JÕHVI VALLAVALITSUS
MÄÄRUS

Jõhvi 19.05.2026 **nr 12**

Jõhvi valla infoturvapoliitika

Määrus antakse kohaliku omavalitsuse korralduse seaduse § 30 lg 1 punkti 3, küberturvalisuse seaduse § 7 lg 6, Vabariigi Valitsuse 09.12.2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 5 lõike 1 ning ettevõtlus- ja infotehnoloogiaministri 16.12.2022 määruse nr 101 „Eesti infoturbestandard“ lisa 1 punkti 6.6 alusel.

§ 1. Infoturvapoliitika sisu ja eesmärk

(1) Jõhvi valla infoturvapoliitika (edaspidi ka *poliitika*) on Jõhvi Vallavalitsuse kui ametiasutuse (edaspidi *ametiasutus*) ja ametiasutuse hallatavate asutuste (edaspidi *hallatav asutus*, koos *asutused*) infoturbe juhtdokument, milles esitatakse asutuse juhtkonna (valitsus kui täitevorgan) infoturbealane kohustumus ning sõnastatakse organisatsiooni infoturbe sihid, vajadused ja põhimõtted, millest kõrvale kaldumine lepitakse vajadusel kokku valdkonna põhiselt või asutusega eraldi.

(2) Asutuste infoturbe eesmärk on tagada nende põhimäärustes loetletud valdkondades poliitika kujundamiseks ja elluviimiseks vajaliku teabe käideldavus, terviklus ja konfidentsiaalsus otstarbekohasel tasemel.

(3) Infoturvet korraldatakse asutustes kooskõlas Eestis kehtivate õigusaktidega, millest tähtsaim on küberturvalisuse seadus, järgides Eesti infoturbestandardi suuniseid, infotehnoloogia häid tavasid, parimaid praktikaid ning, mudeleid ja mõisteid.

(4) Infoturve lähtub asutuse eesmärkidest ja olulistest äriprotsessidest. Infoturbe ülesanne on säilitada äriprotsesside käigus töödeldava teabe turvalisus.

(5) Infoturve kaitseb asutust ohtude eest üksnes äriprotsessidesse loomuliku osana lõimituna. Äriprotsessid, teave ja äriprotsesse teenindavad varad on arvele võetud ja vastutajad määratud.

(6) Infoturbe nõuetega peavad kursis olema ning neid oma töös arvestama kõik ametnikud, töötajad ja teised isikud (edaspidi koos *teenistujad*), kes mõne lepingu alusel asutusele teenust osutavad, on ametisse nimetatud või tööülesandeid täidavad.

(7) Infoturve tagatakse meetmetega, mis on vastavuses äriprotsessi kaitsetarbe ja nõuetega.

(8) Infoturbe korraldamisel eeldatakse, et ükski turvameede ei loo absoluutset turvalisust, need vaid vähendavad turvariski ehk tõenäosust, et andmete terviklus, käideldavus või konfidentsiaalsus kahjustuvad.

§ 2. Terminid

Käesolevas poliitikas kasutatakse termineid järgmises tähenduses:
1) infoturve – teabe põhiomaduste käideldavuse, tervikluse ja konfidentsiaalsuse tagamine;
2) käideldavus – vajalikul ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ning hõlbus kättesaadavus selleks volitatud isikule või tehnilisele vahendile;
3) terviklus – andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine;
4) konfidentsiaalsus – andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile;
5) andmed – mistahes viisil ja mistahes andmekandjale jäädvustatud ning kõikvõimalike (infotehnoloogiliste) vahendite abil edastatav või töödeldav teave;
6) isikuandmed – kõik andmed füüsilise isiku kohta, mille alusel on isiku tuvastamine otseselt või kaudselt võimalik, sõltumata sellest, millisel kujul või millises vormis need andmed on;
7) juhtkond – Jõhvi vallavalitsus kui täitevorgan ja hallatavas asutuses direktor või juhataja;
8) äriprotsess – kogum loogiliselt seotud tegevusi, mis sooritatakse asutuse eesmärkide saavutamiseks. Äriprotsessi tulemusena võidakse luua sise- või väliskliendile väärtust toodete või teenustena;
9) vara – miski, mida asutus, isik või riik oma olemasoluks ja tegutsemiseks vajab ning millel on selle omaniku jaoks väärtus. Varade hulka kuuluvad näiteks teave, andmed, tarkvara, füüsiline vara (taristu, hoone, riistvara, sisseseade), rahaline vara, teenus, inimressurss (inimesed, kvalifikatsioon, oskused, kogemused), oskusteave, mitteaineline vara (maine, kuvand);
10) infoturbe- või turvameetmed ehk meetmed – organisatsioonilised, füüsilised ja infotehnilised toimingud või vahendid andmete ja süsteemide turvalisuse saavutamiseks ning säilitamiseks;
11) infoturbeintsident – soovimatu või ootamatu sündmus, mis võib ohustada teabe turvalisust ja kahjustada asutuse tegevust näiteks konfidentsiaalsete andmete lekkimise, andmete hävimise, tööseisaku, IT teenuse katkemise ja asutuse maine rikkumise kaudu;
12) infoturbeintsidentide haldus – protsessid infoturbeintsidentide avastamiseks, neist teatamiseks, nende hindamiseks, neile reageerimiseks, nende käsitluseks ja neist õppimiseks;
13) infosüsteem – äriprotsesside ja -teenuste toetamiseks ja/või võimaldamiseks vajalike vahendite ja põhimõtete kogum, tark- ja riistvarast koosnev infotehnoloogiline lahendus, mille abil kogutakse, töödeldakse, säilitatakse ja väljastatakse andmeid;
14) teenuseosutaja – asutusele infotehnoloogia- ja kommunikatsiooniteenuseid (edaspidi *IT*) või teisi teabe turvalisusega seotud teenuseid kokkulepitud tingimustel ja tasemel osutav organisatsioon või isik;
15) andmete varundamine – andmetest varukoopiate tegemine, et võimaldada andmete taastamist arvutites ja süsteemides;
16) andmekandja – vahend informatsiooni salvestamiseks, säilitamiseks ja taaskasutamiseks;
17) krüptimine – informatsiooni kaitsmise võimalus, muutes andmed loetamatuks ja kasutamiskõlbmatuks inimesele, kellel puudub vastav dekrüptimise võti;
18) tulemüür – tarkvara või seade, mis turvakaalutlustel piirab ja reguleerib võrguliiklust arvutivõrgus või võrkude vahel vastavalt seadistatud reeglitele. Tulemüüri esmane otstarve on väljastpoolt juurdepääsu takistamine ressurssidele, millele pole sellist juurdepääsu ette nähtud;
19) virtuaalne privaatvõrk ehk VPN (*Virtual Private Network*) – privaatne ja turvaline arvutivõrk, mille loomiseks kasutatakse avalikku sidetaristut.

§ 3. Infoturbe korraldamine asutustes

(1) Infoturbe tagamise ja põhimõtete rakendamise eest asutustes vastutavad asutuste juhid, sh igale äriprotsessile ja/või teenusele vastutava isiku määramise korraldamise eest.

(2) Infoturbe jääkriskid hinnatakse ja aktsepteeritakse ametiasutuses juhtkonna ning hallatavates

asutustes juhi tasemel.

(3) Ametiasutuse infoturbe ja andmekaitse komisjon koordineerib infoturbe- ja andmekaitsealast tegevust asutustes.

(4) Asutused tagavad teabe kaitse vastavalt teabe väärtusest tulenevale kaitsetarbele, ohtude realiseerumise tõenäosusele ja õigusaktides esitatud nõuetele. Andmete turvaliseks töötlemiseks kindlustatakse nõuetele vastav keskkond.

(5) Asutuste teenistujate teadlikkuse tõstmine ja küberhügieen on infoturbe peamine tagatis ning teenistujatele korraldatakse regulaarselt vastavaid koolitusi, mille läbimine on kohustuslik. Asutuste teenistujad läbivad igal aastal küberturvalisuse riikliku digitesti.

(6) IT juht korraldab koostöös ametiasutuse juhiga, IT spetsialistiga või asutuse IT teenust osutava isikuga teenistujate teavitamise infoturbe meetmetest ja -ohtudest.

(7) Infoturbe nõuetega arvestatakse infosüsteemide arendamisel ja muutmisel, samuti nende soetamisel. Turvauuendused paigaldatakse esimesel võimalusel. Infosüsteemi või selle muudatusi testitakse enne kasutusele võtmist.

(8) Kriitiliste infosüsteemide jaoks koostatakse taasteplaan.

(9) Kõik asutuse seadmed, sh võrguseadmed ja püsikaabeldus, peavad olema arusaadavalt tähistatud ja dokumenteeritud.

(10) Infoturvet puudutavad asutuseülesed muudatused ja infoturbe erijuhud kooskõlastatakse IT juhiga.

§ 4. Kasutusulatus ja vastutus

(1) Poliitika laieneb kõigile asutustele ja kehtib kõigis asukohtades, samuti tuleb põhimõtteid arvestada koostöös teenusepakkujatega.

(2) Rolli- või ametikohapõhine infoturbealane vastutus tuleneb asutuse struktuurist, üldisest töökorraldusest, tegevusvaldkondadest ja delegeerimispõhimõtetest.

(3) Asutuste äriprotsessid ja protsessijuhid kinnitatakse eraldi asutuse juhi käskkirjaga.

(4) Asutuste teenistujatele kohalduvad täpsemad infoturbe reeglid sätestatakse asutuse infosüsteemi(de) kasutamise korraga, mis lähtub käesolevast poliitikast.

(5) Infoturbe korraldust asutustes koordineerib ametiasutuse IT juht, kes:
1) esindab asutust riiklikku infoturbe korraldust puudutavates küsimustes;
2) teeb koostööd Riigi Infosüsteemi Ametiga;
3) teavitab asutusi olulistest muudatustest nõuetes;
4) osaleb andmekogude turvaklassi määramisel;
5) suhtleb asutustega intsidentide käsitlemisel ja vajadusel nõustab infoturbe korraldamisel;
6) vastutab asutuses infoturbe poliitika väljatöötamise ja uuendamise eest;
7) kavandab auditeid ning kontrollib turvalisust põhjendatud vajadusel ka erakorraliselt.

(6) Iga asutuse teenistuja, kes kasutab oma teenistus- või tööülesannete täitmiseks IT teenuseid (rakendusi), vastutab infoturbe meetmete rakendamise eest oma tööülesannete täitmisel ning täidab

infoturbe nõudeid ja rakendab asjakohaseid turvameetmeid.

(7) Protsessijuht vastutab äriprotsessi (teenuse) kujundamise, arendamise, juhtimise ja seire eest, sealhulgas teabe töötlemise eesmärgipärasuse eest.

(8) IT juht, IT spetsialist või IT teenust osutav isik vastutab infoturbemeetmete rakendamise eest asutuses, sh asutuses kasutusel olevate infosüsteemide ja tulemüüri toimimise, andmete varundamise ja nende säilimise ja/või kustutamise ning IT tehnilise riistvara korrasoleku ja arvestuse eest.

(9) Andmekaitsespetsialist või andmekaitsespetsialisti ülesandeid täitev teenistuja vastutab isikuandmete kaitse alase teadlikkuse tõstmise eest oma asutustes ning abistab ja kontrollib andmetöötlejat isikuandmete kaitse üldmääruse (Euroopa Parlamendi ja nõukogu määruses (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) täitmisel, samuti koostab oma asutuse teenistujatele isikuandmete töötlemise täpsemad juhendid, mille kinnitab asutuse juht.

§ 5. Arvutitöökoha kasutamine

(1) Asutuse seadmed on ette nähtud tööülesannete täitmiseks.

(2) Tööülesannete täitmiseks loodud e-posti aadressi kasutamist eraviisiliseks otstarbeks tuleb vältida.

(3) Avaliku interneti kasutamine peab toimuma viisil, mis ei kahjusta asutuse ega teenuste mainet.

(4) Asutuse seadmesse tarkvara lisamise, seadmise või eemaldamise eest vastutab ametiasutuse IT spetsialist või asutuse IT teenust osutav isik. Tavakasutajal puuduvad administraatoriõigused. Tarkvara hangitakse ja seda kasutatakse kooskõlas õigusaktides esitatud nõuetega.

(5) Kõikidesse asutuse töökohaarvutitesse on paigaldatud tulemüüritarkvara ning keskselt hallatav viirusetõrje tarkvara, mille eemaldamine või välja lülitamine on keelatud.

(6) Kõikide sülearvutite kõvaketastel on rakendatud krüptimislahendus.

(7) Väliseid andmekandjaid on asutustes keelatud kasutada.

(8) Asutused kehtestavad eraldi haldusaktiga arvutite kasutamise korrad ja koostavad vajadusel asjakohased juhendid.

§ 6. Teabe töötlemine

(1) Teavet töödeldakse ja salvestatakse asutuse hallatavates või pakutavates keskkondades. Kasutajatel on lubatud kasutada ainult Eesti riigi hallatavaid pilveteenuseid või asutuste sõlmitud lepingu alusel kasutatavaid pilveteenuseid. Muudes pilveteenustes tööga seotud teabe töötlemine on keelatud.

(2) Andmete ja/või infosüsteemide ühiskasutamisel teiste organisatsioonide või asutustega tuleb tagada teabe õiguspärane töötlemine, mis lepitakse kokku kas andmevahetus- ja/või konfidentsiaalsuslepingus, kui andmete kasutus pole reguleeritud õigusaktiga.

(3) Teabele, mille suhtes on õigusaktidega kehtestatud juurdepääsupiirang (eelkõige isikuandmed),

kehtestatakse juurdepääsupiirang. Isikuandmete kaitse reeglid ei kehti, kui tegu on juriidilise isiku või asutuse andmetega või teave ei võimalda inimest mõistlike pingutustega tuvastada.

(4) Teabe käsitlemisel, sealhulgas suulises suhtluses, ei avaldata piiratud juurdepääsuga teavet isikutele, kellel puudub selleks õigustatud huvi. Piiratud juurdepääsuga teavet tohib väljastada üksnes juhul, kui on üheselt tuvastatud teabe saaja isik ja tema teabele juurdepääsu saamise õiguslik alus.

(5) Tavalisest tundlikumaid andmeid sisaldava teabe edastamisel andmed krüptitakse, kui nendele volitamatu juurdepääs võib tekitada märkimisväärset kahju.

(6) Kõik tarbetud paberkandjal olevad töödokumendid tuleb hävitada paberihundis või muul selleks ette nähtud turvalisel viisil.

§ 7. Juurdepääsud

(1) Juurdepääsupiiranguga teavet tohivad töödelda ainult teenistusülesannete täitmiseks volitatud isikud ettenähtud korras ja ulatuses ainult selleks õigustatud isikutele ettenähtud korras ja ulatuses. Juurdepääsupiirang määratakse vastavalt avaliku teabe seadusele, teistele õigusaktidele ja/või asutuse teabehalduse korrale.

(2) Igale teenistujale on loodud parooliga kaitstud isiklik kasutajakonto. IT spetsialist või asutuse IT teenust osutava isiku loodud kasutajakontot kasutatakse juurdepääsu andmiseks kõikjal, kus tehniliselt võimalik.

(3) Kasutajakonto parool on vähemalt 15 tähemärki pikk ning sisaldab vähemalt ühte suur- ja väiketähte ning numbrit ja sümbolit.

(4) Eelistatud on kasutaja autentimine ID-kaardi, Mobiil-ID, Smart-ID või füüsilise turbevõtme abil. Parooli kasutamisel lülitatakse võimalusel sisse mitmeastmeline autentimine.

(5) Iga teenistuja vastutab oma identiteedi kaitse eest. Sama kasutajakonto kasutamine mitme isiku poolt ei ole lubatud.

(6) Juurdepääs infosüsteemidele, andmetele, hoonetele ja ruumidele on rollipõhine ning põhjendatud vastavalt tööalasele vajadusele.

(7) Algparoolide kasutamine infosüsteemides on keelatud ja need tuleb vahetada esimesel sisselogimisel.

(8) Kaugjuurdepääs asutuse sisestele infosüsteemidele on lubatud üle VPNi, ametiasutuse IT spetsialisti või asutuse IT teenust osutava isiku hallatavatest seadmetest ja kindlaks määratud IT teenustele.

(9) Ruumid, sealhulgas tehnilise taristu ruumid peavad vastama tingimustele, mis tulenevad seal töödeldavate andmete kaitsetarbest.

(10) Välise teenusepakkuja personal tohib tehnilise taristu ruumi siseneda ja seal viibida ainult koos asutuse personali hulka kuuluva saatjaga, kellel on volitatud ligipääs.

(11) Juurdepääsude haldus peab olema regulaarselt kontrollitud, tuvastatav ja jälgitav.

(12) Ametiasutuse IT spetsialist või asutuse IT teenust osutav isik logib asutuse ressursside poole pöördumisi või pöördumiskatseid, mis sisaldavad minimaalselt infot nende aja, lähtekoha, tegija ja tegevuse kohta ning säilitab logisid. Logide säilitamine on kooskõlastatud asjasse puutuvate teenuste omanikega.

(13) Asutused korraldavad pääsuõiguste haldamise ja pääsuõiguste üle arvestuse pidamise.

§ 8. Arvutivõrgu turvalisuse tagamine

(1) Asutuse sisevõrk on välisvõrgust eraldatud tulemüüriga. Asutuse sisevõrk on minimaalselt jaotatud tulemüüriga eraldatud tsoonideks:
1) sisevõrk serveritele;
2) töökohaarvutitele;
3) traadita võrgule;
4) asutuse VPNi klientidele;
5) serveritele, mis on kättesaadavad välisvõrgust;
6) IOT süsteemidele;
7) valvekaameratele.

(2) Asutuse sisevõrgus asuvad seadmed ei tohi olla otse kättesaadavad väljastpoolt, välja arvatud seadmed, mis asuvad just selleks otstarbeks loodud võrgutsoonides.

(3) Asutuse sisevõrku lubatakse vaid ametiasutuse IT spetsialisti või asutuse IT teenust osutava isiku hallatavaid seadmeid. Võõrseadmete sisevõrku ühendamine ei ole lubatud.

(4) Asutused kehtestavad eraldi haldusaktiga arvutivõrgu turvalisuse rakendamiseks täpsema arvutivõrgu kasutamise korra ja kasutusõigused.

§ 9. Intsidentide üldine haldus

(1) Infoturbeintsidendi või intsidendiohu ilmnemise korral, sh töövälisel ajal, teavitab teenistuja sellest viivitamatult IT juhti ja ametiasutuse IT spetsialisti või asutuse IT teenust osutavat isikut.

(2) Kui intsident mõjutab isikuandmeid, siis teavitatakse intsidendist ka andmekaitsespetsialisti või andmekaitsespetsialisti ülesandeid täitvat teenistujat.

(3) Kõik infoturbeintsidendid dokumenteeritakse.

(4) Infoturbeintsidente käsitletakse asutuses kokkulepitud protseduuri järgi intsidendi põhjuste ja tagajärgede tuvastamiseks ning lahenduste leidmiseks sarnaste intsidentide vältimiseks tulevikus.

(5) Olulise mõjuga infoturbeintsidentidest teavitab IT juht asutuse juhtkonda ja Riigi Infosüsteemi Ametit.

(6) Intsidendil on oluline mõju, kui on täidetud vähemalt üks järgmistest tingimustest:
1) intsidendi tagajärg on vastavalt intsidentide käsitlemise korrale vähemalt suur;
2) intsidendi tõttu ei ole teenuse osutamist võimalik jätkata teenustaseme kokkuleppes või teenuse toimepidevuse nõuetes sätestatud teenuse maksimaalse lubatud katkestuse aja möödumisel;
3) intsidendi tõttu on häiritud teise teenuse osutaja teenuse toimepidevus;
4) intsidendi lahendamiseks tuleb rakendada erakorralisi abinõusid;
5) asutusele, teise teenuse osutajale või teenuse kasutajatele on intsidendi tõttu tekkinud või võib tekkida märkimisväärne kahju.

(7) Asutused kehtestavad asutuse juhi haldusaktiga turvaintsidentide käsitlemise korra.

§ 10. Riskihaldus, standardid ja mõjuhinnang

(1) Riskihaldus ja infoturbe meetmete rakendamine põhineb Eesti infoturbestandardil, millega määratakse minimaalsed meetmed, mida tuleb rakendada IT teenusele ettenähtud turvataseme saavutamiseks ja säilitamiseks.

(2) Kui mõnda turvameedet ei ole võimalik või otstarbekas täita, rakendatakse alternatiivsed meetmed riski leevendamiseks. Meetme mitterakendamise aktsepteerib asutuse juht kirjalikult.

(3) Riskide minimeerimiseks vastuvõetavale tasemele võetakse asutuses kasutusele järgmised meetmed:
1) füüsilised meetmed ruumidele (näiteks uste, akende, seinte ja lukkudega seotud abinõud);
2) organisatsioonilised meetmed teenistujatele (näiteks protseduurireeglid, korrad ja eeskirjad turvanõuete täitmiseks);
3) infotehnoloogilised meetmed infosüsteemidele ja andmekogudele (näiteks ligipääsuõiguste andmise ja kasutamisega, viirusetõrjega, krüptimisega, varukoopiate tegemise ja ID-kaardi kasutamisega seotud abinõud).

(4) Andmekogudega seotud turvameetmete rakendamisel järgitakse auditeeritavuse printsiipi. Rakendatavad turvameetmed peavad olema põhjendatud ja dokumenteeritud selliselt, et hiljem oleks võimalik hinnata nende vajalikkust ning asjakohasust.

(5) Andmekaitse mõjuhinnang viiakse läbi, kui isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib füüsiliste isikute õigustele ja vabadustele tõenäoliselt suur oht. Mõjuhinnang tuleb läbi viia ka siis, kui hakatakse kasutama (uut) tehnoloogiat, millega varem kokkupuudet pole olnud.

(6) Andmekaitse mõjuhinnangu koostamist korraldab andmekaitsespetsialist või andmekaitsespetsialisti ülesandeid täitev teenistuja.

§ 11. Infoturvapoliitika ülevaatus

(1) Infoturve pole ühekordne tegevus, vaid pidevalt toimiv protsess, mida toetab infoturbe halduse süsteem ehk poliitikad, juhised ja toimingud ning nendega seotud ressursid ja tegevused teabe põhiomaduste asjakohase taseme saavutamiseks ja säilitamiseks.

(2) Infoturvapoliitika vaadatakse üle ja vajadusel uuendatakse vähemalt üks kord aastas ning ülevaatuse korraldamise eest vastutab IT juht.

§ 12. Määruse rakendamine

(1) Jõhvi Vallavalitsuse 16.04.2024 määrus nr 22 „Jõhvi valla asutuste infoturbe põhimõtted” tunnistatakse kehtetuks.

(2) Määrus jõustub üldises korras.

(allkirjastatud digitaalselt)

Vallo Reimaa
Vallavanem

(allkirjastatud digitaalselt)

Piia Lipp
vallasekretär