					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII24					Názov dokumentu: **Politika ochrany súkromia pri CCTV a monitorovaní fyzických priestorov**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma / predpis	Kapitola / kontrola / článok	Uplatniteľnosť	Typ pokrytia	Poznámka
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Zdokumentované a prevádzkové kontroly
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorovanie a nápravné opatrenia
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	Účel, právny základ, spúšťač rizika a záznamy
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Rozdelenie zodpovedností sprostredkovateľa a spoločného prevádzkovateľa
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	Povinnosti voči dotknutým osobám a žiadosti
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	Zber, spracúvanie, minimalizácia, uchovávanie a likvidácia
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Záznamy o poskytnutí a žiadosti
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	Zmluvy sprostredkovateľa, pokyny, podpora a záznamy
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	Práva sprostredkovateľa a podpora pri poskytovaní údajov
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrana záznamov a logovanie
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Zásady a preukázateľná zodpovednosť
GDPR	Article 6	Controller	Primary	Právny základ

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparentnosť a oznámenia
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Žiadosti o uplatnenie práv
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Správa a riadenie, sprostredkovatelia, záznamy, bezpečnosť, DPIA a poradenstvo
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Účel, zber, minimalizácia, uchovávanie a poskytovanie
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparentnosť, účasť, preukázateľná zodpovednosť, bezpečnosť a súlad
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Riziko ochrany súkromia a spúšťače DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Kontroly ochrany súkromia pri ochrane PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Kontroly prístupu a fyzického vstupu
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, monitorovanie fyzických priestorov, obmedzenie prístupu a logovanie

1. Rozsah

1.1 Táto politika sa vzťahuje na CCTV, video monitorovanie, monitorovanie návštevníkov, logy fyzického riadenia prístupu, záznamy z monitorovania vykonávaného strážnou službou, systémy monitorovania priestorov a súvisiace činnosti monitorovania fyzických priestorov, pri ktorých sa zhromažďujú alebo inak spracúvajú PII.

1.2 Táto politika sa vzťahuje na organizácie konajúce ako prevádzkovatelia PII pre svoje vlastné priestory a činnosti monitorovania fyzických priestorov.

1.3 Táto politika sa vzťahuje aj na podporné činnosti sprostredkovateľa alebo ďalšieho sprostredkovateľa, pri ktorých organizácia prevádzkuje, hostuje, preskúmava, uchováva, poskytuje, vymazáva alebo inak spracúva záznamy z monitorovania, údaje o návštevníkoch alebo logy fyzického prístupu v mene zákazníka.

1.4 Táto politika pokrýva definovanie účelu monitorovania, schvaľovanie, oznámenia a označenie priestorov, obmedzenia prístupu, poskytovanie údajov, uchovávanie, výmaz, outsourcing, eskaláciu incidentov, smerovanie žiadostí o uplatnenie práv, preskúmanie a správu dôkazov.

1.5 Táto politika neposkytuje poradenstvo v oblasti pracovného práva, právny komentár k zamestnaneckej rade, postupy pre orgány presadzovania práva ani samostatný register CCTV.

1.6 Dôkazy špecifické pre monitorovanie sa udržiavajú v kanonických dôkazových objektoch PIMS určených v tejto politike.

2. Účel

2.1 Účelom tejto politiky je ustanoviť kontroly ochrany súkromia pre CCTV a monitorovanie fyzických priestorov tak, aby monitorovacie činnosti mali určený účel, boli transparentné, primerané, riadené prístupovými oprávneniami, uchovávané počas vymedzených období, poskytované iba prostredníctvom schválených kanálov a podporené auditovateľnými dôkazmi PIMS.

2.2 Táto politika podporuje jednotné nakladanie so záznamami z monitorovania, záznamami o návštevníkoch, logmi fyzického prístupu a súvisiacimi PII z monitorovania bez vytvárania ďalších registrov, výborov, dashboardov alebo nekanonických rolí.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 definovať účely monitorovania a rozsah spracúvania pred začatím monitorovania;

3.1.2 dokumentovať CCTV, fyzický prístup, monitorovanie návštevníkov a činnosti monitorovania fyzických priestorov v REG02;

3.1.3 identifikovať monitorovacie činnosti, ktoré vyžadujú preskúmanie rizík ochrany súkromia alebo preverenie potreby DPIA v REG04;

3.1.4 udržiavať dôkazy o transparentných oznámeniach a označení priestorov v REG07;

3.1.5 obmedziť prístup, prezeranie, export, poskytovanie a uchovávanie PII z monitorovania;

3.1.6 smerovať žiadosti dotknutých osôb prostredníctvom REG06;

3.1.7 riadiť outsourcovaných poskytovateľov monitorovania a dôkazy o zdieľaní údajov prostredníctvom REG08;

3.1.8 eskalovať podozrenia na incidenty týkajúce sa PII súvisiace s monitorovaním prostredníctvom REG10;

3.1.9 zaznamenávať preskúmania, výnimky, nezhody, nápravné opatrenia, auditné zistenia a zlepšenia v REG12.

4. Vyhlásenia politiky

4.1 Evidencia monitorovania, účel a schválenie

4.1.1 [Controller] Process Owner / Business Owner musí zaznamenať každú činnosť CCTV, monitorovania návštevníkov, logovania fyzického riadenia prístupu alebo monitorovania fyzických priestorov v REG02 pred začatím tejto činnosti.

4.1.2 [Controller] Privacy Lead / PIMS Manager musí pred aktiváciou novej alebo podstatne zmenenej monitorovacej činnosti validovať záznam REG02 z hľadiska účelu, právneho základu, monitorovaného miesta, kategórií PII, kategórií dotknutých osôb, uchovávania, oznámenia, prístupu a polí poskytovania údajov.

4.1.3 [Controller] Process Owner / Business Owner musí v REG02 zaznamenať schválené monitorované zóny, vylúčené zóny a hranice zberu pred povolením kamier, snímačov, záznamov o návštevníkoch alebo logovania riadenia prístupu.

4.1.4 [Conditional] Process Owner / Business Owner musí získať rozhodnutie o riziku ochrany súkromia v REG04 pred aktiváciou monitorovania, ktoré zahŕňa systematické monitorovanie, zvukový záznam, biometrickú identifikáciu, detekciu s podporou analytiky, citlivé miesta, zraniteľné osoby alebo nezjavné monitorovanie.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager musí zaznamenať rozdelenie zodpovedností za spoločné monitorovanie v REG08 pred začatím zdieľaného monitorovania s prenajímateľom, partnerom v oblasti správy priestorov, zákazníkom alebo iným spoločným prevádzkovateľom.

4.1.6 [Processor] Privacy Lead / PIMS Manager musí zaznamenať pokyny zákazníka k monitorovaniu a povolené hranice spracúvania v REG08 pred spracúvaním záznamov z monitorovania, záznamov o návštevníkoch alebo logov fyzického prístupu v mene zákazníka.

4.2 Oznámenie a transparentnosť

4.2.1 [Controller] Process Owner / Business Owner musí zabezpečiť, aby dôkazy o označení monitorovania alebo rovnocennom oznámení v čase potreby boli zaznamenané v REG07 pred sprístupnením monitorovaných priestorov dotknutým osobám.

4.2.2 [Controller] Privacy Lead / PIMS Manager musí prepojiť každé oznámenie o monitorovaní v REG07 so zodpovedajúcim účelom spracúvania v REG02 pred zverejnením alebo podstatnou zmenou.

4.2.3 [Processor] Privacy Lead / PIMS Manager musí poskytnúť podporné informácie k oznámeniu o monitorovaní v REG08, ak organizácia prevádzkuje monitorovacie služby podľa pokynov zákazníka.

4.2.4 [Conditional] Process Owner / Business Owner musí zaznamenať alternatívne opatrenia transparentnosti v REG07 a REG04 pred aktiváciou nezjavného alebo núdzového monitorovania.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Výnimky

9.1 [All] Privacy Lead / PIMS Manager musí zaznamenať každú výnimku z tejto politiky v REG12 pred použitím výnimky.

9.2 [Conditional] Data Protection Officer / Privacy Advisor musí zdokumentovať poradenstvo k ochrane súkromia v REG04 alebo REG12 pred schválením výnimiek zahŕňajúcich nezjavné monitorovanie, zvukový záznam, biometrickú identifikáciu, monitorovanie s podporou analytiky alebo citlivé monitorované miesta.

9.3 [All] Top Management musí schváliť výnimky presahujúce 90 dní v REG12 pred predĺžením nad rámec pôvodného obdobia výnimky.

9.4 [All] Privacy Lead / PIMS Manager musí najmenej mesačne preskúmavať otvorené výnimky týkajúce sa monitorovania v REG12 až do ich uzavretia.

10. Uplatňovanie politiky

10.1 [All] Privacy Lead / PIMS Manager musí zaznamenať zlyhania monitorovacích kontrol ako nezhody v REG12 do piatich pracovných dní od potvrdenia.

10.2 [Both] Information Security Lead musí pozastaviť neoprávnený prístup k monitorovaciemu systému do jedného pracovného dňa od potvrdenia a zaznamenať opatrenie v REG10 alebo REG12.

10.3 [All] Top Management musí pri opakovaných alebo podstatných porušeniach politiky priradiť vlastníctvo nápravného opatrenia v REG12 do 10 pracovných dní.

10.4 [Conditional] Incident Response Coordinator musí pri podozrení na neoprávnené poskytnutie, stratu alebo kompromitáciu PII z monitorovania spustiť pracovný tok incidentu týkajúceho sa PII v REG10.

11. Preskúmanie a údržba

11.1 [All] Privacy Lead / PIMS Manager musí najmenej raz ročne preskúmať túto politiku a súvisiace dôkazy o monitorovaní v REG12.

11.2 [Controller] Process Owner / Business Owner musí najmenej raz ročne revalidovať každý aktívny účel monitorovania, oznámenie, rozsah miesta a záznam o uchovávaní v REG02 a REG07.

11.3 [Both] System Owner / Application Owner musí najmenej raz ročne a po podstatnej zmene systému revalidovať prístup k monitorovaciemu systému, logovanie, výmaz a kontroly exportu v REG12.

11.4 [Conditional] Vendor / Procurement Owner musí najmenej raz ročne a pred obnovením zmluvy revalidovať dôkazy o outsourcovanom poskytovateľovi monitorovania v REG08.

11.5 [All] Privacy Lead / PIMS Manager musí aktualizovať súvisiace dôkazy REG02, REG04, REG07, REG08, REG10 alebo REG12 do 30 kalendárnych dní po schválených zmenách politiky.

12. Súvisiace politiky

12.1 PII02 - Politika rolí, zodpovedností a preukázateľnej zodpovednosti v oblasti ochrany súkromia

12.2 PII03 - Politika evidencie spracúvania PII a právneho základu

12.3 PII04 - Politika oznámení o ochrane údajov a transparentnosti

12.4 PII06 - Politika riadenia práv dotknutých osôb

12.5 PII07 - Politika posudzovania rizík ochrany súkromia a DPIA

12.6 PII08 - Politika ochrany súkromia už od návrhu a štandardne

12.7 PII09 - Politika zberu, používania, poskytovania a zdieľania PII

12.8 PII10 - Politika uchovávania, výmazu a likvidácie PII

12.9 PII12 - Politika riadenia sprostredkovateľov, ďalších sprostredkovateľov a tretích strán v oblasti ochrany súkromia

12.10 PII13 - Politika medzinárodných prenosov PII

12.11 PII14 - Politika bezpečnosti PII a riadenia prístupu

12.12 PII15 - Politika riadenia incidentov a porušení ochrany PII

12.13 PII17 - Politika zdokumentovaných informácií a správy dôkazov PIMS

12.14 PII18 - Politika monitorovania, auditu a zlepšovania PIMS

12.15 PII19 - Politika ochrany súkromia zamestnancov

12.16 PII21 - Politika ochrany súkromia pri AI a automatizovanom rozhodovaní

12.17 PII23 - Politika cloudového sprostredkovateľa PII

13. Referenčné normy a rámce

13.1 Táto politika je mapovaná na nasledujúce normy a predpisy. Mapovanie vysvetľuje, ako politika podporuje citované požiadavky, a identifikuje interné body, ktoré ich implementujú alebo podporujú.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapované na zdokumentované dôkazy o monitorovaní, prevádzkové plánovanie, kontroly aktivácie, záznamy účelu, väzbu na oznámenie, konfiguráciu prístupu, konfiguráciu uchovávania a riadenie zmien pri CCTV a činnostiach monitorovania fyzických priestorov. 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** - Mapované na meranie monitorovacích kontrol, preskúmanie poskytovateľov, preskúmanie prístupu, auditné zistenia, nezhody, nápravné opatrenia, eskaláciu oneskorených opatrení a dôkazy o zlepšovaní. 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** - Mapované na definovanie účelu monitorovania prevádzkovateľom, dokumentáciu právneho základu, rozhodnutia podľa spúšťačov rizika ochrany súkromia a záznamy o činnostiach spracúvania v rámci monitorovania v REG02 a 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** - Mapované na rozdelenie outsourcovaných poskytovateľov monitorovania, rozdelenie zodpovedností za spoločné monitorovanie a dôkazy o sprostredkovateľovi alebo spoločnom prevádzkovateľovi v 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** - Mapované na povinnosti voči dotknutým osobám súvisiace s monitorovaním, smerovanie žiadostí, uchovanie potrebné na posúdenie žiadostí a dôkazy o správe a riadení na podporu práv. 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** - Mapované na obmedzenie zberu pri monitorovaní, hranice spracúvania, minimalizáciu, obdobia uchovávania, výmaz, prepisovanie, pozastavenia výmazu a kontrolu extrahovaných kópií. 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** - Mapované na záznamy o externom poskytnutí, vybavovanie žiadostí o poskytnutie, minimalizáciu pred poskytnutím a poskytnutia súvisiace s incidentmi zahŕňajúcimi PII z monitorovania. 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** - Mapované na pokyny zákazníka pre sprostredkovateľa, povolené hranice spracúvania, podporu oznámení, pokyny na uchovávanie a výmaz, súčinnosť pri právach a záznamy sprostredkovateľa pre outsourcované monitorovacie služby. 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** - Mapované na podporu sprostredkovateľa pri povinnostiach zákazníka, oprávnenie na poskytnutie, záznamy o poskytnutí, oznamovanie žiadostí o poskytnutie a vybavovanie právne záväzných poskytnutí PII z monitorovania. 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** - Mapované na ochranu monitorovacích záznamov, obmedzený prístup, preskúmanie privilegovaného prístupu, logovanie prístupu, zamedzenie šírenia pri neoprávnenom prístupe a dôkazy o logovaní monitorovacích systémov. 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)** - Mapované na zákonnosť, spravodlivosť, transparentnosť, obmedzenie účelu, minimalizáciu údajov, obmedzenie uchovávania a dôkazy preukázateľnej zodpovednosti pri monitorovacích činnostiach. 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 - Mapované na dokumentáciu právneho základu pre CCTV, monitorovanie návštevníkov, logy fyzického prístupu a iné činnosti monitorovania fyzických priestorov. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mapované na transparentné oznámenia o monitorovaní, dôkazy o označení priestorov, väzbu oznámenia na účely spracúvania, podporné informácie sprostredkovateľa k oznámeniu a alternatívne opatrenia transparentnosti. 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** - Mapované na prístup, opravu, výmaz, obmedzenie, námietku, smerovanie žiadostí, uchovanie potrebné na posúdenie žiadostí a súčinnosť zákazníkovi súvisiacu s monitorovaním. 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** - Mapované na správu a riadenie prevádzkovateľa, rozdelenie spoločného prevádzkovateľa, riadenie sprostredkovateľov, záznamy o spracúvaní, bezpečnosť monitorovacích systémov, preskúmanie rizík ochrany súkromia, spúšťače DPIA a poradenstvo k ochrane súkromia. 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** - Mapované na špecifikáciu účelu, obmedzenie zberu, minimalizáciu údajov, obmedzenie použitia, obmedzenie uchovávania a obmedzenie poskytovania PII z monitorovania. 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** - Mapované na transparentnosť, účasť jednotlivca, preukázateľnú zodpovednosť, informačnú bezpečnosť, preskúmanie súladu, preskúmanie prístupu, smerovanie práv, eskaláciu incidentov a dôkazy o nápravných opatreniach. 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** - Mapované na preverenie rizík ochrany súkromia a spúšťačov DPIA pri systematickom, nezjavnom, zvukovom, biometrickom monitorovaní, monitorovaní s podporou analytiky, monitorovaní citlivých miest, zraniteľných osôb alebo inom monitorovaní fyzických priestorov s vyšším rizikom. 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** - Mapované na kontroly ochrany PII pre účel, zber, minimalizáciu, uchovávanie, poskytovanie a účasť dotknutých osôb v kontextoch monitorovania. 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** - Mapované na zriaďovanie prístupu, obmedzenie prístupu k informáciám a kontroly fyzického vstupu relevantné pre prístup k monitorovaciemu systému a záznamy fyzického riadenia prístupu. 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 - Mapované na ochranu súkromia a ochranu PII, fyzický vstup, monitorovanie fyzickej bezpečnosti, privilegovaný prístup, obmedzenie prístupu k informáciám a kontroly logovania pre CCTV a systémy monitorovania fyzických priestorov. 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].