					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P26					Заглавие на документа: **Политика за сигурност на трети страни и доставчици**							
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**

Съответствие със стандарти и регулаторни изисквания

Стандарт/регулация	**Клауза/член**	**Коментар**
ISO/IEC 27001:2022	Клауза 8	Оперативно планиране и контрол: изисква формални контроли върху услуги от трети страни, които оказват въздействие върху СУИС
ISO/IEC 27002:2022	Контроли 5.19–5.22	Политики и процедури за взаимоотношения с доставчици; Управление на риска, свързан с доставчиците; Управление на предоставянето на услуги от доставчици; Мониторинг и преглед на доставчиците
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Външни системни услуги; Управление на конфигурацията от разработчика; Взаимосвързаност между системи; Сигурност на персонала на трети страни
GDPR на ЕС	Членове 28, 32, 33	Задължения на обработващия лични данни; Сигурност на обработването; Уведомяване при нарушение на сигурността на личните данни
NIS2 на ЕС	Член 21(2)(e–f)	Управление на доставчиците, базирано на риска, и надзор върху сигурността
DORA на ЕС	Членове 28, 30	ИКТ риск, свързан с трети страни; Надзор върху критични външни доставчици на ИКТ услуги
COBIT 2019	BAI05, DSS02, MEA03	Управление на организационната промяна; Управление на заявки за услуги и инциденти; Мониторинг, оценяване и преценка на съответствието

1. Цел

1.1 Настоящата политика определя изискванията за информационна сигурност при установяване, управление и поддържане на сигурни взаимоотношения с доставчици и външни доставчици на услуги.

1.2 Тя гарантира, че всички доставчици с достъп до данните, системите или инфраструктурата на организацията подлежат на строги мерки за сигурност, договорни защитни механизми и непрекъснат надзор през целия жизнен цикъл на услугата.

1.3 Политиката подпомага контроли 5.19 до 5.22 от Приложение A на ISO/IEC 27001, като въвежда изисквания за сигурност в процесите по възлагане, въвеждане, надлежна проверка на доставчиците, управление на договорите, мониторинг на услугите и прекратяване.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички външни доставчици, външни изпълнители, облачни доставчици и организации, предоставящи услуги, които обработват или имат достъп до информационни активи на организацията

2.1.2 Всички вътрешни роли, участващи в оценка на доставчици, въвеждане, договаряне, управление на риска, мониторинг или прекратяване на взаимоотношения

2.1.3 Всички взаимоотношения с доставчици, които включват достъп до чувствителни данни, интеграция с продукционни услуги или поддръжка на критични бизнес функции

2.2 Политиката обхваща както преките доставчици, така и техните подизпълнители, когато е приложимо, и включва софтуер, инфраструктура, поддръжка и управлявани услуги, предоставяни от трети страни.

3. Цели

3.1 Да се гарантира, че рисковете за сигурността, свързани с доставчиците, се идентифицират, оценяват и третират последователно през целия жизнен цикъл на взаимоотношенията.

3.2 Да се въведат стандартизирани изисквания за сигурност във всички договори с доставчици, включително задължения за уведомяване при инциденти, клаузи за право на одит и отговорности по защита на данните.

3.3 Да се изисква формална надлежна проверка на доставчиците и документирани оценки на риска преди ангажиране на нови доставчици или подновяване на високорискови договорености за услуги.

3.4 Да се установят механизми за непрекъснат мониторинг на съответствието на доставчиците, включително прегледи на изпълнението, одити и ескалация на инциденти.

3.5 Да се управляват промените в услугите на доставчиците и да се прилага сигурно извеждане от експлоатация, както и връщане/унищожаване на данни при прекратяване.

3.6 Да се съгласуват контролите за сигурност на трети страни с приложимите регулаторни и договорни задължения, включително GDPR, NIS2, DORA и стандартите ISO/IEC 27001.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за тази политика и осигурява нейното съгласуване с цялостната система за управление на информационната сигурност (СУИС), управлението на риска и стратегията за съответствие.

4.1.2 Одобрява нивата на класификация на доставчиците, резултатите от прегледите по сигурността и високорисковите изключения.

4.1.3 Участва в ескалацията при сериозни инциденти, свързани с доставчици, и в договорни преговори за критични услуги.

4.2 Функция по възлагане и управление на доставчици

4.2.1 Гарантира, че всички нови и подновени договори с доставчици включват одобрени клаузи за сигурност и защита на данните.

4.2.2 Поддържа централизиран регистър на доставчиците и координира с Правни въпроси и Съответствие документацията, свързана с риска от трети страни.

4.2.3 Инициира процесите по въвеждане на доставчици и гарантира съгласуваност с оценките по сигурността преди сключване на договор.

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

9. Изисквания за преглед и актуализация

9.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно или по-рано в случай на:

9.1.1 Съществени промени в стратегията за възлагане или екосистемата от доставчици

9.1.2 Актуализации в правната или регулаторната рамка (напр. DORA, GDPR)

9.1.3 Съществени инциденти с трети страни, нарушения на сигурността на данните или неуспешни одити

9.1.4 Констатации от оценки на риска или от външни сертифициращи органи

9.2 Процесът по преглед се управлява съвместно от директора по информационна сигурност (CISO), функцията по възлагане, Правни въпроси и функциите по управление на риска.

9.3 Всички ревизии на политиката трябва да бъдат документирани в регистъра на документите на СУИС, да са под управление на версиите и да бъдат комуникирани до съответните заинтересовани страни чрез каналите за управление на доставчиците и програмите за осведоменост на служителите.

9.4 Заменените версии трябва да се архивират за минимум три години с цел проследимост и правно съответствие.

10. Свързани политики и връзки

10.1 P1 – Политика за информационна сигурност. Определя общия ангажимент за защита на всички операции на организацията, включително зависимостта от външни доставчици и външни доставчици на услуги.

10.2 P6 – Политика за управление на риска. Регламентира идентифицирането, оценката и третирането на рисковете, свързани с взаимоотношенията с трети страни, включително наследени или системни рискове от екосистемите на доставчици.

10.3 P17 – Политика за защита на данните и поверителност. Прилага се за всички доставчици, които обработват лични данни, като изисква подходящи договорни условия, защитни механизми при прехвърляне и принципи за защита на личните данни още при проектирането.

10.4 P4 – Политика за контрол на достъпа. Регламентира как персоналът на трети страни получава достъп до организационните системи, като налага разрешения, базирани на роли, контрол на сесиите и процедури за отнемане.

10.5 P22 – Политика за регистриране и мониторинг. Изисква достъпът на доставчиците до системите да бъде наблюдаван, журнализиран и преглеждан, особено в среди, в които се извършват привилегировани дейности или дейности, свързани с данни.

10.6 P30 – Политика за реагиране при инциденти. Определя процедурите за ескалация и изискванията за докладване на нарушения за събития по сигурността с произход от доставчици или съвместни разследвания, включващи системи на трети страни.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001: Клауза 8.1 – Оперативно планиране и контрол: Изисква формални контроли върху услуги от трети страни, които оказват въздействие върху СУИС.

11.2 ISO/IEC 27002:2022 – Контроли 5.19 до 5.22:

11.2.1 Контрол 5.19 от Приложение A – Политики и процедури за взаимоотношения с доставчици: Налага контроли за управление на взаимодействията с доставчици.

11.2.2 Контрол 5.20 от Приложение А – Управление на риска, свързан с доставчиците: Фокусира се върху идентифицирането, оценката и текущия надзор върху рисковата позиция по отношение на сигурността на доставчиците.

11.2.3 Контрол 5.21 от Приложение А – Управление на предоставянето на услуги от доставчици: Изисква съответствие на изпълнението и сигурността с договорните очаквания.

11.2.4 Контрол 5.22 от Приложение А – Мониторинг и преглед на доставчиците: Подчертава необходимостта от текущо валидиране и повторна оценка на съответствието на трети страни.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SA-9 – Външни системни услуги: Определя изискванията за сигурност и риск за системи, управлявани от външни субекти.

11.3.2 SA-10 – Управление на конфигурацията от разработчика: Прилага се, когато трети страни доставят софтуер или среди.

11.3.3 CA-3 – Взаимосвързаност между системи: Изисква надзор и съгласуване на потоците от данни между системи на различни субекти.

11.3.4 PS-7 – Сигурност на персонала на трети страни: Гарантира, че външните изпълнители и персоналът на доставчиците се проверяват и наблюдават по подходящ начин.

11.4 GDPR на ЕС (2016/679):

11.4.1 Член 28 – Задължения на обработващия лични данни: Изисква писмени споразумения с обработващите лични данни, включително технически и организационни мерки.

11.4.2 Член 32 – Сигурност на обработването: Изисква подходящи защитни мерки както от администраторите, така и от обработващите лични данни.

11.4.3 Член 33 – Уведомяване при нарушение на сигурността на личните данни: Изисква своевременно уведомяване от доставчиците при нарушение.

11.5 Директива NIS2 на ЕС (2022/2555):

11.5.1 Член 21(2)(e–f): Изисква управление на доставчиците, базирано на риска, и надзор върху сигурността, особено във веригите за цифрови доставки на съществени и важни субекти.

11.6 DORA на ЕС (2022/2554):

11.6.1 Член 28 – ИКТ риск, свързан с трети страни: Налага задължения за оценка на риска, договорни условия за сигурност и стратегии за изход за доставчици на финансови услуги.

11.6.2 Член 30 – Надзор върху критични външни доставчици на ИКТ услуги: Установява засилен мониторинг и надзорни очаквания за ключови доставчици.

11.7 COBIT 2019:

11.7.1 BAI05 – Управление на организационната промяна: Гарантира, че преходите с участието на доставчици се управляват по сигурен начин.

11.7.2 DSS02 – Управление на заявки за услуги и инциденти: Прилага се за докладвани от доставчици проблеми и интеграция на обработването на инциденти.

11.7.3 MEA03 – Мониторинг, оценяване и преценка на съответствието: Подчертава измерването на изпълнението на доставчиците и мониторинга на съответствието.