalusel kasutama kaheastmelist identifitseerimist.

8. Infosüsteemi kasutuskoha turvalisuse tagamine halduri tasemel

- 8.1. Infosüsteemi kasutuskohaks on tark- ja riistvara komplekt, mis on ühendatud kolledži infosüsteemiga.
- 8.2. Infosüsteemi kasutuskoha turvalisuse eest vastutab kolledži IT-spetsialist, tagades:
- 8.2.1. iga kasutuskoha seadistused viisil, mis välistab autoriseerimata kasutuse;
 - 8.2.2. iga kasutuskoha seadistuste asjakohasuse;
 - 8.2.3. igale kasutajale piisava toe ja nõustamise.

9. Infosüsteemi kasutuskoha turvalisuse tagamine kasutajatasemel

- 9.1. Infosüsteemi kasutaja vastutab kasutuskoha turvalisuse eest, tagades:
- 9.1.1. kasutajakonto ainukasutamise;

- 9.1.2. kasutuskohast lahkudes kasutuskoha lukustamise väljudes infosüsteemist ja/või lülitades kasutuskoha välja;
- 9.1.3. informatsiooni ja andmekandjate säilitamise tingimustes, mis välistavad kõrvaliste isikute juurdepääsu.

10. Interneti turvalise kasutamise tagamine halduri tasemel

- 10.1. Internetiühenduse haldur on kolledži IT-spetsialist, kes vastutab ühenduse kasutamise eest halduri tasemel, tagades:
 - 10.1.1. interneti ühenduse olemasolu kolledži hoonetes;
 - 10.1.2. seadistab internetiühenduse sätteid tulemüüris, mis tagavad ühenduse turvalisuse (HTTPS, VPN);
 - 10.1.3. igale kasutajale piisava toe ja nõustamise.

11. Interneti turvalise kasutamise tagamine kasutajatasemel

- 11.1. Infosüsteemi kasutaja vastutab internetikasutuse turvalisuse eest, tagades:
 - 11.1.1. interneti kasutamise vaid tööalasteks eesmärkideks vastavalt kehtestatud kordadele ja juhenditele;
 - 11.1.2. tundmatu ja tundmatust allikast saadeta informatsiooni mittesattumise kolledži infosüsteemi;
 - 11.1.3. krüpteeringu kasutamise AK-märkega andmete edastamisel.

12. E-posti kasutamise turvalisuse tagamine halduri tasemel

- 12.1. E-posti haldur on kolledži IT-spetsialist, kes vastutab e-posti kasutamise eest halduri tasemel, tagades:
 - 12.1.1. e-posti serveri seadistused, mis tagavad e-posti liikluse turvalisuse (SSL/TLS protokoll, kirjade krüpteering, vajadusel kaheastmeline autentimine);
 - 12.1.2. kolledži infosüsteemi kasutajatele e-posti aadresside ja esmase salasõna loomise;
 - 12.1.3. igale kasutajale piisava toe ja nõustamise.

13. E-posti kasutamise turvalisuse tagamine kasutajatasemel

- 13.1. Infosüsteemi kasutaja vastutab e-posti turvalisuse eest, tagades:
 - 13.1.1. e-posti kasutamise vaid tööalasteks eesmärkideks;
 - 13.1.2. sissetuleva e-postiga saadava informatsiooni asjakohasuse ja adekvaatsuse kontrolli;
 - 13.1.3. mistahes informatsiooni liikumise vältimise e-posti kaudu mitteasjakohastele adressaatidele;
 - 13.1.4. AK-märkega informatsiooni liikumise vältimise e-posti kaudu asjasse mittepuutuvatele adressaatidele.

14. Andmekogude kasutamise turvalisuse tagamine halduri tasemel

- 14.1. Andmekogude turvalise kasutamise eest halduri tasemel vastutab andmekogu haldur oma tööülesannete piires kooskõlastades sammud kolledži IT-spetsialistiga, tagades:

- 14.1.1. andmekogude loomisel, muutmisel ja kasutamisel tingimused, mis välistavad turvaintsidendi tekkimise võimaluse;
- 14.1.2. igale kasutajale piisava toe ja nõustamise.

15. Andmekogude kasutamise turvalisuse tagamine kasutajatasemel

- 15.1. Andmekogude kasutaja vastutab kogude turvalise kasutamise eest, tagades:
 - 15.1.1. andmekogude kasutamise ja jagamise ainult tööülesannete täitmisel;
 - 15.1.2. andmekandjate ja teiste ressursside efektiivsuse.

16. Turvalisuse tagamine sülearvutite kasutamisel infosüsteemi mobiilsete osadena või väljaspool kolledži infosüsteemi halduri tasemel

- 16.1. Turvalisuse tagamisel infosüsteemi mobiilsete osadena või väljaspool kolledžit kasutamise eest halduri tasemel vastutab IT-spetsialist, tagades:
 - 16.1.1. infosüsteemi mobiilsele osale VPN võimaluse.

17. Turvalisuse tagamine sülearvutite kasutamisel infosüsteemi mobiilsete osadena või väljaspool kolledži infosüsteemi kasutajatasemel

- 17.1. Infosüsteemi kasutaja vastutab sülearvuti kasutamisel infosüsteemi mobiilse osana või väljaspool infosüsteemi, tagades:
 - 17.1.1. sülearvuti hoiustamise ja kasutamise tingimustes, mis välistavad sellele kõrvaliste isikute juurdepääsu;
 - 17.1.2. sülearvutis oleva informatsiooni varukoopia olemasolu halduri poolt viidatud viisil ja keskkonnas.

18. Turvalisuse tagamine uue riist- ja tarkvara kasutuselevõtul halduri tasemel

- 18.1. Uue riist- ja tarkvara kasutuselevõtu turvalisuse eest vastutab haldur oma tööülesannete piires kooskõlastades sammud kolledži infosüsteemi üldhalduriga, tagades:
 - 18.1.1. riist- ja tarkvara konfiguratsioonide vastavuse kolledži infosüsteemidele;
 - 18.1.2. riist- ja tarkvara kooskõla infoturbe nõuetega;
 - 18.1.3. igale kasutajale piisava toe ja nõustamise.

19. Turvalisuse tagamine uue riist- ja tarkvara kasutuselevõtul kasutajatasemel

- 19.1. Uue riist- ja tarkvara kasutuselevõtt kasutaja tasemel on keelatud.

20. Andmete varundamise turvalisuse tagamine halduri tasemel

- 20.1. Andmete varundamise eest vastutab infosüsteemi haldur, tagades:
 - 20.1.1. vaid tööalaseks kasutamiseks mõeldud andmete varundamise viisi, regulaarsuse, säilimise ja taaskasutamise võimaluse;
 - 20.1.2. andmete varundamise kvaliteedi ülevaatuse ning asjakohaste muudatuste tegemise;
 - 20.1.3. igale kasutajale piisava toe ja nõustamise.

21. Andmete varundamise turvalisuse tagamine kasutajatasemel

- 21.1. Andmete varundamise eest vastutab infosüsteemi kasutaja, tagades:

- 21.1.1. informatsiooni varukoopia olemasolu halduri poolt viidatud viisil ja keskkonnas.

22. Vastutus reeglistiku rikkumise korral

- 22.1. Reeglistiku rikkumisest tulenevate turvaintsidentide eest vastutab reeglistiku rikkuja.
- 22.2. Reeglistiku rikkuja selgitatakse välja asjassepuutuvate uuringutoimingute teel.
- 22.3. Reeglistiku rikkujale rakendatakse rikkumise ja tagajärgedega proportsionaalseid sanktsioone vastavalt seadusele.

23. Infosüsteemi osade haldurid

	Infosüsteemi osa halduri tegevus	Halduri ametikoht
1.	Salasõnade halduse turvalisuse tagamine	IT-spetsialist
2.	Infosüsteemi kasutuskoha turvalisuse tagamine	IT-spetsialist
3.	Interneti turvalise kasutamise tagamine	IT-spetsialist
4.	E-posti kasutamise turvalisuse tagamine	IT-spetsialist
5.	Andmekogude kasutamise turvalisuse tagamine	
	EHIS	kantseleispetsialist
	TAHVEL	projektijuht
	MOODLE	projektijuht
	SAIS	projektijuht
	EIS	direktor
	FITEKIN	raamatupidaja
	ERPLY	raamatupidaja
	RTIP	kantseleispetsialist-juhiabi
	PINAL	kantseleispetsialist-juhiabi
	Riigihangete register	kulujuht
	Projektide aruandlussüsteem	projektijuht, projektikoordinaator
	Koduleht	arenguspetsialist
	Sotsiaalmeedia kontod	noortejuht
	Loetelus nimetamata andmekogud	direktor või direktori volitatud töötaja
6.	Turvalisuse tagamine sülearvutite kasutamisel infosüsteemi mobiilsete osadena või väljaspool kolledži infosüsteemi	IT-spetsialist
7.	Turvalisuse tagamine uue riist- ja tarkvara kasutuselevõtul	IT-spetsialist
8.	Andmete varundamise turvalisuse tagamine	IT-spetsialist