

Infohalduse kord (K31)

Protsess: Infohaldus

Protsessi omanik: Kvaliteedijuht

Versioon: 1

Kinnitatud: 07.11.2024

Infohalduse kord sisaldab:

1. Üldosa
2. Infohalduse üldised põhimõtted
3. Kasutatavad infosüsteemid ja keskkonnad
4. Õiguste haldus
5. Failide loomine ja jagamine
6. Infohalduse optimaalne korraldus

LISAD – töökorra lisad on töödokumendid, mida ei kinnitata korra koosseisus käskkirjaga ja mille muutmise, täiendamise, täpsustamise õigus on protsessi omanikul. Lisa muutmisel tagab protsessi omanik, et muudetud lisa oleks avaldatud siseveebis ja töötajaid teavitataks olulisematest muudatustest.

1. Üldosa

1.1 Eesmärk ja ulatus

Infohaldus Riigi Tugiteenuste Keskuses (edaspidi RTK) on tugiprotsess, mille eesmärk on toetada organisatsiooni põhiprotsesse, ressursside efektiivset kasutamist ning laiemas plaanis organisatsiooni eesmärkide saavutamist. Korrektse infohalduse tulemuseks on kiired ja kvaliteetsed juhtimisotsused ning RTK tegevuse järjepidevus.

Riigi Tugiteenuste Keskuse infohalduse kord kehtestab infohalduse põhimõtted Riigi Tugiteenuste Keskuses. Infohalduse korra eesmärgiks on anda terviklik ülevaade organisatsiooni infohalduse põhimõtetest, kasutatavatest infosüsteemidest ja keskkondadest ning nende haldamisest.

Infohalduse tegevuseesmärkideks on kindlustada RTK:

- ülesannete täitmiseks vajalik info;
- info aktuaalsus;
- info nõuetekohasus;
- info säilimine;

- info käideldavus;
- info terviklus;
- info konfidentsiaalsus ja isikuandmete kaitse;
- infohalduse optimaalne korraldus.

Infohalduse kord (K31) selgitab RTK sisemist infohaldust kasutusulatusena kõigile RTK töötajatele.

Dokumendihalduse kord (K2) koordineerib RTK dokumendihaldus- ja arhiiviteenuste osakonna tööprotsessi dokumendihaldus- ja arhiiviteenuse osutamisel RTK-le.

1.2 Infohalduse korraldamine lähtub järgmistest õigusaktidest ja RTK töökordadest:

- [Arhiiviseadus](#);
- [Avaliku teabe seadus](#);
- [Isikuandmete kaitse seadus](#);
- Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 [Isikuandmete kaitse üldmäärus \(GDPR\)](#);
- Vabariigi Valitsuse 25.05.2017 määrus nr 88 [Teenuste korraldamise ja teabehalduse alused](#);
- Vabariigi Valitsuse 22.12.2011 määrus nr 181 [Arhiivieeskiri](#);
- [Riigi personali- ja palgaarvestuse andmekogu asutamine ja selle põhimäärus](#);
- [Riigihangete registri põhimäärus](#);
- [Struktuuritoetuse registri pidamise põhimäärus](#);
- [Rahvusarhiivi digiteerimise juhis asutustele](#);
- Dokumendihalduse kord (K2);
- Liigitusskeem;
- [Infosüsteemide kasutamise kord \(K8\)](#);
- [Personali värbamise ja töö- ning teenistussuhete haldamise kord \(K11\)](#);
- [Kommunikatsiooni korraldamise põhimõtted \(K28\)](#);
- [RTK juhtimissüsteemi käsiraamat \(K1\)](#).

1.3 Mõisted

Digiprügi - kasutatud, aegunud, dubleeritud andmed, mida enam keegi ei vaja ega kasuta ning mis ei loo lisaväärtust ei üksikindiviidi ega organisatsiooni tasandil.

Dokumendihaldus - infohalduse ala, mis tegeleb dokumentide loomise, saamise, säilitamise, kasutamise ning eraldamise tõhusa ja süstemaatilise juhtimisega, sealhulgas organisatsiooni tegevust ja toiminguid kajastava tõestusmaterjali ja informatsiooni dokumendihaldussüsteemi hõlmamise ning dokumentidena alalhoidmisega.

Dokument - mis tahes kandjale jäädvustatud terviklik info (sünonüüm: teave), mis on loodud või saadud asutuse või isiku tegevuse käigus ning mille sisu, vorm ja struktuur on küllaldane faktide või tegevuse tõendamiseks.

Dokumendihaldussüsteem - infosüsteem, mille ülesanne on dokumentide hõlmamine ja kontrollitud haldamine dokumendi elukäigu jooksul.

Info - teave, mis on kogutud, töödeldud, hoitud ja jagatud, et toetada organisatsiooni eesmärke ja tegevusi (sünonüüm: teave).

Info terviklus - tähendab andmete pärinemist autentsest allikast ning veendumust, et need pole hiljem muutunud ja/või neid pole hiljem volituseta muudetud.

Info konfidentsiaalsus - hõlmab salastatust, teabe kaitsmist ja/või privaatsust.

Infohaldus - info kogumine eri allikatest ja selle töötlemine, säilitamine ning kasutajatele jagamine eri kanalite kaudu. Oma põhiolemuselt on infohaldus protsess, mis hõlmab andmete ja info kogumist, kategoriseerimist, kaitsmist, säilitamist ja hilisemat levitamist. Infohalduse peamine eesmärk on tagada, et õige teave oleks õigetele inimestele õigel ajal kättesaadav. Lisaks võimaldab hästi korraldatud infohaldus organisatsiooni info efektiivset kasutamist ja aitab kaasa protsessides kiiremale infotötlusele ja juhtimisotsuste tegemisele ning teadmuse juhtimisele organisatsioonis. Infohalduse puhul kasutatakse ka mõistet teabehaldus, RTK-s ja käesolevas korras kasutame mõistet infohaldus.

Infosüsteem - tehnoloogiline lahendus RTK põhitegevuse käigus tekkiva info/andmete kogumiseks, säilitamiseks, töötlemiseks, jaotamiseks ja/või kasutamiseks.

Infotehnoloogiline keskkond (edaspidi keskkond)- on tehnoloogiline lahendus RTK tugitegevuse käigus tekkiva info/andmete kogumiseks, säilitamiseks, töötlemiseks, jaotamiseks ja/või kasutamiseks.

Isikuandmed - mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta sõltumata andmete vormist ja sisust.

Isikuandmete töötlemine - iga isikuandmetega tehtav toiming, sealhulgas isikuandmete vaatamine, kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, riskasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest.

Juurdepääsupiirang - õigusaktist tulenev alus teabele piiratud juurdepääsu kehtestamiseks.

Käideldavus - info omadus olla õigeaegselt kättesaadav ja kasutuskõlblik.

Liigitusskeem - infohalduse alusdokument asutuse tegevuse käigus tekkiva info elukäigu planeerimiseks ja juhtimiseks.

Tõendusväärus - omadus tõendada fakte või tegevuste toimumist.

Tõendusväärusega info - info, mis on kirjeldatud liigitusskeemis, omab säilitustähtaega ja omanikku.

1.4 Vastutusvaldkonnad

Info omanik - töötaja või osakond, kes vastutab info kvaliteedi, aja- ja asjakohasuse eest, määratleb, millised andmed on olulised ja vajalikud ning milline on nende tähtsus ja prioriteet, vastutab selle eest, et andmed oleksid kättesaadavad ainult nendele isikutele või osakondadele,

kellel on selleks vajalikud õigused. Töötaja vahetumisel saab uueks info omanikuks töö üle võtnud töötaja või muu isik, kes töötaja vahetumisel info omanikuks määratakse. Edaspidi on info omanikud leitavad liigitusskeemist¹.

Osakonna infohalduse kontaktisik – osakonna juhataja või tema poolt määratud töötaja või töötajad, kelle ülesandeks on käesolevas korras kirjeldatud põhimõtete rakendatavuse tagamine oma üksuses ja kes on peamiseks koostööpartneriks arendusosakonnale.

Infosüsteemi peakasutaja - vastutab infosüsteemis oleva info struktureerimise, infosüsteemi kasutamise, õiguste haldamise ja sisu ajakohastamise ning õigsuse eest, analüüsib arendusvajadusi, on kontaktiks IT partneritele, koolitab ja juhendab kasutajaid. Info peakasutajate ja kasutajate kohta on leitav [Protsesside käsiraamatust](#).

Arendusosakond (kvaliteedijuht) - vastutab RTK infohalduse põhimõtete kujundamise ja korralduse eest.

2. Infohalduse üldised põhimõtted

Infohalduse puhul tuleb järgida järgmisi peamisi põhimõtteid²:

- õige info, õigel ajal, õiges kohas, õigel kujul;
- infot sisestatakse ainult üks kord ja infot ei dubleerita mitmesse asukohta;
- teada on info tekkekoht, säilituskoht, omanik, lõpptarbija, formaat ning säilitamise/arhiveerimise põhimõtted ning kui tegemist on tõendusväärtusega infoga, siis need kajastuvad RTK liigitusskeemis;
- kõik osapooled on kaasatud ning informeeritud;
- kõigil vajalikel osapooltel on juurdepääs asja- ja ajakohasele infole;
- tööprotsessist on ülevaade ning probleemidega tegeletakse ennetavalt;
- info on ajakohane ning õigeaegne;
- asutuse tegevuse tõendamiseks oluline info (tõendusväärtuslik) dokumenteeritakse;
- järgitakse [infoturbealaseid kokkuleppeid](#) ning isikuandmete kaitse ja töötlemise põhimõtteid.

Info leitavuse ja käideldavuse eelduseks on info struktureerimine, mis hõlmab endas õige asukoha/hoiukoha valikut (kasutatavad infosüsteemid ning keskkonnad on kirjeldatud järgmises peatükis), korrektset failide nimetamist, omaniku ning säilitustähtaja määramist.

Tõendusväärtusega info organiseerimist puudutavad detailid lepatakse kokku liigitusskeemis. Sealsed säilitustähtajad lähtuvad õigusaktidest või organisatsioonisisestest kokkulepetest, milline info on organisatsiooni tegevuse järjepidevuse seisukohalt oluline.

¹ Liigitusskeem kajastab ka teavet, mis asuvad muudes infosüsteemides/hoiukohtades (teabeväärtusega teave). Tulevikus hakkab sisaldama ka hoiukohti, kus on töömaterjalid jm (nt MS SharePoint jm)

² Info jagamise põhimõtted väljapoole RTK-d on toodud Kommunikatsiooni korraldamise põhimõtetes (K28) ja meediasuhtlus kommunikatsioonistrateegias.

3. Kasutatavad infosüsteemid ja keskkonnad

3.1 Kasutatavate infosüsteemide ja keskkondade jagunemine

Kasutatavad infosüsteemid ja keskkonnad jagunevad:

- põhitegevuse infosüsteemid
 - RTK hallatavad ja arendatavad infosüsteemid
 - RTK välised infosüsteemid
- põhitegevust toetavad keskkonnad
 - keskkonnad info ja andmete loomiseks ja hoiustamiseks
 - suhtlus- ja meeskonnatöö keskkonnad

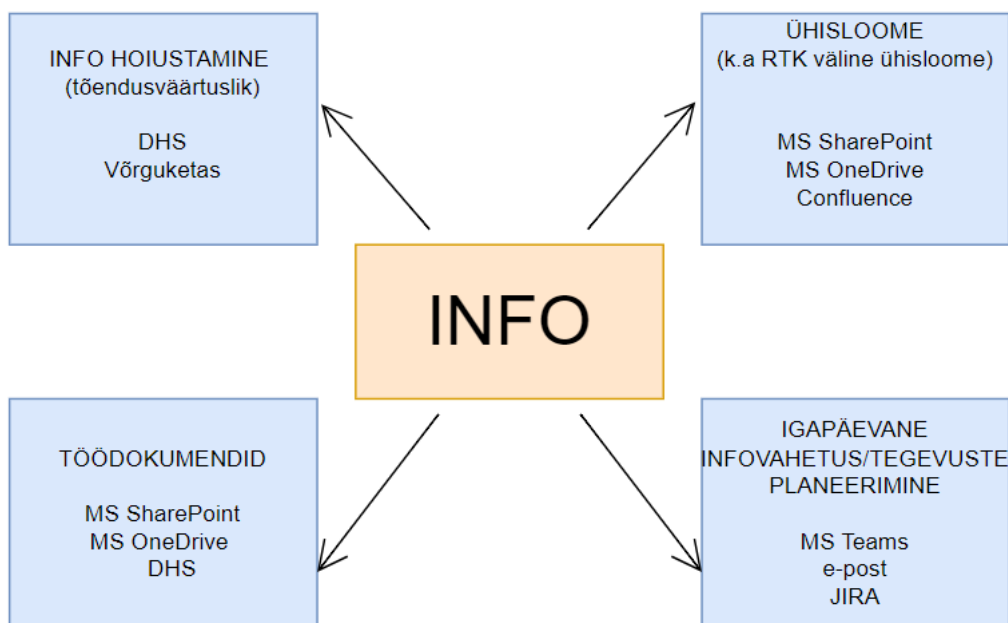
Põhitegevuse infosüsteemides toimub teenuse pakkumine ja teenusega seotud andmete haldamine. Põhiteenuse infosüsteemid on infosüsteemid, mida RTK ise haldab ja arendab (nt SAP, RTIP, SFOS). Lisaks kasutab RTK väliseid infosüsteeme, mis on nt Rahandusministeeriumi hallatavad (REIS, KAIS), Registrate- ja Infosüsteemide Keskuse hallatavad (dokumendihaldussüsteem Delta), jne.

Toetavad keskkonnad info ja andmete loomiseks ja hoiustamiseks – põhitegevuse infosüsteemidest välja jääva info loomine, koosloome, tegevuste ja projektide juhtimine. Seal asuvad ka olulised teadmusjuhtimise tööriistad nt elektrooniline protsesside käsiraamat ja siseveeb, mis asuvad Confluence's ja tööde juhtimise ning pöördumiste lahendamise tööriistad Jira-s ja OTRS-is, mis võimaldavad täpselt jälgida tegevuste seisu. Samuti mitmed meeskonnatöö ja koosloome tööriistad nagu nt Miro keskkond. Info ja andmete hoiustamiseks on kasutusel pilveteenused ja võrgukettad.

Suhtlus- ja meeskonnatöö keskkonnad on mõeldud kiireks, igapäevaseks infovahetuseks, aga ka info jagamiseks nt majakoosolekutel ja veebipõhistel koolitustel. Ametlikumad ja tõisemad vestlused peetakse üldjuhul MS Teams's või fikseeritakse e-kirja teel. Siia kuuluvad ka sotsiaalmeediakanalid, mille kaudu ollakse nähtav ka väljapoole.

RTK-s (2024 I poolasta seisuga) kasutatavad infosüsteemid ja keskkonnad ning nende kasutamise eesmärgid on kirjeldatud käesoleva korra [lisas](#).

Joonis 1. Hetkel eelistatud toetavad keskkonnad



3.2 Uue infosüsteemi/keskkonna kasutusele võtmise kriteeriumid

Uue infosüsteemi/keskkonna kasutusele võtmisel tuleb hinnata infosüsteemi/keskkonna poolt loodavat väärtust:

- milliseid protsesse uus infosüsteem/keskkond muudab lihtsamaks;
- kui kasutusel on sarnaste võimalustega süsteem, siis millised on ühe või teise infosüsteemi/keskkonna eelised;
- millised on mahud (kes kui palju kasutab, kui tihti) ja millised on kulud;
- kas kasutusele võetav infosüsteem/keskkond toetab ainult ühe kitsa lõigu vajadusi või on kasu laiem ja organisatsioonile tervikuna kasulik;
- milliseid teadmisi vajab uue infosüsteemi/keskkonna kasutamine, kes saab nende osas tuge pakkuda;
- kas mõnest varasemast kasutusel olnud süsteemist on võimalik loobuda ja kuidas toimub sellisel juhul info ülekandmine ühest süsteemist teise.

Uue infosüsteemi/keskkonna kasutusele võtmine tuleb kooskõlastada teenuse eest vastutava juhiga, kvaliteedijuhiga ning kulujuhiga.

Infosüsteemide/keskkondade kasutamist reguleerib [Infosüsteemide kasutamise kord \(K8\)](#).

4. Õiguste haldus

Tõhus infohalduse protsess ei hõlma ainult andmete kogumist ja kategoriseerimist, vaid ka tagamist, et õiged inimesed pääsevad sellele teabele õigel ajal juurde.

Õiguste haldamise süsteem tuleb hoida võimalikult lihtsana. Tuleb selgelt määratleda, millistes infosüsteemides/keskkondades on töötajatel baasõigused ja milliste infosüsteemide/keskkondade või kaustade puhul on vajalikud rollipõhised õigused või eriõigused.

RTK uuele töötajale tellitakse õigused töökoha tellimise ankeedi kaudu, lähtuvalt rollist rakenduvad talle ametikohale vajalikud õigused vajalikes infosüsteemides/keskkondades. Õiguseid tellib töötaja vahetu juht. Õiguste tellimine uuele töötajale on kirjeldatud personali värbamise ja töö- ning teenistussuhete haldamise korras (K11).

Töölt lahkumisel on töötaja kohustatud teavitama oma juhti kõikidest (välistest) infosüsteemidest/keskkondadest, millele juurdepääs on talle antud tööst tulenevalt ning juht vastutab juurdepääsude sulgemise eest. Välisteks infosüsteemideks/keskkondadeks on kõik need, mis ei ole loetletud tabelis 1 põhisinfosüsteemide all ja/või mille kasutusõigus ei sulgu automaatselt koos töötaja RTK konto sulgemisega (nt e-riigikassa, EMTA).

Õigused jaotuvad:

- baasõigused - õiguste ja ligipääsude kogum, mis omistatakse igale töötajale tema tööle tulekul;
- rollipõhised õigused, kui roll on sisustatud ja kirjeldatud;
- eriõigused (mis ei kuulu rollidesse), kui juht need tellib.

Kasutajale omistatakse baas-, rollipõhiseid ja/või eriõiguseid tähtajaliselt või tähtajatult.

Kui infosüsteemi kasutajal tekib põhjendatud vajadus juurdepääsuks infole, millele tal juurdepääs puudub, tuleb pöörduda infosüsteemi eest vastutava teenistuja/peakasutaja/kasutajatoe poole juurdepääsuõiguse saamiseks.

Õiguseid RTK põhiinfosüsteemidele (SAP, RHR, SFOS) antakse põhimäärustes (vt p 1.2) toodud alustel.

Kasutajaõiguste andmine, kehtetuks tunnistamine ja korrastamine on reguleeritud [Infosüsteemide kasutamise töökorras \(K8\)](#).

5. Failide loomine ja jagamine

5.1 Failinimede loomine

Põhimõtted failinimede loomisele on soovituslikud tuginedes rahvusarhiivi nõuetele.

Järjepideva ja kindla failinime formaadi kasutamine aitab tagada failide leidmist, avamist ning säilitamist nii kaua, kui vaja. Informatiivne failinimi võimaldab faili hiljem hõlpsamini üles leida.

Failid tuleb pealkirjastada selliselt, et on aru saada, millise infoga, mis ajast ja kelle poolt koostatud infoga on tegemist.

Failinime koostamise põhimõtted on järgmised:

- failinimes ja laiendis on soovitav kasutada ainult väiketähti
- failinime pikkus (laiendita) ei tohiks ületada 30 tähemärki
- kasutada ei tohiks järgmisi tähemärke: \ / : * ? “ < > | [] & \$,

- vältida tühikute kasutamist. Tühiku asendajana kasutada tähemärkide eraldamiseks alakriipsu () või sidekriipsu (-) ning sõnade eristamiseks või rõhutamiseks kasutada vajadusel suurtähti
- kuupäeva kirjeldamisel failinimes tuleks kasutada formaati „AAAANKPP“

Näide: 2024_02_20_kaaskiri_1

5.2 Failide jagamine

Kui faili loomisesse ja ülevaatamisse on kaasatud mitmed inimesed, siis valitakse asjakohane koosloome keskkond (hetkel Confluence, MS OneDrive, MS SharePoint), et vältida erinevate versioonide tekkimist ja kuhjumist.

Faile säilitatakse ainult ühes asukohas järgides põhimõtet üks info ühes asukohas, st faile ei dubleerita. Kui faili on võimalik luua dokumendihaldussüsteemis, siis eelistatakse dokumendi koostamist otse süsteemis kasutades dokumendihaldussüsteemis pakutavaid malle.

Välditakse e-kirja kaudu mahukate failide vahetamist. Eelistatakse jagada meili kaudu eelkõige infot faili algsele asukohale nt lingina mitte saates faili ennast.

Dokumendid, mis on koostamise varajases staadiumis, võivad paikneda kasutaja personaalses (võrgu)keskkonnas. Küll aga tuleb dokument paigutada koosloome keskkonda kohe, kui tekib vajadus selle jagamiseks või ühistööks, ka siis, kui tegemist on veel mustandversiooniga. Sellega tagatakse, et dokumendist on ainult üks ja tõene versioon.

6. Infohalduse optimaalne korraldus

Digiprügi vältimiseks tuleb infot korrastada:

- info korrastamine töötajate poolt on pidev tegevus (nt kui materjali enam ei vajata, siis kustutatakse see kohe);
- info hoidmise infosüsteemid/keskkonnad vaadatakse keskselt (arendusosakonna ja osakonna infohalduse kontaktisiku/-isikute eestvedamisel) üle vähemalt 1 kord aastas vahemikus juuni-august, selle käigus kustutatakse mittevajalik või aegunud info (kaustad, failid jms);
- infosüsteemide korrastamise eest vastutavad infosüsteemide ja info omanikud;
- fotode ja videote säilitamise põhimõtted on väljatöötamisel.

Digiprügi mõju on lai ja ulatub üle erinevate valdkondade, mõjutades muuhulgas failide turvalisuse, ressursside vajaduse ning seadmete efektiivsusega seotud aspekte:

- digiprügi tekitab ohtu failide turvalisusele. Suure hulga vanade ja kasutamata failide säilitamine võib tekitada turvariske, kuna neid faile ei pruugi olla piisavalt kaitstud või neis võib peituda pahavara. Turvalisuse tagamine muutub keerulisemaks, kui infot on raske leida ja hallata suure digiprügi hulga tõttu;
- digiprügi suurendab lisaressursi vajadust, näiteks tingides vajaduse osta juurde lisaruumi failide säilitamiseks. Mida rohkem digiprügi koguneb, seda rohkem vajab organisatsioon

või üksikisik lisaruumi tarbetute failide säilitamiseks, mis omakorda toob kaasa suuremad kulud ning negatiivsed mõjud keskkonnale;

- digiprügi aeglustab seadmete tööd ja pikendab seeläbi aega, mis kulub vajaliku teabe leidmisele - suur kasutute failide või rakenduste hulk vähendab seadme jõudlust, mis omakorda pärsib tööviljakust ja tõhusust. Kasutute failide tõttu kulub rohkem aega vajaliku teabe leidmiseks, kuna see on peidus vanade ja ebaoluliste failide vahel