

SILLAMÄE GÜMNAASIUMI INFOTURBE POLIITIKA

1. Sissejuhatus

- 1.1. Käesolev poliitika määratleb infoturbe strateegia üldalused ja sellega on kohustatud tutvuma Sillamäe Gümnaasiumi (edaspidi *kool*) töötajad.
- 1.2. Sillamäe Gümnaasiumi infoturbe poliitika eesmärk on deklareerida valdkonnaga tegelemise vajalikkust ning kirjeldada Sillamäe Gümnaasiumi üldist, strateegilist lähenemisviisi infoturbe tagamisel.

2. Mõisted

- 2.1. Kooli infosüsteemide varad (edaspidi *infovara*) on käesoleva poliitika tähenduses koolis kasutusel olevad infotehnoloogilised vahendid ja viimaste abil töödeldavad andmed. Infotehnoloogilised vahendid on riist-, tarkvara ja andmesideseadmed.
- 2.2. Andmed võivad olla mis tahes viisil ja mis tahes andmekandjale jäädvustatud või dokumenteeritud teave ning kõikvõimalike (infotehnoloogiliste) vahendite abil edastatav või töödeldav teave.
- 2.3. Infoturbe ehk andmekaitse tähendab andmete kolme põhiomaduse – tervikluse, käideldavuse ja konfidentsiaalsuse tagamist, kus:
 - 2.3.1. käideldavus tähendab informatsiooni kasutuskõlblikkust ja õigeaegset kättesaadavust volitatud isikule;
 - 2.3.2. terviklus tähendab, et info pärineb autentsest allikast ning seda ei ole volitamatu muudetud ega kustutatud;
 - 2.3.3. konfidentsiaalsus tähendab, et informatsioon on kättesaadav vaid volitatud isikutele.
- 2.4. Infoturbe haldus on protsess, mida kasutatakse infovara konfidentsiaalsuse, tervikluse ja käideldavuse asjakohaste tasemete saavutamiseks ja säilitamiseks.
- 2.5. Konfidentsiaalseks ehk avaldamisele mitte kuuluvaks teabeks peetakse selliseid andmeid, millele on juurdepääs lepingu või seaduse alusel või mis on mõnel muul alusel kuulutatud mitteavalikuks.
- 2.6. Infoturbeintsidendiks loetakse kõiki reaalse või potentsiaalse kahju juhtumeid, mis võivad ohustada või halvata infovara turvalisust, põhjustades nende käideldavuse (töökindlus), tervikluse (andmete õigsuse ja muutumatus) või konfidentsiaalsuse (andmete salastatuse) kao. Infoturbeintsidentideks loetakse muuhulgas ka toimingud, mis ei ole infoturbe valdkonda reguleerivate õigusaktidega kooskõlas.

3. Infoturbe eesmärk

- 3.1. Kool täidab seadusest tulenevaid ja Vabariigi Valitsuse poolt seaduse alusel kehtestatud põhimääruses antud ülesandeid. Kooli põhiülesanded ning kehtivas arengukavas määratud eesmärgid ja nendeni jõudmise teed on kõik erineval määral seotud infotehnoloogia ja selle võimalustega.
- 3.2. Kooli infoturbe eesmärkideks on tagada:

- 3.2.1. igapäevane asjaajamine ja infovahetus, kus põhieesmärgiks on töötaja ootustele vastava, stabiilse, turvalise ja töökindla töökeskkonna tagamine ja talitlusvõime säilitamine;
- 3.2.2. kooli ning õpilaste ja vanamate vaheline infovahetus, kus eesmärgiks on edastada õigeaegne informatsioon õppeprotsessi kohta.
- 3.2.3. töötlemiseks või hoidmiseks antud andmete konfidentsiaalsus ja terviklus;
- 3.2.4. infosüsteemide ja andmekogude pidamine vastavalt Eesti Vabariigis kehtivatest õigusaktidest tulenevatele infoturbenõuetele.

4. Infoturbe organisatsioon ja juhtimine

- 4.1. Infoturbe toimimiseks on vajalik lisaks eesmärkide teadvustamisele, et koolis oleks kindlalt määratletud turvaalased rollid ja vastutused. Infoturbe on kooli kollektiivne tegevus ja kõikide töötajate kohustus. Iga töötaja peab teadma, milles seisneb tema panus infoturbesse.
- 4.2. Infoturbealane vastutus jaguneb üldiseks ja konkreetseks vastutuseks:
- 4.3. Üldine infoturbealane vastutus on kooli töötajal ja seisneb antud valdkonda reguleerivate kordade järgimises ning infoturbeintsidentidest teavitamises.
- 4.4. Konkreetne, st rolli- või ametikohapõhine vastutus järgib kooli struktuurilist ülesehitust, üldist töökorraldust, tegevusvaldkondi ja kehtivaid delegerimispõhimõtteid. Kõige kõrgemal tasemel on vastutajaks kooli juhtkond, seejärel kandub vastutus edasi iga töötaja individuaalse turvaalase vastutuseni välja.
- 4.5. Infoturbealased otsused teeb kooli juhtkond talle esitatud ettepanekute alusel.
- 4.6. Administraator on käesoleva poliitika mõistes isik, kes teostab infovarade haldust, tagades nendega töötamiseks vajalikud tingimused. Administraatori ülesanneteks on:
- 4.7. infoturbalase aruandluse ja statistika läbivaatamine;
 - 4.7.1. suurematele infoturbalastele probleemidele lahenduste leidmine;
 - 4.7.2. infoturbalaste prioriteetide paika panemine;
 - 4.7.3. infoturbalaste ostuste tegemine oma volituste piires.

5. Infoturbe protsess

- 5.1. Turvameetmete pideva asjakohasuse tagamiseks on vajalik turvameetmete hooldus, regulatsioonide perioodilised läbivaatused, töökeskkonna igapäevane seire, infoturbe perioodiline vastavusekontroll, muudatustele reageerimine ja infoturbeintsidentide käsitlemine.
- 5.2. Kõiki infosüsteemi muudatusi tuleb enne nende läbiviimist kaaluda infoturbe seisukohast. Muutunud nõuete või uute ohtude korral tuleb turvameetmed ümber hinnata.
- 5.3. Kooli jaoks on väga oluline pidev turvanõuete vastavuse kontroll, et tagada turvanõuete täitmine ning turvanõuete vastavus tegelikule olukorrale.

6. Infoturbeintsident ja kontrolljäljed

- 6.1. Infoturbeintsidentist ja selle ohust peab iga töötaja võimalikult kiiresti teavitama kooli infosüsteemide administraatorit.
Infoturbeintsidentide lahendamine toimub administraatori või direktori poolt selleks määratud isiku koordineerimisel, kes rakendab vastavalt tekkinud olukorrale asjakohast reageerimist. Infoturbeintsidentide avastamise üheks eelduseks on jälitatavuse toimivus.

- 6.2. Intsidendi lahendamise käigus kogutud informatsioon dokumenteeritakse ja analüüsitakse eesmärgiga vältida sarnaste intsidentide aset leidmist tulevikus ning otsustamaks täiendavate turvameetmete rakendamise vajaduse üle.
- 6.3. Kui turvaintsidendi lahendamise käigus avastatakse kuriteo, väärteo- või distsiplinaarsüüteo või töölepingu rikkumise tunnused, antakse juhtum edasi menetlemiseks vastava menetluse läbiviimise õigust omavale asutusele või isikule.

7. **Konfidentsiaalkohustuse nõue**

- 7.1. 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.
- 7.2. Töötaja, kes puutub tööülesannete täitmisel või töö käigus juhuslikult kokku konfidentsiaalsete andmetega, kohustub minimaalselt:
 - 7.2.1. mitte avalikustama temale teatavaks saanud konfidentsiaalset informatsiooni, välja arvatud kui see on seadusega kohustuslik või vajalik tööülesannete täitmiseks;
 - 7.2.2. järgima kehtivaid andmekaitset puudutavaid õigusakte ja kordasid;
 - 7.2.3. täitma konfidentsiaalkohustuse nõudeid nii töösuhte ajal kui ka peale selle lõppemist.