Kontakt	Publitseerimine
Hannes Laaser	Avalik
Kinnitamise kuupäev	**Kinnitanud**
11.06.2018	Ave-Liis Saluveer
Dokumendi number	**Versiooni number**
T4511-16	6.0

TELIA TURVADIREKTIIVID

1. Kirjeldus

Käesolevas dokumendis (edaspidi **Turvadirektiivid**) kirjeldatakse Tarnijatele (nagu defineeritud allpool) ja Ostja teistele äripartneritele kohaldatavaid turvanõudeid. Konkreetsetel juhtudel võidakse kohaldada täiendavaid turvanõudeid, kui pooled lepivad selles kokku.

2. Mõisted

1. **Leping** on Telia (või Telia Company kontserni muu tuvastatud äripartner) ja Tarnija vaheline leping, millele kohalduvad vastava lepingu osaks olevad Turvadirektiivid.
2. **Ostja** on Telia Eesti AS või Telia Company AB või asjaomane Telia Company kontserni kuuluv ettevõte.
3. **Ostja andmed** on andmed või muu info, mille Ostja või Ostja nimel tegutsev isik teeb Tarnijale kättesaadavaks, sealhulgas Isikuandmed, ning Tarnija poolt nende andmete töötlemise tulemus.
4. **Infotöötlusvahendid** on infotöötlussüsteem, -teenused või -taristu või füüsilised asukohad, kus need asuvad.
5. **Logimine** on info või sündmuste üksikasjade registreerimine organiseeritud registreerimissüsteemi, tavaliselt järjestatuna info või sündmuste toimumise järjekorras.
6. **Isikuandmed** on kõik andmed füüsilise isiku tuvastamiseks, arvestades kohaldatavaid andmekaitse õigusakte, sealhulgas järgmisi: ELi andmekaitse direktiiv (Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta), eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv (Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris) ja isikuandmete kaitse üldmäärus (Euroopa Parlamendi ja nõukogu määrus 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) ja nende muudatused, asendused või uuendused (edaspidi koos: „ELi õigusaktid“), kõik täitmiseks kohustuslikud riigisisesed seadused, millega rakendatakse ELi õigusakte, ja muud täitmiseks kohustuslikud andmekaitse või andmete turbe direktiivid, seadused, määrused ja otsused, mis on vastaval ajal kehtivad. Tuvastatav füüsiline isik on isik, keda on võimalik otseselt või kaudselt tuvastada mõne tunnuse alusel, milleks võib olla näiteks nimi, aadress, sotsiaalkindlustuse number, abonendi number, IP-aadress, asukohaandmed, online-tunnus, liiklusandmed või sõnumi sisu, või ühe või mitme teguri alusel, mis on seotud vastava füüsilise isiku füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse identiteediga.
7. **Teenused** on Tarnija või Tarnija nimel tegutseva isiku poolt Ostjale osutatavad teenused, mis on täpsemalt määratletud poolte vahelises lepingus.
8. **Tarnija** viitab teisele poolele, kes tarnib Ostjale mis tahes kaupa või teenust, ja keda nimetatakse vastavas Lepingus tarnijaks, müüjaks, partneriks või muu sarnase nimega.
9. **Tarnija personal** on Tarnija heaks töötavad isikud, näiteks töötajad, nõustajad, töövõtjad ja alltöövõtjad.
10. **Turvameede** on tehniline turvameede, organisatsiooniline struktuur või protsess, mis aitab hoida IT-süsteemide turvakvaliteediga seotud omadusi.
11. **Turvaintsident** on soovimatud või ootamatud turvasündmused üksikult või sarjana, millel on oluline tõenäosus seada ohtu äritegevust ja ohustada turvalisust.
12. **Tundlikud tooted** ja **Tundlikud teenused** on tooted või Teenused, mille Ostja on määratlenud tundlikuna. Tundlikud tooted või Tundlikud teenused dokumenteeritakse selgelt vastavalt Lepingus sätestatule.
13. **Pseudonüümimine** on isikuandmete töötlemine selliselt, et isikuandmeid ei saa enam omistada konkreetsele andmesubjektile lisateavet kasutamata. Seda eeldusel, et vastavat lisateavet

hoitakse eraldi ning sellele rakendatakse tehnilisi ja organisatoorseid meetmeid tagamaks, et isikuandmeid ei omistata tuvastatud või tuvastatavale füüsilisele isikule.

3. Rakendusala

Turvadirektiive kohaldatakse, kui:

1. Tarnija töötleb Ostja andmeid;
2. Tarnija siseneb Ostja valdustesse;
3. Tarnija siseneb Ostja võrku või IT-süsteemidesse, sealhulgas läbi kaugjuurdepääsu;
4. Tarnija kasutab Ostja infotöötlusseadmeid;
5. Ostja peab Tarnijat Tundlike toodete ja/või Tundlike teenuste pakkujaks ning on Tarnija vastavas Lepingus selliselt määratlenud.

4. Tarnija üldine vastutus

1. Tarnija vastutab täielikult selle eest, et Tarnija personal järgib Turvadirektiive.
2. Tarnija rakendab Turvadirektiivide järgimise tagamiseks nõutavad meetmed enne Ostja jaoks mis tahes ülesande täitmisega alustamist.
3. Tarnija teavitab Ostjat viimasae nõudmisel sellest, kuidas Tarnija Turvadirektiive järgimise tagab ja milliseid meetmeid on Tarnija võtnud kasutusele Turvadirektiivide täitmiseks.
4. Tarnija teatab ostjale aadressil cert@telia.ee mis tahes Turvaintsidendist (sealhulgas Isikuandmete töötlemisega seotud intsidentidest) võimalikult kiiresti, kuid hiljemalt 24 tunni jooksul Turvaintsidendi tuvastamisest. Vt intsidentide halduse kohta allpool.
5. Tarnija tagab, et Ostja andmete töötlemine toimub kooskõlas Turvadirektiividega.
6. Tarnija tagastab või hävitab (vastavalt Ostja otsusele) Ostja andmed ja nende koopiad. Tarnija kinnitab Lepingu lõpetamisel või Ostja taotlusel Ostjale kirjalikult, et Tarnija on selle nõude täitnud.
7. Tarnija ei võimalda ühelegi isikule Lepingut rikkudes juurdepääsu (see võib puudutada ka uut, laiendatud, uuendatud, pikendatud või muul viisil muudetud reaalajalist juurdepääsu üle võrgu) Ostja andmetele ilma Ostja eelneva kirjaliku heakskiiduta.

5. Turvanõuded

5.1. Riskide juhtimine

5.1.1. Turvariskide juhtimine

1. Tarnija tuvastab ja hindab konfidentsiaalsuse, tervikluse ja käideldavusega seotud turvariske ning rakendab vastava hindamise alusel asjakohaseid tehnilisi ja organisatoorseid meetmeid tagamaks riskile vastava turvataseme.
2. Tarnijal on dokumenteeritud protsessid ja praktikad oma tegevuses esinevate riskidega tegelemiseks.
3. Tarnija hindab perioodiliselt infosüsteemide ning info töötlemise, talletamise ja edastamisega seotud riske.

5.1.2. Isikuandmetega seotud turvariskide juhtimine

1. Tarnija tuvastab ja hindab konfidentsiaalsuse, tervikluse ja käideldavusega seotud turvariske ning rakendab vastava hindamise alusel asjakohaseid tehnilisi ja organisatoorseid meetmeid, et tagada turvatase, mis on vastav konkreetsete Isikuandmete liikidest ja Tarnijapoolse töötlemise eesmärkidest tulenevatele riskidele, hõlmades, kui asjakohane, muu hulgas järgmist:
   a) Isikuandmete pseudonüümimine ja krüpteerimine;
   b) võime tagada kestvalt andmete töötlemise süsteemide ja teenuste konfidentsiaalsus, terviklus, käideldavus ja vastupanuvõime;
   c) võime taastada õigeaegselt Ostja andmete käideldavus ja neile juurdepääs füüsilise või tehnilise intsidendi korral;
   d) protsess tehniliste ja organisatoorsete meetmete tõhususe regulaarseks testimiseks ja hindamiseks, et tagada töötlemise turvalisust.

2. Tarnijal on dokumenteeritud protsessid ja praktikad riskide haldamiseks Ostja nimel Isikuandmete töötlemisel.
3. Tarnija hindab perioodiliselt infosüsteemidega ning Isikuandmete töötlemise, talletamise ja edastamisega seotud riske.

5.2. Infoturbepoliitikad

1. Tarnijal on määratletud ja dokumenteeritud infoturbe juhtimissüsteem (*information security management system*, ISMS), sealhulgas kehtestatud infoturbepoliitika ja protseduurid, mille peab kinnitama Tarnija juhtkond. Need avaldatakse Tarnija organisatsioonis ja nendest teavitatakse vastavat Tarnija personali.
2. Tarnija vaatab perioodiliselt üle Tarnija turvapoliitikad ja -protseduurid ning ajakohastab neid vajadusel, tagamaks nende vastavus Turvadirektiividega.

5.3. Infoturbe korraldamine

1. Tarnijal on oma organisatsioonis määratletud ja dokumenteeritud turvarollid ja -vastutused.
2. Tarnija nimetab vähemalt ühe isiku, kellel on asjakohane turbepädevus ja kes kannab üldist vastutust Turvadirektiividest tulenevate turvameetmete rakendamise eest ning kes on Ostja turbepersonalile kontaktisikuks.

5.4. Personaliga seotud turve

1. Tarnija tagab, et Tarnija personal käitleb infot vastavalt Lepingus sätestatud konfidentsiaalsuse tasemele.
2. Tarnija tagab, et asjaomane Tarnija personal on teadlik Lepinguga seotud info, vahendite ja süsteemide heakskiidetud kasutusnõuetest (sealhulgas kasutuspiirangutest vastavalt olukorrale). Ostjal on õigus nõuda igalt Tarnija personali liikmelt allkirjastatud kinnitust selle kohta, et ta on Turvadirektiividest ning info, süsteemide ja vahendite heakskiidetud kasutusest aru saanud ning järgib neid.
3. Tarnija tagab, et Lepingu alusel ülesandeid täitev Tarnija personal on usaldusväärne, vastab kehtestatud turvakriteeriumitele ning on läbinud asjakohase kontrolli ja taustauuringu ning on ülesande täitmise kestel allutatud jätkuvalt nimetatud kohustusele.
4. Tarnija ei kaasa ilma Ostjat eelnevalt teavitamata ja Ostja kirjaliku nõusolekuta Ostjalt saadud ülesande täitmisse Tarnija personali, (i) kellel on huvide konflikt seoses Ostja või vastava ülesandega või (ii) kellele on mõistetud vanglakaristus kuriteo eest kolme (3) aasta jooksul enne ülesande täitmisse kaasamist, i) kui vastav Tarnija personal töötleb mis tahes viisil Ostja klientide või töötajate või Ostja klientide töötajatega seotud Isikuandmeid või ii) kui Tarnija personal abistab ülesannetes, mille Ostja on liigitanud tundlikuks. Ostja annab infot selle kohta, millised ülesanded on liigitatud tundlikuks, Lepingu sõlmimise ajal või vähemalt kaks nädalat enne tarnija personali tööle rakendamist või ülesande algust.
5. Tarnija tagab, et turbeteemade eest vastutav Tarnija personal on piisavalt koolitatud turvalisusega seotud ülesannete täitmiseks.
6. Tarnija tagab või pakub vastavale Tarnija personalile perioodilist turvateadlikkuse koolitust. Vastav tarnija koolitus sisaldab muu hulgas järgmist:
   a) kuidas tegeleda kliendi info turvalisuse tagamisega (st teabe konfidentsiaalsuse, tervikluse ja käideldavuse kaitsmine);
   b) miks on klientide info ja süsteemide kaitsmiseks vaja infoturvet;
   c) turvaohtude tavaliigid (nt nimevargus, kahjurvara, häkkimine, infoleke ja organisatsioonisisene oht);
   d) infoturbepoliitikate järgimise ja seotud standardite/protseduuride rakendamise tähtsus;
   e) isiklik vastutus infoturbe eest (nt kliendi privaatsusega seotud info kaitsmine ning tuvastatud ja võimalikest Turvaintsidentidest teatamine).

5.5. Varahaldus

1. Tarnijal on sätestatud ja dokumenteeritud varahaldussüsteem ning ta peab ajakohastatud registreid kõigi asjakohaste varade ja nende omanike kohta. Infovarade hulka kuuluvad muu hulgas järgmised: IT-süsteemid, tundlikku infot sisaldavad varu- ja/või kaasaskantavaid infokandjad, pääsuõigused, tarkvara ja konfiguratsioon.
2. Tarnija märgistab, käsitleb ja kaitseb infot vastavalt eelnevalt määratletud info turvaliigituse süsteemile kooskõlas kehtivate turvastandarditega (sealhulgas kaasaskantavatele infokandjatele salvestamine, eemaldamine ja füüsiline ülekandmine).
3. Tarnija rakendab meetmed tagamaks, et edastatavad, talletatavad või muul viisil töödeldavad Ostja andmed oleks kaitstud juhusliku, volitamata või ebaseadusliku kaotsimineku, hävimise, muutmise või kahjustumise eest.
4. Tarnija peab ajakohastatud nimekirja töödeldavatest Ostja andmetest. Nimekiri sisaldab järgmist:
   a) töödeldavad andmed;
   b) andmete säilitamise üksikasjad, nt vara nimi, asukoht jne.

5.6. Juurdepääsu kontroll

1. Tarnija on sätestanud ja dokumenteerinud juurdepääsu kontrolli poliitika juurdepääsuks vahenditele, asukohtadele, võrgule, süsteemile, rakendustele ja infole/andmetele (sealhulgas füüsilise, loogilise ja kaugjuurdepääsu nõuded), kasutajale juurdepääsu ja kasutussõiguste andmise protsessi, protseduurid juurdepääsuõiguste tühistamiseks ning Tarnija personali juurdepääsuõiguste lubatud kasutusviisid.
2. Tarnija on rakendanud formaalse ja dokumenteeritud kasutajate registreerimise ja deregistreerimise protsessi juurdepääsuõiguste andmiseks.
3. Tarnija annab kõik juurdepääsuõigused lähtudes põhjendatud vajaduse ja vähimate vajalike õiguste hulga põhimõttest.
4. Tarnija kasutab tugevat autentimist (multiautentimist) kaugjuurdepääsu kasutajate puhul ja kasutajate puhul, kes loovad ühenduse ebausaldusväärsest võrgust.
5. Tarnija tagab, et Tarnija personalil on isiklik ja ainulaadne tunnus (kasutajatunnus), ja kasutatakse asjakohast autentimismeetodit, mis kinnitab ja tagab kasutajate tuvastamise.

5.7. Krüptograafia

1. Tarnija tagab konfidentsiaalse ja salajase turvaliigitusega info (näiteks Isikuandmete) osas krüptograafia nõuetekohase ja tõhusa kasutuse vastavalt Ostja konfidentsiaalsuse turvaliigituse skeemile, nagu on allpool täpsemalt selgitatud.
2. Tarnija kaitseb krüptovõtmeid.

5.8. Füüsiline ja keskkonnaturve

1. Tarnija kaitseb infotöötlusvahendeid välis- ja keskkonnaohtude ja -riskide eest, sealhulgas voolu-/kaablirikete ja toetavate teenuste riketest põhjustatud muude katkestuste eest. See hõlmab füüsilist perimeetri ja juurdepääsu kaitsmist.
2. Tarnija kaitseb Ostja nimel saadud või saadetud kaupa varguse, manipuleerimise ja hävimise eest.

5.8.1. Lubamine Ostjale kuuluvatesse ja Ostja poolt renditud valdustesse

Tarnija lubamisel Ostja ruumidesse ja territooriumile (nt andmekeskuse hooned, kontorihooned, tehnilised asukohad) arvestatakse järgmist:

1. Tarnija järgib Lepingust tulenevate ülesannete täitmisel Ostja valdustes kehtivaid eeskirju (nt „piiratud alade“ eeskirjad).
2. Tarnija personal kannab Ostja valdustes töötamisel igal ajal nähtavalt tunnuskaarti või külastaja märki.
3. Pärast ülesande täitmise lõpetamist või kui Tarnija personal viiakse üle muudele ülesannetele, teatab Tarnija viivitamata Ostjale muudatusest ning tagastab võtmed, võtmekaardid, tunnistused, külastaja rinnamärgid ja sarnased esemed.

4. Võtmete või võtmekaartide eest annab Tarnija personal isiklikult allkirja ning neid käsitatakse vastavalt nende saamisel antud kirjalikele eeskirjadele.
5. Ostja võtme või võtmekaardi kaotusest teatatakse viivitamata Ostjale.
6. Loata pildistamine Ostja ruumides või territooriumil on keelatud.
7. Ostja kaupa ei tohi ilma loata Ostja valdustest välja viia.
8. Tarnija personal ei luba kõrvalistele isikutele juurdepääsu valdustele.

5.9. Tegevuse turve

1. Tarnija on kehtestanud muutuste juhtimise süsteemi muudatuste tegemiseks äriprotsessides, infotöötlusvahendites ja -süsteemides. Muutuste juhtimise süsteem hõlmab rakendamisele eelnevaid testimisi ja ülevaatamisi, nt protseduure pakiliste muudatustega tegelemiseks, taastamisprotseduure ebaõnnestunud muudatuste korral, logisid, kust on näha, mida on muudetud, millal ja kelle poolt.
2. Tarnija rakendab kahjurvara kaitset tagamaks, et Tarnija poolt Ostjale kauba või teenuste tarnimisel kasutatav tarkvara on kahjurvara eest kaitstud.
3. Tarnija teeb kriitilise tähtsusega infost varukoopiaid ja testib varukoopiaid tagamaks, et infot on võimalik vastavalt Ostjaga kokku lepitule taastada.
4. Tarnija logib ja jälgib tegevusi, nt töödeldavate andmete loomist, lugemist, kopeerimist, muutmist ja kustutamist, aga ka erandeid, rikkeid ja infoturbe sündmusi ning vaatab neid regulaarselt üle. Lisaks Tarnija kaitseb ja talletab (vähemalt 6 kuuks) logi infot ning esitab nõudmise korral jälgimisandmed Ostjale. Anomaaliatest /intsidentidest /sissemurdmisele viitavatest märkidest antakse aru vastavalt intsidentide juhtimise nõuetele 5.13.
5. Tarnija haldab kõigi asjakohaste tehnoloogiate, nt operatsioonisüsteemide, andmebaaside ja rakenduste turvanõrkusi proaktiivselt ja õigeaegselt.
6. Tarnija kehtestab kõigile asjakohastele tehnoloogiatele, nt operatsioonisüsteemidele, andmebaasidele ja rakendustele turbe etalonid (tugevdamine).
7. Tarnija tagab arenduse lahususe testimis- ja tootmiskeskkonnast.

5.10. Side turve

1. Tarnija rakendab infosüsteemide kaitsmiseks võrkude turvameetmed, nt teenusetasemed, tulemüüri ja lahususe.
2. Tarnija tagab, et konfidentsiaalse ja turvalise turvaliigitusega kõneside (vt täpsemalt allpool) on turvaline, mis tähendab seda, et krüpteerimata sidet ei tohi kasutada.

5.11. Süsteemi hankimine, arendamine ja hooldus (kui Tarnija pakub Ostjale tarkvara- või süsteemiarendust)

1. Tarnija rakendab tarkvara ja süsteemide arenduse elutsükli eeskirjad, sealhulgas muutmise ja ülevaatamise protseduurid.
2. Tarnija testib arenduse käigus kontrollitud keskkonnas turvafunktsioonistikku.

5.12. Tarnija suhe alltöövõtjatega

1. Tarnija kajastab käesolevate Turvadirektiivide sisu oma lepingutes alltöövõtjatega, kes täidavad Lepingu alusel antud ülesandeid.
2. Tarnija teostab regulaarselt alltöövõtja poolt Turvadirektiivide järgimise seiret, ülevaatamist ja auditit.
3. Tarnija esitab Ostja nõudmisel Ostjale tõenduse alltöövõtja poolt Turvadirektiivide järgimise kohta.

5.13. Turvaintsidentide haldus

1. Tarnija on kehtestanud protseduurid Turvaintsidentide halduseks.

2. Tarnija teatab Ostjale aadressil cert@telia.ee mistahes turvaintsidendist (sh Isikuandmete töötlemisega seotud intsidentidest) võimalikult kiiresti, kuid hiljemalt 24 tunni jooksul Turvaintsidendi tuvastamisest.
3. Turvalisusega seotud intsidentide kõiki teateid käsitletakse konfidentsiaalse teabena ja need krüpteeritakse, kasutades valdkonna standardiks olevaid krüpteerimise meetodeid, nt PGP.
4. Turvaintsidendi teade sisaldab vähemalt järgmist teavet:
   a) olenemata kohese teavitamise nõudest, koostab Tarnija Ostjale kirjaliku eelteate mis tahes turvaintsidendi kohta, mis võib potentsiaalselt mõjutada Ostjat või Ostja vara mistahes kujutletaval viisil;
   b) sündmuste järjekord, sealhulgas tegevused seoses intsidendi haldamisega;
   c) mõjutatud infrastruktuuri, süsteemi ja andmete osad;
   d) hinnangulised (või kõrge ebaselgustaseme korral kõige mustema stsenaariumi) tagajärjed/mõju;
   e) juba rakendatud tagajärgede leevendamise meetmed;
   f) juba rakendatud riskide vähendamise meetmed;
   g) rakendatavad tagajärgede leevendamise meetmed, sealhulgas rakenduskava (kuupäev; vastutaja; sõltumised);
   h) rakendatavad riskide vähendamise meetmed, sealhulgas rakenduskava (kuupäev; vastutaja; sõltuvused);
   i) kogemuste kokkuvõte.
5. Tarnija osutab Ostjale kohtuliku uurimise puhul abi.

5.14. Äritegevuse järjepidevuse juhtimine

1. Tarnija tuvastab äritegevuse järjepidevusega seonduvad riskid ja võtab kasutusele vastavate riskide kontrollimiseks ning leevendamiseks vajalikud meetmed.
2. Tarnijal on äritegevuse järjepidevuse turbega tegelemiseks dokumenteeritud protsessid ja praktikad.
3. Tarnija tagab, et infoturve on osaks äritegevuse jätkusuutlikkuse tagamise plaanidest.
4. Tarnija hindab perioodiliselt oma äritegevuse järjepidevuse juhtimise tõhusust ja selle vastavust käideldavuse nõuetele (kui need on sätestatud).

5.15. Vastavus

1. Tarnija järgib kõiki asjakohaseid õigusaktidest ja lepingutest tulenevaid nõudeid, sealhulgas Isikuandmete kaitsega seonduvaid.
2. Tarnija esitab nõudmise korral Ostjale käesolevatele Turvadirektiividele vastavuse kohta aruande ilma põhjendamata viivituseta.
3. Ostjal on õigus auditeerida, kuidas Tarnija ja tema alltöövõtjad täidavad Turvadirektiive või vastavaid nõudeid.

6. Infoturbe konfidentsiaalsusklasside kirjeldus ja käitlemise nõuded

6.1. Infoturbe konfidentsiaalsusklasside kirjeldus

Klass	Kirjeldus	Info liikide näited
Salajane	Volitamata juurdepääs infole või info avalikustamine võib **tõsiselt kahjustada** Ostjat, tema organisatsiooni, elutähtsaid funktsioone, töötajaid, äripartnereid ja/või kliente.	- majandusaasta aruanne ja tulem enne avaldamist - teatav info lähtuvalt juriidilistest nõuetest või konkreetsetest kliendilepingutest või konfidentsiaalsuse lepingutest
Konfidentsiaalne	Volitamata juurdepääs infole või info avalikustamine võib **kahjustada** Ostjat, tema organisatsiooni, kriitilise tähtsusega funktsioone, töötajaid, äripartnereid ja/või kliente.	- teatav info lähtuvalt juriidilistest nõuetest, nt klientide või töötajate isikuandmed - tundlikud äriplaanid, strateegiad ja otsused (nt turundusplaanid)
Sisekasutuseks	Volitamata juurdepääs infole või info avalikustamine võib põhjustada **väiksemat kahju** Ostjale, tema organisatsioonile, kriitilise tähtsusega funktsioonidele, töötajatele, äripartneritele ja/või klientidele.	- info, mis on mõeldud TC sisekasutuseks - kõigile TC töötajatele suunatud teabematerjalid, nt mis on seotud TC organisatsiooniga, strateegiaga, toodetega, töötajatele pakutavate teenustega
Avalik	Volitamata juurdepääs infole või info avalikustamine ei põhjusta **kahju** Ostjale, tema organisatsioonile, kriitilise tähtsusega funktsioonidele, töötajatele, äripartneritele ja/või klientidele.	- majandusaasta aruanne ja tulem pärast avaldamist - avaldatud turundusmaterjalid ja pressiteated - info, mida on vaja avaldada juriidilistest nõuetest tulenevalt

6.2. Infoturbe konfidentsiaalsusklasside käitlemise nõuded

Klass	Kellel võib olla juurdepääs infole	Kuidas säilitada	Kuidas üle kanda	Kuidas kasutada	Kuidas hinnata kaitse vajadust (riskipõhine lähenemisviis)

Salajane	Ainult määratud isikud	Loogiliselt ja füüsiliselt turvatud salvestus, st krüpteeritult või lukustatult	Kasutades turvalisi sidekanaleid või turvalist kaasaskantavat salvestusseadet (lukustatult)	Kasutamiseks turvatud aladel, mis on kaitstud (volitamata isikute) pealtnägemise ja pealtkuulamise eest	Kaitse murdmine peab olema väga raske. Üksnes äärmiselt motiveeritud ja/või leidlikud ründajad suudaksid kaitse maha võtta.
Konfidentsiaalne	Ainult piiratud *ja kontrollitud* isikute rühm	Loogiliselt ja füüsiliselt kontrollitud ja usaldatav salvestus range pääsu reguleerimisega	Kasutades turvalisi sidekanaleid või kontrollitud ja usaldatavas võrgus või kasutades turvalist kaasaskantavat salvestusseadet	Kasutamiseks volitatud isikute poolt üksnes äritegevuse eesmärgil kontrollitud töökohal või kohas, mis on kaitstud (volitamata isikute) pealtnägemise ja pealtkuulamise eest	Volitamata isikutel peab olema raske infole juurdepääsu saada. Üksnes hästi motiveeritud ründajad suudaksid kaitse maha võtta.
Sisekasutuseks	Need, kes töötavad Ostja heaks	Loogilise ja füüsilise pääsu reguleerimisega	Kasutades kaitstud sidekanaleid või usaldatavas võrgus	Kasutamiseks volitatud isikute poolt üksnes äritegevuse eesmärgil kontrollitud töökohal või kohas, mis on kaitstud (volitamata isikute) pealtnägemise ja pealtkuulamise eest	Volitamata isikutele peab olema infole juurdepääsu saamine ebatõenäoline. Üksnes motiveeritud ründajad suudaksid kaitse maha võtta.
Avalik	Piirangud puuduvad	Piirangud puuduvad	Piirangud puuduvad	Piirangud puuduvad	Piirangud puuduvad