					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII14					Заглавие на документа: **Политика за сигурност и контрол на достъпа до PII**							
Версия: 1.0		Дата на влизане в сила: 01.01.2025			Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго	

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

Съгласуване със стандарти и регулации

Стандарт / регулация	Клауза / контрол / член	Приложимост	Вид покритие	Коментар
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Планиране и функциониране на контролите за сигурност на PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Доказателства, мониторинг и коригиращи действия
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Идентичност и права за достъп при обработване на PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Защита на крайните точки и сигурна автентикация
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Журнализиране и криптографска защита
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Сигурност на приложенията и сигурна архитектура
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Защита и преглед на записите
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Сигурност, отчетност и контроли за обработващи лични данни
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Интеграция с контроли на ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Насоки за внедряване на контроли за сигурност
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Принципи за информационна сигурност и

				съответствие в областта на поверителността
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Контроли за сигурност за защита на PII

1. Обхват

1.1 Тази политика определя специфичните за PII изисквания за сигурност и контрол на достъпа за системи, приложения, услуги, устройства, облачни среди и оперативни процеси, които съхраняват, предават, обработват, достъпват, администрират или защитават PII.

1.2 Тази политика се прилага в контекст на администратор, съвместен администратор, обработващ лични данни и подизпълнител по обработване, когато организацията определя, експлоатира, поддържа или разчита на контроли за сигурност при обработване на PII.

1.3 Тази политика обхваща следните области на контролите за сигурност на PII:

1.3.1 базов набор от мерки за сигурност на PII и интеграция със съществуващите политики за информационна сигурност;

1.3.2 контрол на достъпа;

1.3.3 автентикация;

1.3.4 привилегирован достъп;

1.3.5 шифроване и сигурно съхранение;

1.3.6 журнализиране и мониторинг;

1.3.7 сигурна конфигурация и управление на уязвимостите;

1.3.8 контроли за достъп от крайни точки и облачни среди;

1.3.9 връзка с доказателства чрез REG02, REG08, REG10 и REG12.

1.4 Тази политика не замества цялостна система за управление на информационната сигурност, политика за мрежова сигурност, политика за сигурна разработка, политика за архивиране, политика за крайни точки, политика за облачна сигурност, криптографски стандарт, процедура за управление на уязвимости или процедура за реагиране при инциденти. Когато такива политики вече съществуват, тази политика определя специфичната за PII връзка и изискванията за доказателства, необходими за увереност по PIMS.

1.5 Тази политика не дублира:

1.5.1 инвентара на обработването на PII и собствеността върху правното основание в PII03;

1.5.2 методологията за риск за поверителността и DPIA в PII07;

1.5.3 контролните точки за поверителност още при проектиране в PII08;

1.5.4 правилата за събиране, използване, разкриване и споделяне в PII09;

1.5.5 изпълнението на съхранението, изтриването и унищожаването в PII10;

1.5.6 управлението на жизнения цикъл на обработващите лични данни в PII12;

1.5.7 контролите върху механизмите за международен трансфер в PII13;

1.5.8 работния процес при инциденти и нарушения в PII15;

1.5.9 управлението на документираната информация в PII17;

1.5.10 управлението на мониторинга, одита и подобрението на PIMS в PII18.

1.6 За целите на тази политика оперативните журнали, резултатите от инструменти за сигурност, експортите от прегледи на достъпа, докладите за уязвимости и доказателствата за конфигурация са източници на доказателства, които се прилагат към, обобщават в или се посочват чрез каноничните доказателствени обекти. Те не са отделни регистри на PIMS.

2. Цел

2.1 Целта на тази политика е да гарантира, че PII е защитена чрез подходящи, съобразени с риска и подлежащи на одитиране контроли за сигурност и достъп през целия процес на обработване.

2.2 Тази политика позволява на организацията да докаже, че контролите за сигурност на PII се планират, внедряват, преглеждат, наблюдават и подобряват чрез REG02, REG08, REG10 и REG12, без да се създават дублиращи регистри за сигурност или да се заменят съществуващи политики за информационна сигурност.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 определи базов набор от контроли за достъп до PII за системи и дейности по обработване;

3.1.2 гарантира, че контролите за автентикация са подходящи спрямо чувствителността и контекста на достъп до PII;

3.1.3 определи изисквания за преглед на привилегирования и обикновения достъп до PII;

3.1.4 определи очакванията за шифроване и сигурно съхранение на PII в покой, при пренос и в съответните облачни или крайни контексти;

3.1.5 определи очакванията за журнализиране и мониторинг на достъпа до, промените в и администрирането на PII;

3.1.6 определи изискванията за доказателства относно сигурната конфигурация и уязвимостите за системи, обработващи PII;

3.1.7 определи очакванията за достъп от крайни точки и облачни среди, без да създава цялостна политика за крайни точки или облачна сигурност;

3.1.8 свърже предполагаемите инциденти по сигурността на PII с REG10, без да дублира работния процес за инциденти;

3.1.9 се интегрира със съществуващите политики за информационна сигурност, когато има такива;

3.1.10 поддържа доказателства, готови за одит, като използва само REG02, REG08, REG10 и REG12.

4. Декларации на политиката

4.1 Базов набор от мерки за сигурност на PII и интеграция с ISMS

4.1.1 [Both] Information Security Lead MUST определи базовия набор от мерки за сигурност на PII за всяка система или услуга, която обработва PII, в REG12, преди системата или услугата да бъде въведена в продукционна среда или да бъде съществено променена.

4.1.2 [Both] System Owner / Application Owner MUST запише местоположението на доказателствата за внедрените контроли за сигурност на PII в REG12, преди да разчита на съществуващ контрол за информационна сигурност за увереност по PIMS.

4.1.3 [Controller] Process Owner / Business Owner MUST идентифицира чувствителността на PII, контекста на обработване и необходимостта от достъп в REG02, преди да поиска нов или съществено променен достъп до PII.

4.1.4 [Processor] Vendor / Procurement Owner MUST запише нарежданията на клиента относно сигурността, границите на отговорност на клиента и ангажиментите на обработващия лични данни по сигурността в REG08, преди да започне или съществено да се промени достъпът на обработващия лични данни до клиентска PII.

4.1.5 [Both] Privacy Lead / PIMS Manager MUST провери, че доказателствата за сигурността на PII са свързани с REG02, REG08, REG10 или REG12, преди да приеме дейността по обработване като подлежаща на одитиране по PIMS.

4.2 Базов контрол на достъпа

4.2.1 [Both] System Owner / Application Owner MUST ограничи достъпа до PII до одобрени роли и оторизирани потребители, записани или проследими в REG02 или REG12, преди достъпът да бъде активиран.

4.2.2 [Both] Process Owner / Business Owner MUST одобри служебната цел за достъп до PII в REG02 или REG12, преди System Owner / Application Owner да предостави достъпа.

4.2.3 [Both] System Owner / Application Owner MUST преглежда потребителския достъп до системи, обработващи PII с високо въздействие или чувствителна PII, най-малко на тримесечна база и да записва резултата от прегледа в REG12.

4.2.4 [Both] System Owner / Application Owner MUST преглежда потребителския достъп до други системи, обработващи PII, най-малко ежегодно и да записва резултата от прегледа в REG12.

4.2.5 [Both] System Owner / Application Owner MUST премахне или измени достъпа до PII в REG12 в рамките на един работен ден след промяна на ролята, прекратяване на правоотношението, приключване на договора или когато достъпът вече не е необходим.

4.2.6 [Processor] Vendor / Procurement Owner MUST потвърди в REG08, че достъпът на обработващия лични данни до клиентска PII е ограничен до документираните нареждания на клиента, преди достъпът да бъде активиран или променен.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST потвърди в REG08, че достъпът на подизпълнителя по обработване до PII е ограничен до разрешените дейности по подизпълнение на обработването, преди достъпът на подизпълнителя по обработване да бъде активиран или променен.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Изключения

9.1.1 [Both] Information Security Lead MUST записва всяко изключение от изискване за сигурност или контрол на достъпа до PII в REG12, преди изключението да бъде активирано.

9.1.2 [Both] Data Protection Officer / Privacy Advisor MUST консултира по-високорисковите изключения по сигурността на PII в REG12 преди одобрение.

9.1.3 [Both] Top Management MUST одобри изключенията по сигурността на PII в REG12 преди активиране, когато изключението засяга PII с високо въздействие, чувствителна PII, привилегирован достъп, шифроване, журнализиране или нерешени високорискови уязвимости.

9.1.4 [Both] Information Security Lead MUST определи срока на изтичане на изключението, компенсиращия контрол и датата за преглед в REG12 преди одобряване на изключението.

9.1.5 [Both] System Owner / Application Owner MUST отстрани, поднови или закрие изтекли изключения по сигурността на PII в REG12 в рамките на пет работни дни след изтичане.

9.1.6 [Processor] Vendor / Procurement Owner MUST запише изключенията по сигурността на обработващ лични данни или подизпълнител по обработване, засягащи клиентска PII, в REG08 и REG12 преди приемане.

10. Прилагане на политиката

10.1.1 [Both] Privacy Lead / PIMS Manager MUST записва несъответствия за липсващи или непълни доказателства за сигурността на PII в REG12 в рамките на пет работни дни от идентифицирането.

10.1.2 [Both] Information Security Lead MUST възложи собственост върху отстраняването на откази на контроли за сигурност на PII в REG12 в рамките на пет работни дни след валидиране.

10.1.3 [Both] System Owner / Application Owner MUST деактивира или ограничи неоторизиран, прекомерен или неподкрепен с доказателства достъп до PII в рамките на един работен ден след валидиране и да запише действието в REG12.

10.1.4 [Conditional] Incident Response Coordinator MUST свърже действията по прилагане на политиката с REG10 в рамките на един работен ден, когато въпросът по прилагането включва предполагаем или потвърден инцидент с PII.

10.1.5 [Both] Top Management MUST преглежда повтарящите се или високорискови несъответствия по сигурността на PII в REG12 преди прегледа от ръководството.

11. Преглед и поддръжка

11.1.1 [All] Privacy Lead / PIMS Manager MUST преглежда тази политика съвместно с Information Security Lead най-малко ежегодно и да записва резултата от прегледа в REG12.

11.1.2 [Both] Information Security Lead MUST прегледа базовия набор от мерки за сигурност на PII в REG12 в рамките на 30 дни след съществена технологична промяна, промяна в заплахите, одит, инцидент или регулаторна промяна, засягаща сигурността на PII.

11.1.3 [Both] System Owner / Application Owner MUST актуализира доказателствата за сигурността на PII на системно ниво в REG12 в рамките на 30 дни след съществена промяна в архитектурата, достъпа, конфигурацията, уязвимостите или журнализирането.

11.1.4 [Processor] Vendor / Procurement Owner MUST прегледа доказателствата за отговорностите по сигурността на PII на обработващи лични данни и подизпълнители по обработване в REG08 в рамките на 30 дни след съществена промяна на услугата, нареждане на клиента или подизпълнител по обработване.

11.1.5 [All] Internal Audit / Compliance Reviewer MUST проверява доказателствата за преглед на политиката и избрани доказателства за контроли за сигурност на PII в REG12 съгласно одобрения план за одит.

12. Свързани политики

12.1 Тази политика следва да се чете заедно със:

12.2 PII01 - Политика за система за управление на неприкосновеността на личната информация;

12.3 PII02 - Политика за роли, отговорности и отчетност във връзка с поверителността;

12.4 PII03 - Политика за инвентар на обработването на PII и правно основание;

12.5 PII07 - Политика за оценка на риска за поверителността и DPIA;

12.6 PII08 - Политика за поверителност още при проектиране и по подразбиране;

12.7 PII09 - Политика за събиране, използване, разкриване и споделяне на PII;

12.8 PII10 - Политика за съхранение, изтриване и унищожаване на PII;

12.9 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни;

12.10 PII13 - Политика за международен трансфер на PII;

12.11 PII15 - Политика за управление на инциденти и нарушения, свързани с PII;

12.12 PII16 - Политика за обучение, осведоменост и компетентност относно поверителността;

12.13 PII17 - Политика за документирана информация и управление на доказателства в PIMS;

12.14 PII18 - Политика за мониторинг, одит и подобрение на PIMS.

13. Референтни стандарти и рамки

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].