					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P26S					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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	Оперативни контроли за взаимоотношения с трети страни и доставчици
ISO/IEC 27002:2022	Контроли 5.19–5.22	Контроли за сигурност на доставчиците, договорни условия за сигурност, управление на промените, мониторинг и преглед
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Контроли при придобиване, конфигуриране, споразумения за свързаност и контрол върху външен персонал
GDPR на ЕС	Членове 28, 32	Споразумения за обработване на лични данни, изисквания за сигурност към обработващите лични данни
NIS2 на ЕС	Членове 21(2)(a)(b)(i), 23(1)	Управление на риска по веригата на доставки, надзор върху услуги от трети страни
DORA на ЕС	Членове 5(1)(2), 28(1)(2)	Управление на ИКТ риска за външни доставчици на услуги
COBIT 2019	APO10, APO12, DSS05	Управление на доставчици и интегриране на риска

1. Цел

1.1 Настоящата политика определя задължителните изисквания за сигурност при възлагане, управление и прекратяване на взаимоотношения с трети страни и доставчици, които имат достъп до данните, системите или услугите на организацията или оказват въздействие върху тях.

1.2 Тя гарантира, че външните доставчици — включително доставчикът на ИТ поддръжка, доставчиците на облачни услуги, разработчиците на софтуер и изпълнителите на бизнес процеси — обработват фирмените активи по сигурен начин и в съответствие с приложимите закони и стандарти.

1.3 Настоящата политика намалява рискове като изтичане на данни, неоторизирани промени по системите, регулаторни санкции или прекъсвания на дейността, причинени от несигурни или слабо управлявани взаимоотношения с трети страни.

2. Обхват

2.1 Настоящата политика се прилага за всички трети страни, които:

2.1.1 предоставят софтуер, инфраструктура, хостинг или облачни услуги

2.1.2 имат достъп до или администрират вътрешни системи, устройства или приложения

2.1.3 обработват фирмени данни, документи или резервни копия

2.1.4 подпомагат бизнес операциите, човешките ресурси (ЧР), финансовите дейности или обслужването на клиенти

2.2 Политиката се прилага също така за:

2.2.1 вътрешен персонал, участващ в подбора, възлагането или надзора върху доставчици

2.2.2 всеки служител, който управлява въвеждането на доставчици, договори, достъп или прегледи

2.2.3 всяка система или процес, зависими от компоненти или услуги на трети страни

3. Цели

3.1 Да се гарантира, че всички доставчици отговарят на ясно определени изисквания за сигурност.

3.2 Да се изисква договорите с доставчици да включват приложимите задължения за сигурност, поверителност и реагиране при инциденти.

3.3 Да се оценяват и документират рисковете, свързани с доставчиците, преди подписване на споразумения или предоставяне на достъп.

3.4 Да се извършват периодични прегледи на доставчици с висок риск или критично значение с цел потвърждаване на съответствието.

3.5 Да се установи формален процес за изключения, управление на инциденти и актуализиране на договорите.

3.6 Да се подпомогне съответствието със задълженията по ISO/IEC 27001:2022, GDPR, NIS2 и DORA, свързани с управлението на доставчици.

4. Роли и отговорности

4.1 Управител (GM)

4.1.1 Носи крайната отговорност за избора на доставчици и съответствието с изискванията за сигурност

4.1.2 Одобрява договори, изключения и ескалации, свързани с доставчици

4.1.3 Осъществява надзор върху реагирането при инциденти и вземането на решения, когато доставчици не изпълняват задълженията си

4.2 Външен доставчик на ИТ услуги или вътрешно лице за контакт по сигурността

4.2.1 Оценява техническия достъп, заявен от доставчици

4.2.2 Прилага правила за контрол на достъпа, преглежда журналите и проверява сигурното обработване на данни

4.2.3 Преглежда доказателства за контроли за сигурност, сертификации или резултати от одит, когато е приложимо

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

9. Преглед и актуализация на изискванията

9.1 Настоящата политика трябва да се преглежда поне веднъж годишно от Управителя, с участието на доставчика на ИТ поддръжка или мениджъра на доставчици.

9.2 Политиката трябва също да бъде преглеждана:

9.2.1 след всяка съществена промяна в правни, регулаторни или договорни задължения

9.2.2 след инцидент по сигурността, свързан с доставчик, или одитна констатация

9.2.3 при въвеждане на нови категории доставчици (напр. критични SaaS платформи)

9.3 Всички актуализации трябва да бъдат:

9.3.1 документирани с история на версиите и обосновка

9.3.2 одобрени от Управителя

9.3.3 комуникирани към съответния вътрешен персонал и мениджърите на доставчици

9.3.4 съхранявани заедно с предходните версии съгласно P14S – Политика за съхранение на данни и унищожаване

10. Свързани политики и връзки

10.1 Ефективността на настоящата политика зависи от координацията със следните SME политики по информационна сигурност:

10.1.1 P2S – Политика за роли и отговорности в управлението: Определя отчетността за надзора върху доставчиците и прилагането на договорните задължения.

10.1.2 P4S – Политика за контрол на достъпа: Определя правилата за ограничаване на достъпа, които трябва да се прилагат, когато на доставчици се предоставя системен достъп.

10.1.3 P17S – Политика за защита на данните и поверителност: Гарантира, че доставчиците, които обработват лични данни, спазват принципите за защита на данните и правните изисквания.

10.1.4 P14S – Политика за съхранение на данни и унищожаване: Прилага се към всички данни или записи, споделени с доставчици или съхранявани от тях, и урежда сигурното унищожаване след прекратяване на договора.

10.1.5 P30S – Политика за реагиране при инциденти: Определя начина на реагиране, когато доставчик причини или участва в инцидент по сигурността, включително процедурите за ескалация и обработване на доказателства.

10.2 Тези политики действат съвместно, за да гарантират, че рискът, свързан с доставчиците, се контролира през целия жизнен цикъл на договора.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква прилагане на оперативни контроли, включително такива, приложими към отношенията с трети страни и доставчици.

11.2 ISO/IEC 27002

11.2.1 Контрол 5.19 – Гарантира, че мерките за сигурност на доставчиците са съгласувани с изискванията на организацията.

11.2.2 Контрол 5.20 – Изисква формални споразумения, обхващащи условията за сигурност, отговорностите и задълженията при нарушение.

11.2.3 Контрол 5.21 – Урежда промените в услугите на доставчиците, които могат да повлияят на рисковата позиция по отношение на сигурността.

11.2.4 Контрол 5.22 – Изисква мониторинг и преглед на услугите на доставчиците и съответствието.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Урежда придобиването на външни системи и услуги, като изисква оценки на риска и ясно определени очаквания.

11.3.2 SA-10 – Контролира процедурите по конфигуриране и промени, свързани със системи, управлявани от трети страни.

11.3.3 CA-3 – Изисква споразумения за свързаност за системи, включващи външни субекти.

11.3.4 PS-7 – Определя изисквания за проверка и отчетност за външен персонал.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 28 – Изисква споразумение за обработване на лични данни с доставчици, действащи като обработващи лични данни.

11.4.2 Член 32 – Изисква подходящи технически и организационни мерки за сигурност за всички обработващи лични данни.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(a), (b), (i) – Изисква управление на риска по веригата на доставки на ИКТ и контроли за трети страни.

11.5.2 Член 23(1) – Изисква документиран надзор върху услуги от трети страни за съществени и важни субекти.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 5(1) – Изисква рамка за управление на ИКТ риска, която обхваща всички критични външни доставчици.

11.6.2 Член 5(2) – Предвижда договорни и оперативни контроли за зависимости от ИКТ услуги.

11.6.3 Член 28(1), (2) – Установява правила за надзор върху риска от ИКТ трети страни във финансовия сектор.

11.7 COBIT 2019

11.7.1 APO10 – „Manage Suppliers“ определя контроли при възлагане и очаквания за управление на взаимоотношенията.

11.7.2 APO12 – „Manage Risk“ интегрира риска, свързан с доставчиците, в управлението на организационния риск.

11.7.3 DSS05 – „Manage Security Services“ се прилага за управлявани трети страни и външно възложени доставчици на услуги.