

Konfidentsiaalse teabe töötlemise reeglid

1. Töökorraldus

1.1. Töökorralduse üldnõuded

- 1.1.1. Teabe saaja on kohustatud jooksvalt läbi kogu tööprotsessi pidama arvestust isikutest, kellel on teabe saaja poolt juurdepääs projektiga seotud juurdepääsupiiranguga ehk „asutusesiseseks kasutamiseks“ (edaspidi AK) kaetud materjalidele ning RKIK nõudmisel esitama selle koondinfo (sh alltöövõtjad).
- 1.1.2. Teabe saaja sisemine tööprotsess ja kasutatavad arvutisüsteemid peavad välistama punktis 1.1.1 nimetatud isikute hulka mittekuuluvate isikute juurdepääsu piiratud infole (sh AK-märkega dokumendid, RKIK projekteerimisjuhised, protokollid jms).

1.2. Juurdepääsupiiranguga (AK) projektide edastamine:

- 1.2.1. Kõik juurdepääsupiiranguga (AK) projekti osad tuleb enne e-kirjalist edastamist krüpteerida DigiDoc3 krüpto programmiga. Teabe saajal, kes ei asu Eesti Vabariigis ja kellel ei ole DigiDoc3 süsteemi kasutamise võimekust, on lubatud juurdepääsupiiranguga (AK) projekti osasid e-kirjaliselt kirja teel edastada, kasutades 7-Zip rakendust, mille kasutamisel peab kaitsema 7-Zip rakenduse konteineris asuvaid dokumente parooliga. Parool ja 7-zip rakenduse konteiner ei tohi sisalduda ühes ja samas e-kirjas.
- 1.2.2. Kõik juurdepääsupiiranguga (AK) projekti osad tuleb andmekandjatele (CD, DVD, mälupulk või muu) salvestades krüpteerida DigiDoc3 krüpto programmiga, kui RKIK-ga ei lepita kokku teisiti. Teabe saajal, kes ei asu Eesti Vabariigis ja kellel ei ole DigiDoc3 süsteemi kasutamise võimekust, on lubatud juurdepääsupiiranguga (AK) projekti osasid andmekandjatele (CD, DVD, mälupulk või muu) salvestada, kasutades 7-Zip rakendust, mille kasutamisel peab kaitsema 7-Zip rakenduse konteineris asuvaid dokumente parooliga. Parool ja 7-zip rakenduse konteiner ei tohi sisalduda ühel ja samal andmekandjal.
- 1.2.3. Juurdepääsupiiranguga (AK) projekti osasid saab edastada RKIK projektipanga tarkvara vahendusel (KAEVIK, KRA Pilv). RKIK väljastab paroolid projektipanga kasutamiseks.
- 1.2.4. Juurdepääsupiiranguga (AK) materjale ei tohi kopeerida Teabe saaja kontrolli alt väljas olevatesse serveritesse (nt Google Drive, DropBox, OneCloud jms). Teabe saajal tuleb täpsustada RKIK-ga projekteerimise või ehitamise alustamisel, kuidas on teabe saajal lubatud juurdepääsupiiranguga materjale käidelda.

1.3. Projektijuhtimine

- 1.3.1. Projekti osadele, mis on juurdepääsupiiranguga (AK) vastavalt avaliku teabe seadusele, tuleb kanda vastav märge.
- 1.3.2. Juurdepääsupiiranguga (AK) projektdokumentatsioon esitatakse Tarbijakaitse ja Tehnilise Järelevalve Ametile (TTJA) ja selle poolt määratud asutustele digitaalsel kujul elektroonilisel andmekandjal (CD, DVD, mälupulk) ja krüpteerida vastavalt punktile 1.2. Vajadusel koostada kooskõlastuste jaoks lisajoonised, mis tuleb märgistada vastavalt punktile 1.3.1. ja esitada vastavalt käesolevas punktis sätestatule.

2. Nõuded konfidentsiaalse teabe töötlemiseks

2.1. Nõuded serverile ja projektipangale (edaspidi ka süsteem)

Serveri / projektipanga kasutamisel AK märkega materjalide töötlemiseks (sh hoidmiseks, edastamiseks, vaatamiseks jms) peab server / projektipank vastama alljärgnevatele nõuetele:

- 2.1.1. Eesti Vabariigis asuva Teabe saaja süsteem peab geograafiliselt asuma Eestis. Teabe saaja, kes ei asu Eesti Vabariigis, süsteem peab asuma teabe saaja perimeetri sees (*on-premise*) või peab olema tagatud dokumentide kaitse serveri teenusepakkuja, kelle teenust teabe saaja kasutab, ligipääsu eest;
- 2.1.2. Juurdepääs süsteemile on piiratud IP aadresside abil;
- 2.1.3. Juurdepääs süsteemile peab olema kaitstud isikustatud kasutajakontode abil;
- 2.1.4. Teabe saaja peab oma süsteemi seadistama nii, et kasutajatel oleks kohustus kasutada turvalist parooli (10+ märki, suured ja väikesed tähed, numbrid, erisümbolid);
- 2.1.5. Teabe saaja peab oma süsteemi seadistama nii, et ühendus klientidega (sh RKIK) toimuks üle krüpteeritud kanalite (https, sftp);
- 2.1.6. Süsteemi laetud AK märkega materjalidele tohib olla ligipääs vaid antud projektiga seotud inimestel;
- 2.1.7. Teabe saaja peab omama pidevat ülevaadet, kellel on juurdepääs AK märkega materjalidele;
- 2.1.8. Teabe saaja peab pidama logiandmeid kõikidest failidele ligipääsudest (õnnestunud ja ebaõnnestunud) ja edastama neid RKIK-le vastavalt RKIK poolt esitatud nõudmisele;
- 2.1.9. Punktides 2.1.1. – 2.1.4. esitatud nõuete täitmise kontrollimiseks võimaldab teabe saaja RKIK ekspertidel serverisüsteemi auditeerida enne selle kasutuselevõttu;
- 2.1.10. Projektipanga (serveri) kasutamise luba fikseeritakse protokolliliselt projekteerimiskoosolekul. Enne RKIK-lt loa saamist ei või projektipanka kasutada AK materjalide töötlemiseks.

2.2. Projekteerimiskeskond peab vastama vähemalt alljärgnevatele tingimustele:

- 2.2.1. Projekteerimiskeskond peab olema teabe saaja poolt hallatavas ja kontrollitavas keskkonnas Eesti Vabariigi territooriumil;
- 2.2.2. Projekteerimiskeskonna kasutajatel peavad olema personaliseeritud kasutajakontod, millest on tuvastatav reaalne kasutaja;
- 2.2.3. Parooli pikkus peab vastama punktis 2.1.4. sätestatud tingimustele;
- 2.2.4. Parooli kehtivus peab olema minimaalselt 1 ja maksimaalselt 90 kalendripäeva;
- 2.2.5. Viimati kasutatud viit (5) parooli ei tohi saada uuesti kasutada;
- 2.2.6. Projekteerimiskeskond peab võimaldama piirata (autoriseerida) ligipääsu erinevatele projekti osadele vastavalt teadmismajadusele;
- 2.2.7. Teabe saaja peab pidama nimekirja projekti osistele ligipääsu omavate isikute osas;
- 2.2.8. Projekteerimiskeskond peab arvestama, et töödeldavad materjalid on vähemalt tasemel ASUTUSESISEKS KASUTAMISEKS vastavalt avaliku teabe seadusele, kui materjalid on vastavalt märgistatud.