| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | | |
| Dokumendi number:<br>PII24 | | | | | Dokumendi pealkiri:<br>**CCTV ja füüsilise seire privaatsuspoliitika** | | | | | | | |
| Versioon:<br>1.0 | | Jõustumiskuupäev:<br>01.01.2025 | | | Dokumendi omanik: | | | | | | | |
| X | Poliitika | | Standard | | Protseduur | | Vorm | | Register | | Muu | |

| **Muudatuste ajalugu** | | | | |
|---|---|---|---|---|
| **Muudatuse number** | **Muudatuse kuupäev** | **Muudatused** | **Läbi vaadanud** | **Protsessi omanik** |
| | | | | |
| | | | | |

| **Kinnitused** | | | |
|---|---|---|---|
| **Nimi** | **Ametikoht** | **Kuupäev** | **Allkiri** |
| | | | |
| | | | |

## Kooskõla standardite ja regulatsioonidega

| Standard/õigusnorm | Punkt/kontrollimeede/artikkel | Kohaldatavus | Katvuse tüüp | Kommentaar |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 7.5; Clause 8.1 | Both | Primary | Dokumenteeritud ja operatiivsed kontrollimeetmed |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Seire ja parandusmeetmed |
| ISO/IEC 27701:2025 | Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9 | Controller | Primary | Eesmärk, õiguslik alus, riskipäästik ja kirjed |
| ISO/IEC 27701:2025 | Annex A.1.2.7; Annex A.1.2.8 | Controller | Supporting | Volitatud töötleja ja kaasvastutava töötleja vastutusvaldkondade jaotus |
| ISO/IEC 27701:2025 | Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10 | Controller | Supporting | Isikuandmesubjektiga seotud kohustused ja taotlused |
| ISO/IEC 27701:2025 | Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9 | Controller | Primary | Kogumine, töötlemine, minimeerimine, säilitamine ja kõrvaldamine |
| ISO/IEC 27701:2025 | Annex A.1.5.4; Annex A.1.5.5 | Controller | Primary | Avalikustamise kirjed ja taotlused |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7 | Processor | Supporting | Volitatud töötleja lepingud, juhised, tugi ja kirjed |
| ISO/IEC 27701:2025 | Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6 | Processor | Supporting | Volitatud töötleja õigused ja avalikustamise tugi |
| ISO/IEC 27701:2025 | Annex A.3.14; Annex A.3.25 | Both | Supporting | Kirjete kaitse ja logimine |
| GDPR | Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2) | Controller | Primary | Põhimõtted ja vastutus |
| GDPR | Article 6 | Controller | Primary | Õiguslik alus |
| GDPR | Article 12; Article 13; Article 14 | Controller | Primary | Läbipaistvus ja teated |
| GDPR | Article 15; Article 16; Article 17; Article 18; Article 21 | Controller | Supporting | Õiguste taotlused |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39 | Both | Supporting | Juhtimine, volitatud töötlejad, kirjed, turvalisus, DPIA ja nõustamine |
| ISO/IEC 29100:2020 | Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6 | Controller | Supporting | Eesmärk, kogumine, minimeerimine, säilitamine ja avalikustamine |
| ISO/IEC 29100:2020 | Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12 | Both | Supporting | Läbipaistvus, osalemine, vastutus, turvalisus ja vastavus |
| ISO/IEC 29134:2020 | Clause 5.1; Clause 6.2 | Controller | Supporting | Privaatsusrisk ja DPIA päästikud |
| ISO/IEC 29151:2022 | Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10 | Both | Supporting | PII kaitse privaatsuskontrollid |
| ISO/IEC 29151:2022 | Clause 9.2.3; Clause 9.4.2; Clause 11.1.3 | Both | Supporting | Juurdepääsu ja füüsilise sisenemise kontrollimeetmed |
| ISO/IEC 27002:2022 | Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 | Both | Supporting | PII, füüsiline seire, juurdepääsupiirang ja logimine |

## 1. Kohaldamisala

1.1 Käesolev poliitika kehtib CCTV, videovalve, külastajate seire, füüsilise juurdepääsu kontrolli logide, turvatöötajate tehtava seire kirjete, ruumide seiresüsteemide ja nendega seotud füüsilise seire tegevuste suhtes, mille käigus kogutakse või muul viisil töödeldakse PII.

1.2 Käesolev poliitika kehtib organisatsioonidele, kes tegutsevad oma ruumide ja füüsilise seire tegevuste puhul PII vastutava töötlejana.

1.3 Käesolev poliitika kehtib ka volitatud töötleja või alltöötleja tugitegevuste suhtes, kui organisatsioon käitab, majutab, vaatab läbi, salvestab, avalikustab, kustutab või muul viisil töötleb kliendi nimel seiresalvestisi, külastajaandmeid või füüsilise juurdepääsu logisid.

1.4 Käesolev poliitika hõlmab seire eesmärgi määratlemist, heakskiitmist, teavitamist ja märgistust, juurdepääsupiiranguid, avalikustamist, säilitamist, kustutamist, allhanget, intsidentide eskaleerimist, õiguste taotluste suunamist, läbivaatamist ja tõendusmaterjali haldust.

1.5 Käesolev poliitika ei anna tööõiguslikku nõu, töötajate esinduskogu õiguslikku kommentaari, õiguskaitseasutuste menetlusjuhiseid ega eraldi CCTV registrit.

1.6 Seirepõhist tõendusmaterjali hoitakse käesolevas poliitikas nimetatud kanoonilistes PIMS-i tõendusobjektides.

## 2. Eesmärk

2.1 Käesoleva poliitika eesmärk on kehtestada privaatsuskontrollid CCTV ja füüsilise seire jaoks, et seiretegevused oleksid eesmärgipärased, läbipaistvad, proportsionaalsed, juurdepääsukontrolliga kaitstud, kindlaksmääratud tähtaegadega säilitatavad, avalikustatavad üksnes heakskiidetud kanalite kaudu ning toetatud auditiks sobiva PIMS-i tõendusmaterjaliga.

2.2 Käesolev poliitika toetab seiresalvestiste, külastajakirjete, füüsilise juurdepääsu logide ja nendega seotud seire PII järjepidevat käitlemist, loomata täiendavaid registreid, komiteesid, juhtpaneele ega mittekanoonilisi rolle.

## 3. Eesmärgid

### 3.1 Käesoleva poliitika eesmärgid on järgmised:

3.1.1 määratleda seire eesmärgid ja töötlemise ulatus enne seire alustamist;

3.1.2 dokumenteerida CCTV, füüsilise juurdepääsu, külastajate seire ja füüsilise seire tegevused tõendusobjektis REG02;

3.1.3 tuvastada seiretegevused, mis nõuavad privaatsusriskide ülevaatust või DPIA vajaduse hindamist tõendusobjektis REG04;

3.1.4 hoida läbipaistva teavituse ja märgistuse tõendusmaterjali tõendusobjektis REG07;

3.1.5 piirata juurdepääsu seire PII-le, selle vaatamist, eksportimist, avalikustamist ja säilitamist;

3.1.6 suunata isikuandmesubjektide taotlused tõendusobjekti REG06 kaudu;

3.1.7 hallata allhanke korras kasutatavaid seireteenuse osutajaid ja andmete jagamise tõendusmaterjali tõendusobjektis REG08;

3.1.8 eskaleerida kahtlustatavad seirega seotud PII intsidendid tõendusobjekti REG10 kaudu;

3.1.9 registreerida läbivaatamised, erandid, mittevastavused, parandusmeetmed, auditileiud ja parendused tõendusobjektis REG12.

## 4. Poliitika põhimõtted

### 4.1 Seire register, eesmärk ja heakskiit

4.1.1 [Controller] Process Owner / Business Owner peab enne tegevuse alustamist registreerima iga CCTV, külastajate seire, füüsilise juurdepääsu kontrolli logi või füüsilise seire tegevuse tõendusobjektis REG02.

4.1.2 [Controller] Privacy Lead / PIMS Manager peab enne uue või oluliselt muudetud seiretegevuse aktiveerimist valideerima REG02 kirje eesmärgi, õigusliku aluse, seiratava asukoha, PII kategooriate, isikuandmesubjekti kategooriate, säilitamise, teavituse, juurdepääsu ja avalikustamise väljade osas.

4.1.3 [Controller] Process Owner / Business Owner peab enne kaamerate, andurite, külastajalogide või juurdepääsukontrolli logimise lubamist registreerima heakskiidetud seirealad, välistatud alad ja kogumise piirid tõendusobjektis REG02.

4.1.4 [Conditional] Process Owner / Business Owner peab enne süstemaatilist seiret, helisalvestust, biomeetrilist tuvastamist, analüütikaga võimaldatud tuvastamist, tundlikke asukohti, haavatavaid isikuid või mitte-ilmset seiret hõlmava seire aktiveerimist saama privaatsusriski otsuse tõendusobjektis REG04.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager peab enne üürileandja, rajatiste partneri, kliendi või muu kaasvastutava töötlejaga ühise seire alustamist registreerima ühise seire vastutusvaldkondade jaotuse tõendusobjektis REG08.

4.1.6 [Processor] Privacy Lead / PIMS Manager peab enne kliendi nimel seiresalvestiste, külastajakirjete või füüsilise juurdepääsu logide töötlemist registreerima kliendi seirejuhised ja lubatud töötlemise piirid tõendusobjektis REG08.

**4.2 Teavitus ja läbipaistvus**

4.2.1 [Controller] Process Owner / Business Owner peab tagama, et seirest teavitavate siltide või samaväärse just-in-time teavituse tõendusmaterjal registreeritakse tõendusobjektis REG07 enne seiratavate alade avamist isikuandmesubjektidele.

4.2.2 [Controller] Privacy Lead / PIMS Manager peab enne avaldamist või olulist muudatust siduma iga seireteate tõendusobjektis REG07 vastava REG02 töötlemise eesmärgiga.

4.2.3 [Processor] Privacy Lead / PIMS Manager peab esitama privaatsusteate tugiteabe tõendusobjektis REG08, kui organisatsioon osutab seireteenuseid kliendi juhiste alusel.

4.2.4 [Conditional] Process Owner / Business Owner peab enne mitte-ilmse või hädaolukorra seire aktiveerimist registreerima alternatiivsed läbipaistvusmeetmed tõendusobjektides REG07 ja REG04.

[ ... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ... ]

**9. Erandid**

9.1 [All] Privacy Lead / PIMS Manager peab enne erandi kasutamist registreerima iga käesoleva poliitika erandi tõendusobjektis REG12.

9.2 [Conditional] Data Protection Officer / Privacy Advisor peab enne mitte-ilmset seiret, helisalvestust, biomeetrilist tuvastamist, analüütikaga võimaldatud seiret või tundlikke seireasukohti hõlmavate erandite heakskiitmist dokumenteerima privaatsusalase nõu tõendusobjektis REG04 või REG12.

9.3 [All] Top Management peab enne pikendamist üle esialgse erandiperioodi heaks kiitma üle 90 päeva kestvad erandid tõendusobjektis REG12.

9.4 [All] Privacy Lead / PIMS Manager peab avatud seireerandeid tõendusobjektis REG12 läbi vaatama vähemalt kord kuus kuni sulgemiseni.

**10. Jõustamine**

10.1 [All] Privacy Lead / PIMS Manager peab registreerima seire kontrollimeetmete tõrked mittevastavustena tõendusobjektis REG12 viie tööpäeva jooksul pärast kinnitamist.

10.2 [Both] Information Security Lead peab peatama loata juurdepääsu seiresüsteemile ühe tööpäeva jooksul pärast kinnitamist ja registreerima tegevuse tõendusobjektis REG10 või REG12.

10.3 [All] Top Management peab korduvate või oluliste poliitikarikkumiste korral määrama parandusmeetme vastutaja tõendusobjektis REG12 10 tööpäeva jooksul.

10.4 [Conditional] Incident Response Coordinator peab seire PII kahtlustatava loata avalikustamise, kaotsimineku või kompromiteerimise korral käivitama PII intsidendi töövoo tõendusobjektis REG10.

## 11. Läbivaatamine ja ajakohastamine

11.1 [All] Privacy Lead / PIMS Manager peab käesoleva poliitika ja sellega seotud seire tõendusmaterjali tõendusobjektis REG12 läbi vaatama vähemalt kord aastas.

11.2 [Controller] Process Owner / Business Owner peab vähemalt kord aastas uuesti valideerima iga aktiivse seire eesmärgi, teavituse, asukoha ulatuse ja säilitamiskirje tõendusobjektides REG02 ja REG07.

11.3 [Both] System Owner / Application Owner peab vähemalt kord aastas ja pärast olulist süsteemimuudatust uuesti valideerima seiresüsteemi juurdepääsu-, logimis-, kustutamis- ja ekspordikontrollid tõendusobjektis REG12.

11.4 [Conditional] Vendor / Procurement Owner peab vähemalt kord aastas ja enne lepingu uuendamist uuesti valideerima allhanke korras kasutatava seireteenuse osutaja tõendusmaterjali tõendusobjektis REG08.

11.5 [All] Privacy Lead / PIMS Manager peab 30 kalendripäeva jooksul pärast heakskiidetud poliitikamuudatusi ajakohastama seotud REG02, REG04, REG07, REG08, REG10 või REG12 tõendusmaterjali.

## 12. Seotud poliitikad

12.1 PII02 - Privaatsusrollide, vastutuste ja vastutuse poliitika

12.2 PII03 - PII töötlemise registri ja õigusliku aluse poliitika

12.3 PII04 - Privaatsusteate ja läbipaistvuse poliitika

12.4 PII06 - Isikuandmesubjekti õiguste haldamise poliitika

12.5 PII07 - Privaatsusriskide hindamise ja DPIA poliitika

12.6 PII08 - Lõimitud ja vaikimisi privaatsuse poliitika

12.7 PII09 - PII kogumise, kasutamise, avalikustamise ja jagamise poliitika

12.8 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika

12.9 PII12 - Volitatud töötleja, alltöötleja ja kolmanda osapoole privaatsushalduse poliitika

12.10 PII13 - Rahvusvahelise PII edastamise poliitika

12.11 PII14 - PII turbe ja juurdepääsukontrolli poliitika

12.12 PII15 - PII intsidendi ja rikkumise haldamise poliitika

12.13 PII17 - PIMS-i dokumenteeritud teabe ja tõendusmaterjali haldamise poliitika

12.14 PII18 - PIMS-i seire, auditi ja parendamise poliitika

12.15 PII19 - Töötajate privaatsuspoliitika

12.16 PII21 - Tehisintellekti ja automatiseeritud otsuste tegemise privaatsuspoliitika

12.17 PII23 - Pilvekeskkonna PII volitatud töötleja poliitika

## 13. Viitestandardid ja raamistikud

13.1 Käesolev poliitika on vastendatud järgmiste standardite ja õigusnormidega. Vastendus selgitab, kuidas poliitika toetab viidatud nõudeid, ning määrab kindlaks sisemised punktid, mis neid rakendavad või toetavad.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Vastendatud dokumenteeritud seire tõendusmaterjali, tegevuse planeerimise, aktiveerimiskontrollide, eesmärgikirjete, teavituse seoste,

juurdepääsukonfiguratsiooni, säilitamiskonfiguratsiooni ja CCTV ning füüsilise seire tegevuste muudatuste ohjega. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Vastendatud seire kontrollimeetmete mõõtmise, teenuseosutajate läbivaatamise, juurdepääsuõiguste läbivaatamise, auditileidude, mittevastavuste, parandusmeetmete, tähtaja ületanud tegevuste eskaleerimise ja parendamise tõendusmaterjaliga. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Vastendatud vastutava töötleja seire eesmärgi määratlemise, õigusliku aluse dokumenteerimise, privaatsusriski päästikute otsuste ning seire töötlemistoimingute kirjetega tõendusobjektides REG02 ja REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Vastendatud allhanke korras kasutatava seireteenuse osutaja vastutusvaldkondade jaotuse, ühise seire vastutusvaldkondade jaotuse ning volitatud töötleja või kaasvastutava töötleja tõendusmaterjaliga tõendusobjektis REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Vastendatud seirega seotud isikuandmesubjekti kohustuste, taotluste suunamise, taotluste hindamiseks vajaliku säilitamise ja õiguste toetamise juhtimise tõendusmaterjaliga. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Vastendatud seirekogumise piiramise, töötlemise piiride, minimeerimise, säilitamistähtaegade, kustutamise, ülekirjutamise, säilitamishoidude ja väljavõetud koopiate kontrolliga. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Vastendatud välise avalikustamise kirjete, avalikustamistaotluste käsitlemise, enne avalikustamist tehtava minimeerimise ning seire PII-ga seotud intsidendiga seotud avalikustamistega. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Vastendatud volitatud töötleja kliendi juhiste, lubatud töötlemise piiride, teavituse toe, säilitamis- ja kustutamisjuhiste, õiguste taotluste abi ning allhanke korras osutatavate seireteenuste volitatud töötleja kirjetega. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Vastendatud volitatud töötleja toega kliendi kohustuste täitmiseks, avalikustamise loa, avalikustamiskirjete, avalikustamistaotlustest teavitamise ja õiguslikult siduva avalikustamise käsitlemisega seire PII puhul. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Vastendatud seirekirjete kaitse, piiratud juurdepääsu, privilegeeritud juurdepääsu läbivaatamise, juurdepääsulogide, loata juurdepääsu ohjeldamise ja seiresüsteemide logimise tõendusmaterjaliga. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

**13.3 GDPR**

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Vastendatud seaduslikkuse, õigluse, läbipaistvuse, eesmärgi piirangu, andmete minimeerimise, säilitamise piirangu ja seiretegevuste vastutuse tõendusmaterjaliga. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Vastendatud CCTV, külastajate seire, füüsilise juurdepääsu logide ja muude füüsilise seire tegevuste õigusliku aluse dokumenteerimisega. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Vastendatud läbipaistvate seireteadete, märgistuse tõendusmaterjali, teavituse seostamisega töötlemise eesmärkidega, volitatud töötleja privaatsusteate tugiteabe ning alternatiivsete läbipaistvusmeetmetega. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Vastendatud juurdepääsu, parandamise, kustutamise, piiramise, vastuväite, taotluste suunamise, taotluste hindamiseks vajaliku säilitamise ning seirega seotud kliendi abistamisega. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Vastendatud vastutava töötleja juhtimise, kaasvastutava töötleja vastutusvaldkondade jaotuse, volitatud töötleja juhtimise, töötlemistoimingute kirjete, seiresüsteemide turvalisuse, privaatsusriski ülevaatuse, DPIA päästikute ja privaatsusalase nõustamisega. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Vastendatud seire PII eesmärgi täpsustamise, kogumise piiramise, andmete minimeerimise, kasutamise piiramise, säilitamise piiramise ja avalikustamise piiramisega. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Vastendatud läbipaistvuse, isiku osalemise, vastutuse, infoturbe, vastavuse läbivaatamise, juurdepääsuõiguste läbivaatamise, õiguste taotluste suunamise, intsidendi eskaleerimise ja parandusmeetmete tõendusmaterjaliga. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

**13.5 ISO/IEC 29134:2020**

13.5.1 **Clause 5.1; Clause 6.2** - Vastendatud süstemaatilise, mitte-ilmse, heli-, biomeetrilise, analüütikaga võimaldatud, tundliku asukoha, haavatavaid isikuid puudutava või muu kõrgema riskiga füüsilise seire privaatsusriski ja DPIA päästikute hindamisega. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

**13.6 ISO/IEC 29151:2022**

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Vastendatud PII kaitse kontrollimeetmetega eesmärgi, kogumise, minimeerimise, säilitamise, avalikustamise ja isikuandmesubjekti osalemise jaoks seire kontekstides. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Vastendatud juurdepääsuõiguste andmise, teabe juurdepääsupiirangu ja füüsilise sisenemise kontrollimeetmetega, mis on seotud seiresüsteemide juurdepääsu ja füüsilise juurdepääsu kontrolli kirjetega. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

**13.7 ISO/IEC 27002:2022**

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Vastendatud privaatsuse ja PII kaitse, füüsilise sisenemise, füüsilise turbe seire, privilegeeritud juurdepääsu, teabe juurdepääsupiirangu ning CCTV ja füüsilise seire süsteemide logimise kontrollimeetmetega. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].