ALGTEKST-TERVIKTEKST

Kinnitatud kantsleri korraldusega nr 209

Redaktsiooni jõustumise kuupäev: 04.12.2024

Lõppkasutajate seadmete haldamise ja kasutamise eeskiri

1. **Üldsätted**
	1. Käesolev lõppkasutajate seadmete haldamise ja kasutamise eeskiri (edaspidi eeskiri) on koostatud eesmärgiga tagada Tallinna Tehnikaülikooli (edaspidi ülikooli) infotehnoloogia varade ja andmete turvalisus, järgides ISO/IEC 27001 standardi nõudeid. Eeskiri kehtib kõigile ülikooli töötajatele, üliõpilastele ja partneritele, kes kasutavad ülikooli hallatavaid seadmeid ja teenuseid. Eeskiri reguleerib nii keskhalduse all olevate kui ka haldamata lõppkasutajate seadmete kasutamist, et tagada informatsiooni turvalisus ja kaitse kogu ülikooli võrgustikus ja süsteemides.
	2. **Seade** – käesoleva eeskirja mõistes tähendab arvutusvõimekusega elektroonilist vahendit, mida kasutatakse Tallinna Tehnikaülikooli tööülesannete täitmiseks või ligipääsuks ülikooli süsteemidele ja võrkudele. Seadmete hulka kuuluvad personaalsed ja kaasaskantavad arvutid, serverid, mobiilsed tööjaamad (sh nutitelefonid) ning muud sarnased vahendid, mis võimaldavad arvutus-, andmetöötlus-, suhtlus- või juhtimisülesannete täitmist.
	3. **Keskhaldus** – käesoleva eeskirja mõistes tähendab infotehnoloogia osakonna tsentraliseeritud haldustegevust, mille kaudu tagatakse ülikooli seadmete ja süsteemide ühtne haldamine, turvalisus ja töökindlus. See hõlmab operatsioonisüsteemide, tarkvarade ja turvapaikade paigaldamist ja uuendamist, seadmete konfiguratsiooni ja profiilide haldamist, kaugseiret ja turvaprobleemide ennetamist, andmekaitsemeetmete rakendamist (sealhulgas seadmete krüpteerimist ja viirusetõrje tarkvara kasutamist) ning kasutajate ligipääsuõiguste haldust. Keskhalduse eesmärk on tagada, et kõik hallatavad seadmed vastavad ülikooli infoturbe- ja tehnilistele nõuetele ning toetavad tõrgeteta tööprotsesse.
2. **Käsitlusala**
	1. Eeskiri kehtib kõikidele ülikooli töötajatele ja tudengitele ning hõlmab järgmiseid tegevusi:
		1. keskhaldusega seadmete kasutamine;
		2. keskselt mittehallatud seadmete kasutamine;
		3. lõppkasutajate seadmete haldamine;
		4. seadmete kasutusele võtmine, kasutamine, kasutusest eemaldamine ja hävitamine;
		5. turvalisuse, andmekaitse ja privaatsuse tagamine.
3. **Kasutajate seadmete profiilid**
	1. **Arvutiklassi ja auditooriumi arvutid**
		1. Profiili kirjeldus:
			1. seadmed on täielikult hallatud ülikooli infotehnoloogia osakonna poolt. Kõik tarkvarauuendused ja turvapaigad tehakse tsentraalselt. Erinevad draiverid uuendatakse regulaarselt, tagades ühendatud seadmete töökindluse;
			2. infotehnoloogia osakond tagab infoturbe, sealhulgas automaatselt uueneva viirusetõrje paigaldamise;
			3. seadmesse sisselogimine toimub UNI-ID kontoga. Kasutajad (sh tudengid) ei oma administraatori õigusi;
			4. Kasutajaprofiilid kustutatakse seadmetest perioodiliselt, seal hulgas profiiliga seotud failid ja andmed.
		2. Kasutajate rollid ja vastutus:
			1. kasutajad saavad kasutada eelnevalt paigaldatud tarkvara;
			2. kasutaja kohustus on järgida ülikooli arvutiklasside kasutamise juhiseid;
			3. kasutaja on koheselt kohustatud teavitama infotehnoloogia (edaspidi IT) kasutajatuge probleemidest ja anomaaliatest seadme kasutamisel.
		3. Haldusprotsess:
			1. tarkvarauuendused ja turvapaigad paigaldatakse automaatselt;
			2. süsteemi toimimist ja turvalisust jälgitakse pidevalt haldustarkvara kaudu;
			3. kasutajaprofiilid kustutatakse seadmetest automaatselt.
	2. **Lõppkasutajate seadmed**
		1. Lõppkasutajate seadmetele, mida kasutatakse organisatsiooni tööülesannete täitmiseks, kehtivad üldreeglid:
			1. kasutajatel on õigus saada tuge ja juhiseid IT-osakonnalt seoses seadmete kasutamise, tarkvara installimise ning võimalike tehniliste probleemide lahendamisega;
			2. kasutajad võivad kasutada seadmeid tööülesannete täitmiseks vastavalt seadme profiilile ning ülikooli juhistele ja poliitikatele;
			3. kasutajad vastutavad seadmes olevate andmete turvalisuse eest ning peavad selle tagamiseks järgima ülikooli poolt sätestatud infoturbe juhiseid ja poliitikaid;
			4. kui kasutaja kasutab täielikult hallatud seadet, siis andmete varundamine toimub vastavalt organisatsiooni infotehnoloogia halduspoliitikatele ja süsteemidele;
			5. kui kasutaja kasutab osaliselt hallatud või isiklikku seadet, vastutab kasutaja seadmes olevate andmete varundamise eest ise;
			6. viirustõrje lahenduste ja logide loomise protsessi väljalülitamine on keelatud;
			7. mittelitsentseeritud tarkvara kasutamine ei ole ülikooli seadmetes ja süsteemides lubatud;
			8. seadmete kasutamine peab olema kooskõlas ülikooli kehtestatud turvanõuete ja juhistega, sh tarkvarauuendused, viirustõrje ja krüpteerimine.
	3. **Täielikus keskhalduses Windows seadmed**
		1. Profiili kirjeldus:
			1. seadmed on täielikult hallatud ülikooli infotehnoloogia osakonna poolt. Kõik tarkvarauuendused ja turvapaigad tehakse tsentraalselt. Erinevad draiverid uuendatakse regulaarselt, tagades seadme külge ühendatud seadmete töökindluse;
			2. seadmesse sisselogimine toimub UNI-ID kontoga. Kasutajatel puuduvad administraatori õigused;
			3. seadmete andmekandjad on krüpteeritud BitLockeriga. Krüptograafilisi võtmeid hoitakse haldustarkvaras seadme kirje juures;
			4. infotehnoloogia osakond installeerib seadmesse vaikimisi profiilile vastava tarkvara. Ülikool pakub kasutajale täiendavaid tarkvarasid, mis on lisatud kesksesse tarkvarade repositooriumi. Kasutaja saab ülikooli keskse tarkvarade repositooriumi kaudu paigaldada oma seadmesse täiendavat tarkvara. Kogu tsentraalselt paigaldatud tarkvara on litsentseeritud. Kui on vajadus mõne muu tarkvara järele, tuleb selle paigaldus tellida IT kasutajatoe kaudu;
			5. seadmerikke korral saab kasutada asendusseadet, et töö saaks jätkuda katkematult;
			6. pärast installeerimist on seadmes üks keskhalduse administraatori konto mis on mõeldud IT kasutajatoele.
		2. Kasutajate vastutus:
			1. kasutaja kasutab seadet eelkõige tööülesannete täitmiseks. Isiklikuks otstarbeks kasutamine (nt e-kirjade saatmine, veebis sirvimine) on lubatud mõistlikkuse piires, tingimusel, et see ei kahjusta seadme töökindlust ega ülikooli infoturbe nõuete täitmist;
			2. seadme nime (*hostname*) muutmine on keelatud;
			3. kasutajad ei saa iseseisvalt paigaldada ega eemaldada tarkvara;
			4. kasutajal on kohustus teatada viivitamatult infotehnoloogia osakonnale kõikidest probleemidest ja anomaaliatest;
				1. kasutajal on kohustus järgida ülikooli infoturbe juhiseid ja poliitikaid.

#### Haldusprotsess:

* + - * 1. infotehnoloogiaosakond jälgib pidevalt süsteemi toimivust ja turvalisust;
				2. tarkvara paigaldamine ja uuendamine toimub automaatselt;
				3. turvanõrkuste avastamisel rakendatakse parandusmeetmed vastavalt turvanõrkuste haldamise korrale.
	1. **Keskhalduses on privilegeeritud õigustega kasutajate Windows seadmed.**
		1. Profiili kirjeldus:
			1. seadmed on täielikult hallatud ülikooli infotehnoloogia osakonna poolt, kuid kasutajatele on antud täiendavad õigused seadmete haldamiseks läbi privileegitud õiguste (lokaalsed administraatori õigused). Kasutajad saavad paigaldada ja eemaldada tarkvara. Kõik tarkvarauuendused ja turvapaigad tehakse tsentraalselt (v.a tarkvarad, mida kasutaja ise paigaldanud). Erinevad draiverid uuendatakse regulaarselt, tagades seadme külge ühendatud seadmete töökindluse;
			2. seadmesse sisselogimine toimub UNI-ID kontoga;
			3. seadmete andmekandjad on krüpteeritud BitLockeriga. Krüptograafilisi võtmeid hoitakse haldustarkvaras seadme kirje juures;
			4. infotehnoloogia osakond installeerib seadmesse vaikimisi profiilile vastava tarkvara. Ülikool pakub kasutajale täiendavaid tarkvarasid, mis on lisatud kesksesse tarkvarade repositooriumi. Kasutaja saab keskse tarkvarade repositooriumi kaudu paigaldada oma seadmesse täiendavat tarkvara;
			5. infotehnoloogia osakond pakub seadmele kasutajatuge. Suuremahuliste (aega nõudvate) probleemide korral teostatakse seadme uus install, kusjuures senised andmed ja tarkvarad kustutatakse;
			6. seadmerikke korral saab kasutada asendus seadet, et töö saaks jätkuda katkematult;
			7. pärast installeerimist on seadmes kaks kohalikku kasutajakontot:
				1. Administraatori konto (administraatori õigustes): mõeldud lõppkasutajale üksnes eriõigusi vajavate toimingute teostamiseks. Kasutaja sisestab ise sobiva salasõna seadme kättesaamisel;
				2. keskhalduse administraatori konto: mõeldud infotehnoloogia IT kasutajatoele. Antud kontot ei tohi deaktiveerida, vastasel juhul kaob IT kasutajatoe poolne juurdepääs seadmele ja tugi selle haldamiseks;

#### Kasutajate vastutus:

* + - * 1. Kasutaja kasutab seadet eelkõige tööülesannete täitmiseks. Isiklikuks otstarbeks kasutamine (nt e-kirjade saatmine, veebis sirvimine) on lubatud mõistlikkuse piires, tingimusel, et see ei kahjusta seadme töökindlust ega ülikooli infoturbe nõuete täitmist;
				2. kasutajad vastutavad nende poolt paigaldatud tarkvara ja süsteemi toimumise eest;
				3. seadme nime (*hostname*) muutmine on keelatud;
				4. kasutajad peavad regulaarselt paigaldama turvapaigad ja uuendused;
				5. tööülesannete täitmiseks kasutab kasutaja tavakasutaja kontot, administraatori konto kasutamine on lubatud ainult tööülesannetega seotud tegevuste eriõigusi vajavate toimingute teostamiseks;
				6. kasutajad vastutavad täielikult kõikide toimingute eest, mis on administraatori kontoga tehtud. Seadmes probleemide tekkimisel vastutab kasutaja ise ning IT kasutajatugi aitab vaid seadme taastepaigaldamisega;
				7. viirusetõrje tarkvara keelamine ja logide loomise protsessi peatamine on keelatud.

#### Haldusprotsess:

* + - * 1. infotehnoloogiaosakond jälgib pidevalt süsteemi toimimist ja turvalisust;
				2. tarkvara paigaldamine ja uuendamine toimub automaatselt;
				3. IT-osakond korraldab regulaarselt kontrolle, et tagada vastavus turvanõuetele.
		1. IT-osakonna poolt haldamata seadmed.

#### Profiili kirjeldus:

* + - * 1. ülikooli poolt soetatud seadmed, mis ei ole hallatud ülikooli IT-osakonna poolt. Kasutajad saavad paigaldada ja eemaldada tarkvara. Tarkvarauuenduste, turvapaikade ja draiverite paigaldamise eest vastutab lõppkasutaja;
				2. infotehnoloogia osakond võimaldab infoturbe, sealhulgas automaatselt uueneva viirusetõrje paigaldamise Windowsi ja macOS seadmetesse;
				3. seadmesse sisselogimine toimub tavaliselt kohaliku kontoga;
				4. seadmete andmekandjad ei ole vaikimisi krüpteeritud. Kasutaja ise vastutab andmete krüpteerimise ja võtmete hoidmise eest;
				5. seadmes olevad failid ei ole varundatud. Kasutaja peab ise leidma lahenduse varundamiseks ning selle seadistama. Infotehnoloogia osakond soovitab kasutada Microsoft OneDrive lahendust;
				6. Infotehnoloogia osakond pakub antud seadmetele kasutajatuge parima pingutuse (*best effort)* baasil.

#### Kasutajate rollid ja vastutus:

* + - * 1. kasutaja kasutab seadet eelkõige tööülesannete täitmiseks. Isiklikuks otstarbeks kasutamine (nt e-kirjade saatmine, veebis sirvimine) on lubatud mõistlikkuse piires, tingimusel, et see ei kahjusta seadme töökindlust ega ülikooli infoturbe nõuete täitmist;
				2. kasutajad vastutavad nende poolt paigaldatud tarkvara ja süsteemi toimimise eest;
				3. kasutajad on kohustatud kasutama ainult ametlikku ja litsentseeritud tarkvara;
				4. kohustus paigaldada kõik olulised turvapaigad ja uuendused;
				5. kohustus kasutada tugevaid salasõnu ja järgida infoturbe parimaid tavasid;
				6. administraatori õiguseid tohib kasutada ainult tööülesannete täitmiseks vajalike seadistuste või tarkvaramuudatuste tegemiseks. Igapäevaseks tööks tuleb kasutada tavakasutaja õiguseid, et vähendada infoturberiske;
				7. seadmes olevate andmete varuandamise eest vastutab kasutaja;
				8. viirusetõrje tarkvara keelamine ja logide tekitamise protsessi peatamine on keelatud;
				9. kasutajad vastutavad täielikult kõikide toimingute eest, mis on tehtud seadmega. Seadmes probleemide tekkimisel vastutab kasutaja ise ning IT kasutajatugi aitab vaid seadme taastepaigaldamisega.

#### Haldusprotsess:

* + - * 1. infotehnoloogia osakond jälgib süsteemi toimimise ja turvalisust ning annab juhiseid ja nõuandeid turvalisuse tagamiseks;
				2. võrguliikluse ja seadmete ühendamise turvalisus tagatakse võrgu segmentimise ja turvapoliitikate kaudu.
	1. **Lõppkasutajate arvutid, telefonid ja tahvelarvutid, mis ei ole ostetud ega hallatud ülikooli poolt (edaspidi nimetatud kui BYOD-seadmed).**
		1. Profiili kirjeldus:
			1. kasutajad enda isiklikud arvutid, tahvelarvutid, mobiilsed seadmed, mida kasutatakse ülikooli võrgus või millel kasutatakse ülikooli UNI-ID kontot.
		2. Kasutajate rollid ja vastutus:
			1. isiklike seadmete kasutamine ülikooli võrkudele ja süsteemidele ligipääsemiseks on lubatud, kuid nende kasutamisel kehtivad järgmised infoturbe nõuded:
				1. BYOD-seadmed peavad vastama minimaalsetele turvanõuetele, sealhulgas, kuid mitte ainult:
				2. seadmel peab olema ajakohane operatsioonisüsteem ja turvavärskendused;
				3. seadmel peab olema aktiivne ja ajakohane viirusetõrje ja pahavaratõrje;
				4. seadmel peab olema turvaline autentimine, näiteks PIN-kood, sõrmejälg või muu mitmefaktoriline autentimine;
				5. seadmel peab olema sisse lülitatud andmete krüpteerimine.
			2. Kõik ülikooliga seotud tundlikud andmed (sh isikuandmed, teadustöö materjalid, finantsandmed jms) tuleb hoida kaitstud kujul ka BYOD-seadmetes, rakendades selleks asjakohaseid turvameetmeid (mitmefaktoriline või biomeetriline autentimine, tugevad paroolid, krüpteerimine vms).
			3. Isikliku seadme kasutamise korral peab kasutaja järgima organisatsiooni kehtestatud turvapoliitikaid ja -protokolle, sealhulgas võib nõutud olla spetsiaalse haldustarkvara paigaldamine seadmele, et tagada turvanõuete täitmine ja seadmest ligipääsu kontrollimine.
			4. Kasutaja vastutab oma isiklikus seadmes olevate andmete turvalise varundamise eest.
			5. Juhul kui seade on kadunud või varastatud, peab kasutaja viivitamatult teavitama IT-tuge, et saaks rakendada andmete kustutamise või ligipääsu eemaldamise meetmeid.
			6. Kui seade kaotab juurdepääsu ülikooli süsteemidele töölt lahkumise, seadme asendamise või muude muudatuste tõttu, tuleb kustutada kõik tundlikud ja tööga seotud andmed vastavalt IT osakonna juhistele.
		3. Haldusprotsess:
			1. IT-osakond annab juhiseid ja nõuandeid turvalisuse tagamiseks;
			2. võrguliikluse ja seadmete ühendamise turvalisus tagatakse võrgu segmentimise ja võrgupoolsete turvaseadistuste ja monitooringu kaudu.
1. **Lõppkasutajate seadmete soetamine, väljaandmine ja kasutusest eemaldamine**
	1. **Seadmete soetamine**
		1. Lõppkasutajate seadmete tellimine toimub riigihanke korra alusel. Iga struktuuriüksus esitab oma seadmete tellimuse infotehnoloogia osakonnale, kes vastutab tellimuste menetlemise ja korraldamise eest. Tellimuse maksumuse tasub vastav struktuuriüksus. Seade kantakse IT osakonna poolt hallatavasse seadmete registrisse.
	2. **Seadme kasutusele võtmine läbi kingituse või annetuse**
		1. Kui struktuuriüksus soovib talle kingitud või annetatud seadet ülikoolis kasutusele võtta, tuleb esitada IT kasutajatoele vastav tellimus. IT kasutajatugi korraldab seadme puhastamise, arvutite registrisse kandmise ja seadme väljaandmise.
	3. **Seadme ehitamine ja arvele võtmine**
		1. Juhul kui struktuuriüksus soovib ehitada erinevatest komponentidest seadme, siis pärast komplekteerimist tuleb sellest teavitada IT kasutajatuge, kes võtab seadme arvele arvutite registrisse.
	4. **Seadme profiili valimine**
		1. Infotehnoloogia osakond väljastab vaikimisi seadmed täieliku keskhalduse Windowsi profiiliga (v.a seadmed, mis vaikimisi ei toeta Windowsi profiili, mille puhul rakenduvad punktis 3.5 kirjeldatud tingimused). Vajadusel struktuuriüksus ja/või kasutaja saavad tellimuse tegemisel hetkel märkida mõne muu soovitud profiili. Kui hiljem tekib vajadus või soov profiili muuta, siis tuleb selleks pöörduda IT kasutajatoe poole, kes saab vastavad muudatused teostada.
	5. **Seadmete väljaandmine**
		1. Kui seade on tarnitud, valmistatakse see IT kasutajatoe poolt ette vastavalt profiilile. Ettevalmistustööd hõlmavad operatsioonisüsteemi paigaldamist, vajaliku tarkvara installeerimist ja turvaseadistuste konfigureerimist. Kui seadmesse on infotehnoloogia osakonna poolt paigaldatud litsentsitud tarkvara, millel on aktiveerimisvõti, ei tohi kasutaja seda tarkvara iseseisvalt teisele seadmele paigaldada ega seda teisele kasutajale anda ilma infotehnoloogia osakonda teavitamata. Infotehnoloogia osakond peab muudatused registreerima varade haldussüsteemis. Pärast ettevalmistust väljastatakse seade lõppkasutajale koos kasutusjuhiste ja turvanõuete teavitusega.
	6. **Seadmete kasutamine**
		1. Infotehnoloogia osakond vastutab ülikooli seadmete tehnilise haldamise, turvapaikade ja tarkvarauuenduste tsentraalse paigaldamise ning infoturbe tagamise eest. Struktuuriüksus ja tema töötaja vastutavad neile välja või kasutusse antud seadmete igapäevase turvalise kasutamise ja hooldamise eest. Järgnevate punktide täitmine on kohustuslik tagamas seadmete turvalisus ja töökindlus kasutaja kasutuses:
			1. kasutaja peab tagama, et seadmed on kaitstud füüsiliste ohtude (vargus, kahjustus) ja keskkonnariskide eest;
			2. kasutaja peab hoidma seadmeid ajakohasena, paigaldades kõik vajalikud turvapaigad ja uuendused. Keelatud on mittelitsentseeritud tarkvara kasutamine;
			3. kasutaja peab kasutama tugevaid salasõnu ja järgima ülikooli autentimisnõudeid, sealhulgas kahefaktorilist autentimist;
			4. Kui kasutajad paigaldavad seadmesse oma tarkvara või teevad muudatusi, mis mõjutavad seadmete haldust (nt seadme nimi, kasutaja või tarkvara), tuleb sellest teavitada infotehnoloogia osakonda, et muudatused saaksid korrektselt kajastuda varade registris. Teavituses tuleb esitada seadme nimi, lõppkasutaja nimi ja tarkvara andmed (nt nimi ja aktiveerimisinfo);
			5. kasutajad peavad regulaarselt varundama kõik olulised andmed kasutades soovitatud varunduslahendusi;
			6. kasutajad peavad järgima kõiki ülikooli infoturbe poliitikaid ja juhiseid, teavitades infotehnoloogia osakonda viivitamatult kõikidest turvaprobleemidest või kahtlustatavatest rikkumistest.
	7. **Seadme kasutamise lõpetamine**
		1. Kasutuses oleva seadme puhastamine
			1. Kui seadme kasutaja lahkub ülikoolist, siis vastav struktuuriüksus teeb IT kasutajatoele tellimuse seadme puhastuseks ehk IT kasutajatugi eemaldab kõik eelneva kasutajaga seotud andmed ja profiilid ning teeb arvutite registris ja seadmete haldustarkvaras vajalikud muudatused. Puhastatud seade jääb struktuuriüksuse haldusesse ja kantakse seadmete nimekirja.
		2. Seadme üleandmine uuele kasutajale
			1. Struktuuriüksus saab anda puhastatud seadme kasutamiseks uuele kasutajale. Seadme väljastamisel uuele kasutajale struktuuriüksus teeb vastava kasutaja muudatuse arvutite registrisse. Seade väljastatakse uuele kasutajale vastavalt määratud seadme profiilile ja ülikooli turvanõuetele.
	8. **Seadmete lõplik kasutusest eemaldamine ja hävitamine**
		1. Seadme lõplikult kasutamisest eemaldamise eelduseks on seadme puhastamine ehk seadmest andmete ja profiilide kustutamine ning arvutite registris ja seadmete haldustarkvaras vajalike muudatuste teostamine. Kõik seadmes olevad andmed kustutatakse turvaliselt, et vältida andmete leket.
	9. **Seadmete lõpliku kasutamise eemaldamise stsenaariumid**
		1. Seadme müük ja/või annetamine kolmandale isikutele.
			1. Struktuuriüksus saab otsustada oma seadmete müümise või annetamise kolmandale isikule (nt töölt lahkuv töötaja või muu osapool). Seadme müügihinna määrab IT kasutajatugi, tuginedes turuhinnale ja/või seadme jääkväärtusele. Enne seadme müüki või annetamist tuleb esitada tellimus IT kasutajatoele seadme puhastamiseks. Puhastamise käigus kustutatakse kõik andmed ja paigaldatakse seadme ostuga kaasas olnud operatsioonisüsteem ning tehakse vastavad muudatused arvutite registris ja seadmehaldussüsteemis. Seejärel seade väljastatakse uuesti struktuuriüksusele, kes saab selle edasi müüa (vormistades müügiarve) või annetada kolmandale isikule vastavalt ülikoolis kehtestatud korrale.
		2. Seadme amortiseerumine, kahjustumine ja utiliseerimine.
			1. Kui seade amortiseerub ehk ei ole enam sobilik tööalaste ülesannete täitmiseks või kui seade kahjustub, siis tuleb selle kohta teha tellimus IT kasutajatoele seadme puhastamiseks. Puhastamise käigus kustutatakse seadmes olevad andmed (või võetakse andmekandja seadmest välja ja suunatakse eraldi hävitamisele), kustutatakse vastav kirje seadmehaldussüsteemist ja tehakse vastav märge arvutite registrisse seadme juurde. IT kasutajatugi korraldab seadme utiliseerimise järgides turva- ja keskkonnanõudeid.
		3. Seadme kadumine või varastamine
			1. Kasutaja peab viivitamatult teavitama infotehnoloogia osakonda seadme kadumisest või vargusest. Infotehnoloogia osakond tõkestab ligipääsu ja tagab andmete kaugelt kustutuse (v.a mittehallatud seadmed, kus kustutamine ei ole võimalik). Seadme kirje eemaldatakse haldussüsteemist ja seadme kirje juurde arvuti registrisse tehakse vastav märge.
2. **Turvalisus, andmekaitse ja privaatsus**
	1. Ülikooli IT-osakonna infoturbe talitus kasutab erinevaid automaatseid töövahendeid turvalisuse tagamiseks ja potentsiaalsete ohtude ennetamiseks, nagu logide analüüs, anomaaliate tuvastamine, veebiskaneeringud, turvaskaneeringud, viirusetõrje ja pahavara tuvastamine. Kõik monitooringutoimingud on seaduslikud ja kooskõlas Eesti ja EL andmekaitse regulatsioonidega (GDPR). Monitooringutoimingud on proportsionaalsed ja kasutavad võimalikult vähe privaatsust riivavaid meetmeid. Eesmärk on tagada IT-süsteemide turvalisus ja ennetada võimalikke turvaohte. Kogutud andmeid kasutatakse üksnes süsteemide turvalisuse tagamiseks ja võimalike turvaohtude ennetamiseks.
3. **Koolitused, teavitused ja tugi**
	1. Infotehnoloogia osakond:
		1. korraldab regulaarselt infoturbe koolitusi töötajatele ja tudengitele;
		2. teavitab uute ohtude ja turvanõrkuste kohta;
		3. pakub tuge ja abi kõikidele kasutajatele seadmete ja tarkvara probleemide lahendamisel täielikus keskhalduses olevatele arvutitele. Teistel juhtudel ülikooli infotehnoloogia osakond pakub tuge parima pingutuse *(best effort)* printsiibil.
4. **Järelevalve**
	1. Lõppkasutajate seadmete haldamise ja kasutamise eeskirja rakendamist järgib siseauditi osakond lähtuvalt siseauditi tööplaanist. Avastatud mittevastavuste korral rakendatakse parandusmeetmeid ja nende rakendamine dokumenteeritakse.
	2. Eeskirja rikkumiste või infoturbealaste poliitikate mittejärgimise korral rakendatakse asjakohaseid sanktsioone, mis võivad hõlmata hoiatusi, juurdepääsu piiramist, töösuhte lõpetamist või muid õiguslikke meetmeid.

1. **Rakendamine**
	1. Eeskirja rakendatakse selle kehtestamise hetkest kõikide uute seadmete väljastamisel. Varasemalt kasutajatele väljastatud seadmete profiilides võib olla mitmeid erisusi kehtestatud korraga. Need seadmed viiakse järk-järgult vastavusse kehtestatud korrale. Infotehnoloogia osakonnale jääb õigus teatud varasemalt välja antud seadmetele jätta sisse erisused, mis tulenevalt tehnoloogilisest keerukusest või on majanduslikult ebamõistlikud. Need erisused dokumenteeritakse varade registrisse.
	2. Eeskirja vaadatakse vähemalt üks kord aastas üle lähtuvalt muutuvast tehnoloogiast, regulatsioonidest ja kasutajate vajadustest.