IT-teenuste kasutamise kord töötajale

Jõgevamaa Gümnaasium

Sisukord

Sissejuhatus

1.1. IT-teenuste kasutaja kord (edaspidi kord) on Jõgevamaa Gümnaasiumi (edaspidi kool või asutus) infoturbe korra lisa, mis sätestab ameti IT-teenuseid kasutavate töötajate ja väliste kasutajate õigused ja kohustused IT-varaga töötamisel ja teabe töötlemisel. Selle eesmärk on aidata kaasa kooli infovarade konfidentsiaalsuse, tervikluse ja käideldavuse tagamisele ning toetada kooli üldisi infoturbe eesmärke, nagu sätestatud infoturbe kontseptsioonis.

1.2. Korda vaadatakse üle perioodiliselt, aga vähemalt 1 kord aastas, ning pärast oluliste muudatuste tegemist IT-süsteemides. Korra ajakohastamise korraldab infoturbejuht või tema poolt määratud töötaja.

1.3. Kasutaja on kohustatud täitma käesoleva korra nõudeid ning peab tegutsema vastutustundlikult ja professionaalselt. Kooli IT-teenuse kasutamise korral eeldatakse, et kasutaja on tutvunud kehtiva korra nõuetega.

1.4. Kool võib infoturbejuhi loal logida, üle vaadata ja muul viisil kasutada mis tahes teavet, mis on salvestatud või läbib asutuse seadmeid ja süsteeme.

1.5. Uus töötaja kinnitab enne IT-vahendite kasutuselevõttu kirjalikult, et on eeskirjaga tutvunud.

2. Mõisted

2.1. Eeskirjas kasutatakse mõisteid järgmises tähenduses:

Mõiste	**Selgitus**
Andmed	Teabe ehk informatsiooni taastõlgendatav esitus formaliseeritud kujul, mis sobib edastuseks, tõlgenduseks või töötluseks. Andmed hõlmavad mis tahes viisil ja mis tahes andmekandjatele jäädvustatud või dokumenteeritud teavet ning kõigi sh infotehnoloogiliste vahendite abil edastatavat või töödeldavat teavet. Andmed on jaotatud tundlikkuse järgi rühmadesse, milledele kehtivad erinevad salastusnõuded.
Arvutivõrk	Kogum erinevatest andmesideseadmetest, mille kaudu on arvutid, printerid, serverid, nutitelefonid ja teised seadmed andmevahetuse või ressursside jagamise eesmärgil omavahel ühendatud.
Intsident	Sündmus, mis tegelikult või potentsiaalselt ohustab ilma seadusliku volituseta teabe või infosüsteemi konfidentsiaalsust, terviklust või kättesaadavust; või kujutab endast turvapoliitika, turbeprotseduuride või

	vastuvõetava kasutuse poliitika rikkumist või vahetut ohtu rikkuda, põhjustades võimaliku kahju või häire asutuse infosüsteemide toimimises.
Irdseade	Seade, mida lõppkasutaja saab oma tavapärase töö käigus süsteemiga ühendada või sealt eemaldada, nt USB-mälupulk. Info ja kommunikatsioonitehnoloogilise seadme väline andmekandja, mida lõppkasutaja saab oma tavapärase töö käigus süsteemiga ühendada, näiteks mälupulgad, välised kõvakettad, mälukaardid ja CD/DVD/BR -plaadid
IT-teenused	Infotehnoloogilised seadmed ja süsteemid (arvutid, printerid, serverid, võrguühendused, tarkvara jms) ning nende kasutamist tagav töökorraldus
Kasutaja	Asutuse töötaja või väline kasutaja, kellele tööülesannetest või muudest vajadustest tulenevalt on antud õigused asutuse IT-teenuste isikuandmete töötlemise ja väliste andmekandjate kasutamiseks
Kasutajatunnus, kasutajakonto	Pääsuõiguse tunnus, mis annab kasutajale pärast salasõna sisestamist õiguse juurde pääseda piiratud andmetele ja ressurssidele.
Monitoorimine	Protsess, mille käigus jälgitakse ja hinnatakse süsteemi, teenuse või tegevuse jõudlust ja turvalisust. Monitoorimise eesmärk on tuvastada ja reageerida võimalikele probleemidele, ohtudele või kõrvalekalletele varases staadiumis, et tagada süsteemide katkematu ja turvaline toimimine.
Pilverakendus	Interneti kaudu kasutatav tarkvara, mis töötab väljaspool asutuse vahetut kontrolli olevas kaugserveris.
Salasõna	Salajane märgijada, millega tõestatakse oma isikusamasust arvutisüsteemi või rakendusse sisenemisel.
Turvanõrkus	Viga tööprotsessis või arvutirakenduses (sh konfiguratsioonis), mida on saab kuritarvitada pahatahtlikel eesmärkidel, näiteks arvutisüsteemile ligi saamiseks või info hankimiseks.

3. Kasutaja üldised kohustused

3.1. Kasutaja kohustub:

3.1.1. **kasutama ja kaitsma temale määratud kasutajatunnuseid, sh**

3.1.1.1. asendama talle antav esmane salasõna (parool) esimesel sisselogimisel;

3.1.1.2. hoidma saladuses oma kasutajatunnust ja salasõna (parool), mitte jagama neid teistega;

3.1.1.3. kasutama erinevates infosüsteemides ja internetikeskkondades erinevaid paroole ning mitte kasutama varem kasutusel olnud paroole, enda ja oma lähedaste isikuandmeid või muid seotud andmeid st välistama kasutaja isiku identifitseerimise võimaluse.;

3.1.1.4. kasutama parooli, mis on vähemalt kümme tähemärki pikk, sisaldab suur- ja väiketähti ning numbreid, kirjavahemärke või muid sümboleid. Soovitavalt kasutama täiendava turvameetmena kaheastmelist autentimislahendust infosüsteemides, kus see on saadaval;

3.1.1.5. vahetama oma parooli vähemalt 1 kord aastas;

3.1.1.6. teavitama koheselt IT-juhile või infoturbejuhile ning vahetama esimesel võimalusel parool, kui see on saanud teatavaks teistele isikutele või on tekkinud sellekohane kahtlus.

3.1.1.7. mitte kasutama teiste kasutajate kasutajatunnuseid;

3.1.2. **kaitsma kooli andmeid ja vara**, sh

3.1.2.1. vältima andmete lubamatut levitamist, s.h. kooli õpilaste isikuandmete levitamist

3.1.2.2. kaitsma oma käsutusse antud asutuse vara, sh tagades nende järelevalve;

3.1.2.3. tagama, et kõrvalistel isikutel ei oleks võimalik ligi pääseda kasutajale ligipääsetavaks tehtud andmetele ega neid lugeda;

3.1.2.4. tagama, et kõrvalistel isikutel ei oleks võimalik kirjutada tema failikataloogidesse ega failidesse;

3.1.2.5. tagama asutuse vara ja andmete kaitstuse nende kasutamisel väljaspool asutuse arvutivõrku.

3.1.3. **järgima õigusakte ja käituma eetiliselt**, sh

3.1.3.1. kasutama asutuse IT-vara ja teavet vaid lubatud tegevusteks;

3.1.3.2. järgima asutuse regulatsioone, riigi õigusakte ning üldtunnustatud moraali- ja eetikanorme;

3.1.3.3. läbima õigeaegselt kõik ettenähtud IT ja infoturbe-alased koolitused.

3.1.4. **olema vastutustundlik**, sh

3.1.4.1. järgima turvanõudeid ning mitte kuritarvitama tuvastatud turvanõrkuseid;

3.1.4.2. andma esimesel võimalusel infoturbejuhile teada kõigist turvarikkumistest ning leitud turvanõrkustest.

3.1.5. **austama teiste õiguseid**, sh

3.1.5.1. kasutama teiste andmeid ja intellektuaalset omandit vaid legaalsel viisil;

3.1.5.2. mitte takistama teiste kasutajate õiguspäraseid tegevusi.

4. Üldised kasutustingimused

4.1. Kooli IT-vara ja teave on ette nähtud kasutamiseks kooskõlas asutuse eesmärkidega.

4.2. Kasutaja vastutab enda kasutajakontoga infosüsteemis ja arvutivõrgus tehtud toimingute (sh erinevate internetilehekülgede, sotsiaalmeedia, suhtlusportaalides tehtavad toimingud) ja infosüsteemi sisestatud andmete õigsuse eest.

4.3. Kasutaja toiminguid infosüsteemides ja arvutivõrgus logitakse ning nende õiguspärasuse üle teostab järelevalvet infoturbe ja IT-juht. Intsidentide ennetamiseks ja tõkestamiseks võib kool jälgida (monitoorida) kõigi kasutajate tegevust asutuse IT-seadmetes, IT-süsteemides ja arvutivõrkudes, ning võib vajadusel piirata või tõkestada kasutaja tegevust või selle tulemusel toimuvat andmete liikumist.

4.4. Kasutaja teatab viivitamatult kooli IT-vara või teabega seotud kahjulikest sündmustest või eeskirjade rikkumistest (intsident) IT-juhti (email: kool@gymnaasium.ee, tel 5681 3034) või infoturbe kontaktisikut.

4.5. Intsidendi uurimisel on kasutaja kohustatud aitama kaasa juhtunu selgitamisele.

5. Turvakoolitus ja teadlikkus

5.1. Kõik asutuse töötajad peavad läbima turvateadlikkuse koolituse iga kahe aasta järel.

5.2. Kõik asutuse uued töötajad peavad läbima turvateadlikkuse koolituse hiljemalt 30. päeva jooksul pärast tööle asumist. Selle käigus antakse töötajale ülevaade kehtivatest infoturbe nõuetest, tavadest ja tegevusjuhistest ning selgitatakse igapäevaseid tööprotseduure, infoturvameetmeid ning nende mõju äriprotsessile ja töökeskkonnale.

5.3. Turvakoolituse läbiviimise eest vastutab infoturbejuht.

6. Tarkvara ja riistvara

6.1. Kasutaja vastutab tema valduses oleva asutuse vara ja teabe eest.

6.2. Kasutajale tööülesannete täitmiseks antud riist- ja tarkvara tuleb kasutada tööeesmärgil.

6.3. IT-varade tervikluse ja turvalisuse säilitamiseks ning haavatavuste või pahavara sisseviimise vältimiseks *ei ole* kasutajal lubatud installeerida täiendavat riist- või tarkvara tööarvutisse ilma IT-juhi loata, välja arvatud automaatsed tarkvara täiendused ja uuendused, ühendada uut riistvara asutuse sisevõrku ning seadmeid sisevõrgus ümber paigutada, välja arvatud sülearvutid.

6.4. Kasutaja kohustub viivitamatult teavitama IT-juhti infotehnoloogiliste seadmetega seotud probleemidest või arvutitöökohast pahavara avastamise kahtluse korral.

6.5. Töölepingu lõppemisel on kasutaja kohustatud tagastama koheselt kõik tema käsutuses olnud infotehnoloogilised seadmed.

7. Juurdepääsuõigused

7.1. Kasutaja juurdepääsuõigus on tagatud talle tööalaseks kasutamiseks antud kasutajatunnusega. Kasutajatunnus on personaalne ja seda ei ole lubatud edasi anda teistele isikutele kasutamiseks.

7.2. Kasutaja vastutab isiklikult oma kasutajatunnusega teostatud toimingute eest.

7.3. Esmasel sisselogimisel infosüsteemi peab kasutaja ära muutma IT-juhi poolt antud salasõna. Salasõna tuleb sisestada kõrvalistele isikutele märkamatult. Salasõna peab koosnema soovitavalt vähemalt 10-st tähe-numbri kombinatsiooni moodustavast sümbolist ning välistama kasutaja isiku identifitseerimise võimaluse.

7.4. Turvalisuse tagamiseks ei ole lubatud salasõna üles kirjutada, samuti elektrooniliselt edastada, välja arvatud töövajadusest tingitud erandolukorras. Sellisel juhul edastatakse salasõna krüpteeritult.

7.5. Kui on tekkinud kahtlus, et salasõna on saanud teatavaks kõrvalistele isikutele, tuleb viivitamatult kasutusele võtta uus salasõna.

7.6. Töökohalt pikemaks ajaks lahkudes peab kasutaja end arvutist välja logima või kasutajakonto ajutiselt lukustama.

8. Andmeturve

8.1. Kasutajal on keelatud asutuse konfidentsiaalset teavet salvestada oma isiklikesse seadmetesse.

8.2. Füüsilisel viisil edastatav konfidentsiaalne teave peab olema kaitstud kooskõlas kooli nõuetega. Konfidentsiaalse teabe füüsilise edastamise korral peab seda tegema isiklikult või kasutama asutuse poolt heakskiidetud kullerteenust.

8.3. Konfidentsiaalse või siseteabe jagamiseks, salvestamiseks ja digitaalseks edastamiseks võib kasutada ainult kooli poolt lubatud IT-teenuseid ja pilverakendusi.

8.4. Konfidentsiaalset ja siseteavet on pilveteenuse vahendusel lubatud edastada ainult krüpteerituna.

8.5. Teavet tuleb käsitleda vastavalt tema tundlikkusele, sh jagada, käsitseda, edastada, salvestada ja hävitada.

8.6. Kasutaja ei tohi pidada konfidentsiaalseid vestlusi avalikes kohtades, avatud kontorites ja kohtumispaikades või ebaturvaliste sidekanalite kaudu.

8.7. Kõik konfidentsiaalset teavet sisaldavad elektroonilised andmekandjad tuleb peale kasutuse lõppu turvaliselt kõrvaldada kooskõlas kooli poolt kehtestatud nõuetega.

8.8. Kasutaja ei tohi kustutada kooli andmeid ilma oma otsese juhi loata.

9. Irdseadmete kasutamine

9.1. Kasutaja isiklike irdseadmete kasutamine on keelatud.

9.2. Irdseadmeid ei tohi jätta järelevalveta. Asutuses leitud irdseadmed tuleb viia IT-kasutajatoe kätte, nende kasutamine on keelatud.

9.3. Konfidentsiaalset ja siseteavet tohib irdkandjale salvestada ainult krüpteeritud kujul. Kasutaja vastutab krüpteerimisvõtme säilitamise eest.

9.4. Kõiki eemaldatavaid andmekandjaid tuleb hoida turvaliselt.

9.5. Koolile kuuluva irdseadme kaotsiminekust või vargusest tuleb teavitada koheselt IT-juhti ja infoturbejuhti, täpsustades irdseadmele salvestatud teabe olemust ning seda, kas irdseade või sellele salvestatud teave oli krüpteeritud.

10. Internet

10.1. Kasutaja on kohustatud interneti kasutamisel tegutsema legaalselt ning lähtuma üldkehtivatest eetikanormidest ja isiku eraelu puutumatuse põhimõttest. Kasutaja vastutab interneti kaudu edastatud info eest.

10.2. Interneti kasutamine ebasündsatel eesmärkidel, samuti tundmatute ja illegaalsete failide allalaadimine või käivitamine on keelatud.

10.3. Interneti kasutamisel sülearvutis avalikes traadita võrkudes tuleb arvestada võimalusega, et võrk on ebaturvaline ning edastatav info võib sattuda kõrvaliste isikute valdusesse.

11. E-post ja OneDrive

11.1. Kasutaja tööle asumisel loob kool talle personaalse kasutajakonto koos privaatse OneDrive ruumi ning e-posti aadressi. Töölt lahkumisel kasutajakonto ja e-posti aadress suletakse.

11.2. E-posti aadress ja OneDrive on antud personaalseks kasutamiseks tööalaselt. Keelatud on edastada e-posti ja hoida OneDrive's faile, mille sisu on illegaalne, ebaeetiline, seotud isikliku tulu teenimisega või kahjustab asutuse mainet.

11.3. E-posti lugemiseks ja saatmiseks tuleb kasutada kooli poolt seadistatud klienditarkvara või asutuse e-posti veebiteenust.

11.4. E-posti ja OneDrive ressursi tahtlik raiskamine või muu tegevus, mis häirib süsteemi kasutust asutuse poolt määratud otstarbel, on keelatud. E-posti manuse maksimaalne lubatud suurus on 25 megabaiti, mida vajadusel suurendatakse.

11.5. Kasutaja on kohustatud regulaarselt korrastama oma e-posti ja OneDrive's asuvaid andmeid, kustutades või arhiveerides ebaolulised kirjad ja failid.

11.6. Kasutajal on keelatud avada kahtlasena tunduvalt aadressilt saabunud e-kirjas olevaid linke või manuseid ning ta on kohustatud teavitama olukorrast IT-juhti ja infoturbejuhti.

11.7. Kasutajal on keelatud kasutada e-posti aadressi erasuhtluseks.

12. Viirustõrje

12.1. Viiruse või ründetarkvara kahtlusega e-posti manuste, veebilehtede, failide ning internetiviidete avamine on keelatud.

12.2. Viiruse või ründetarkvara avastamisel tuleb viivitamatult teavitada it-juhti ning seisata oma töö arvutis kuni IT-juhilt loa saamiseni töö jätkamiseks.

12.3. Arvutite, serverite ja andmekandjate teadlik nakatamine viiruste või ründetarkvaraga on keelatud, samuti automaatse taustkontrolli väljalülitamine, viirustõrjeprogrammide määrangute muutmine ning aktiveerunud ründetarkvara omaalgatuslik eemaldamine.

13. Kaugtöökoht, andmekandjad, sülearvutid

13.1. Kaugtöötamise kord ja tingimused on sätestatud asutuse töökorralduse reeglites.

13.2. Tööülesannete täitmisel väljaspool põhitöökohta peab olema tagatud kaugtöökoha turvalisus.

13.3. Mobiilsete seadmete (sülearvutid, välised kõvakettad, mälupulgad jms) järelevalveta jätmine ning muul moel kõrvalistele isikutele volitamata ligipääsu võimaldamine on keelatud.

13.4. Mistahes andmekandja üleandmisel teisele isikule tuleb veenduda selles, et kõik mittevajalikud andmed on taastamatult kustutatud.

13.5. Mobiilsete seadmete ja andmekandjate rikkumisest või kadumisest tuleb koheselt teavitada IT-juhti.

14. Puhta laua poliitika

14.1. Kasutaja on kohustatud IT-teenusest või arvutist välja logima, kui neid hetkel enam ei kasutata.

14.2. Konfidentsiaalset või tundlikku materjali ei tohi jätta järelevalveta. See tuleb koheselt töölaualt eemaldada, nt paigutada lukustatud sahtlisse kui töökoht on järelevalveta. Füüsilisi ja/või elektroonilisi võtmeid, mida kasutatakse konfidentsiaalsele teabele juurdepääsuks, ei tohi jätta järelevalveta lauale ega järelevalveta tööruumi, kui tööruum ise ei ole füüsiliselt kaitstud.

14.3. Järelevalveta arvutid peavad olema välja logitud/lukustatud või kaitstud parooliga.

14.4. Kasutajal tuleb konfidentsiaalne dokumentatsioon eemaldada peale printimist või kopeerimist koheselt printeritest või koopiamasinatest.

14.5. Kõik mittevajalikud tundlikud materjalid tuleb hävitada, sh trükised tuleb ära visata konfidentsiaalsesse prügikasti või hävitada dokumendi purustaja abil.

14.6. Kõik mittevajalik tundlik teave tuleb koosolekuruumidest eemaldada iga koosoleku lõpus

15. Kasutajatunnuste sulgemine

15.1. Kooliga lepingulise suhte lõppemisele eelnevalt peab kasutaja:

15.1.1. andma üle asutusele kuuluva teabe;

15.1.2. tagastama kasutaja valduses olevad kooli IT-vara;

15.1.3. eemaldama oma isiklikud andmed asutuse seadmetest.