					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P27					Заглавие на документа: **Политика за използване на облачни услуги**							
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	Изисквания за оперативно планиране и контрол при използването на облачни услуги.
ISO/IEC 27002:2022	Контроли 5.23–5.25	Изисквания относно използването, политиката и сигурността на облачните услуги.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Използване на външни системи, договорни и технически изисквания, криптографски мерки за защита, защита на веригата на доставки.
EU GDPR	Членове 28, 32, Глава V	Изисквания към обработващите лични данни в облачна среда, сигурност на обработването, прехвърляне на данни.
EU NIS2	Член 21(2)(f, i)	Изисквания за риска от трети страни и веригата на доставки.
EU DORA	Членове 5(2), 28	Надзор върху ИКТ и трети страни (облачни услуги) за финансови субекти.
COBIT 2019	BAI04, DSS01, DSS05	Наличност на облачните услуги, операции и управление на сигурността.

1. Цел

1.1 Настоящата политика установява задължителните изисквания на организацията за сигурно, съответстващо и отговорно използване на услуги за облачни изчисления в рамките на моделите за предоставяне Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) и Software-as-a-Service (SaaS).

1.2 Политиката има за цел да гарантира, че облачните услуги се внедряват и управляват по начин, който защитава поверителността, целостта и наличността на информационните активи, като същевременно изпълнява регулаторните, правните и договорните задължения.

1.3 Тя определя контроли за управление на риска при използването на облачни услуги, защита на данните, наблюдение на съответствието на доставчиците и предотвратяване на неоторизирано използване. Политиката също така подпомага бизнес иновациите чрез облачни платформи, като съгласува сигурността, оперативната надеждност и разходната ефективност.

2. Обхват

2.1 Настоящата политика се прилага за всички служители, външни изпълнители, външни доставчици на услуги и външни консултанти, които предоставят, конфигурират, достъпват, управляват или използват облачни услуги от името на организацията.

2.2 Тя се прилага за всички среди, в които се обработват данните или работните натоварвания на организацията, включително:

2.2.1 Публични, частни, хибридни и общностни облачни внедрявания

2.2.2 Всички модели на облачни услуги (IaaS, PaaS, SaaS)

2.2.3 Многооблачни и федеративни архитектури

2.2.4 Използване на shadow IT или лични облачни акаунти за служебни цели

2.3 Политиката обхваща всички нива на класификация на данните и се прилага както за вътрешни системи, така и за платформи, хоствани от доставчици, в които се съхраняват или обработват данни, притежавани от организацията или подлежащи на регулаторни изисквания.

3. Цели

3.1 Да осигури сигурно и последователно използване на облачни технологии чрез ясно определени правила за използване, базови конфигурации за сигурност и управленски роли.

3.2 Да сведе до минимум оперативните и регулаторните рискове, свързани с използването на облачни изчисления, включително неоторизиран достъп, нарушения на сигурността на данните, неправилна конфигурация, несъответствие и прекъсване на услугите.

3.3 Да наложи изисквания за сигурност и поверителност към всички доставчици на облачни услуги и да проверява съответствието чрез договорни клаузи, оценки и право на одит.

3.4 Да даде възможност за мащабируемо и устойчиво внедряване на облачни услуги, без компромис със степента на сигурност, правните изисквания или непрекъсваемостта на дейността.

3.5 Да съгласува управлението и използването на облачни услуги с рамката на СУИС на организацията, правните задължения (напр. GDPR, DORA), секторно-специфичните указания и добрите практики в индустрията (напр. NIST, COBIT).

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява Политиката за използване на облачни услуги и стратегическата пътна карта за внедряване на облачни услуги.

4.1.2 Преглежда и одобрява изключенията с висок риск от стандартните изисквания за управление на облачни услуги.

4.1.3 Осигурява облачните инициативи да получават достатъчно финансиране, надзор и интеграция с рамките за управление на корпоративния риск.

4.2 Директор по информационна сигурност (CISO)

4.2.1 Отговаря за настоящата политика и за организационния Регистър на облачните услуги.

4.2.2 Одобрява включването на нови доставчици на облачни услуги въз основа на надлежна проверка и оценка на риска.

4.2.3 Преглежда документацията за съответствие на доставчиците и валидира съгласуваността на мерките за сигурност.

[... 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 бъде преглеждана най-малко веднъж годишно и актуализирана при необходимост, за да се осигури трайно съгласуване със:

9.1.1 Развиващите се правни и регулаторни изисквания (напр. GDPR, NIS2, DORA)

9.1.2 Промените в стандартите ISO/IEC 27001 или ISO/IEC 27002

9.1.3 Актуализациите в облачната архитектура на организацията, пейзажа на заплахите или портфолиото от услуги

9.1.4 Разследвания на инциденти, резултати от одити или извлечени поуки от оперативното използване

9.2 CISO отговаря за иницииране на прегледа и свикването на съответните заинтересовани страни, включително:

9.2.1 Архитект по сигурността на облачни услуги

9.2.2 Екип по правни въпроси и съответствие

9.2.3 Мениджъри по снабдяване и доставчици

9.2.4 Собственици на услуги и ИТ операции

9.3 Всички актуализации трябва да бъдат:

9.3.1 Под управление на версиите и датирани

9.3.2 Одобрени от Изпълнителното ръководство

9.3.3 Комуникирани до засегнатите страни, включително служители, външни изпълнители и трети страни

9.3.4 Архивирани в съответствие с вътрешните политики за документация

9.4 Междинни прегледи могат да бъдат задействани от:

9.4.1 Нови ангажименти с CSP или съществени миграции

9.4.2 Възникващи заплахи за облачната инфраструктура

9.4.3 Съществени промени в договорните, правните или секторно-специфичните задължения

10. Свързани политики и връзки

10.1 Настоящата политика е тясно свързана и зависима от следните вътрешни политики:

10.1.1 P1 – Политика за информационна сигурност: Установява основните принципи за сигурната експлоатация на системи и услуги, които настоящата политика прилага в контекста на облачните услуги.

10.1.2 P5 – Политика за управление на промените: Всички промени в конфигурацията на облачните услуги трябва да следват процедурите за контрол на промените, определени в P5.

10.1.3 P13 – Политика за класификация и етикетиране на данните: Определя как се оценяват данните преди прехвърляне към облака и как се прилагат контроли като криптиране и местонахождение на данните.

10.1.4 P18 – Политика за криптографски контроли: Предоставя стандарти за криптиране, управление на ключове и използване на криптографски алгоритми, пряко приложими при конфигурирането на облачни услуги.

10.1.5 P22 – Политика за регистриране и мониторинг: Определя изискванията за събиране, съхранение и анализ на журнали, които трябва да се прилагат в облачни среди.

10.1.6 P30 – Политика за реагиране при инциденти: Определя процедурите за ескалация, ограничаване и отстраняване при събития по сигурността, свързани с облачни услуги.

10.1.7 P33 – Политика за мониторинг на одита и съответствието: Подпомага готовността за одит и непрекъснатото осигуряване, че контролите за облачни услуги се прилагат и наблюдават.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001: Клауза 8.1 – Оперативно планиране и контрол: Изисква организациите да внедрят и контролират процесите, необходими за изпълнение на изискванията за информационна сигурност, включително тези, свързани с облачни среди.

11.2 ISO/IEC 27002:2022 – Контроли 5.23 до 5.25:

11.2.1 Приложение A, контрол 5.23 – Използване на облачни услуги: Изисква оценка, базирана на риска, формално одобрение и документиране на използването на облачни услуги.

11.2.2 Приложение A, контрол 5.24 – Политика за използване на облачни услуги: Изисква установяване и прилагане на формални политики за използване на облачни услуги, съгласувани с организационните нужди и рискове.

11.2.3 Приложение A, контрол 5.25 – Сигурност при облачни услуги: Налага необходимостта от интеграция на сигурността, договорни защити и мониторинг на работните натоварвания и данните, хоствани в облака.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Използване на външни системи: Изисква определени правила и условия за достъп до организационни ресурси от външни или облачно базирани системи.

11.3.2 SA-9(5) – Услуги на външни информационни системи: Налага договорни изисквания за сигурност, надзор и непрекъснат мониторинг на съответствието за външни облачни системи.

11.3.3 SC-12 до SC-28 – Криптографски мерки за защита, защита на границите и цялост при преноса: Съответстват на изискванията за криптиране, идентичност и достъп за активи, услуги и данни, хоствани в облака и при пренос.

11.3.4 SR-5 – Защита на веригата на доставки: Подпомага проверката и договорния контрол върху CSP, участващи в предоставянето на услугата.

11.4 EU GDPR (2016/679):

11.4.1 Член 28 – Задължения на обработващия лични данни: Изисква формални договори с доставчици на облачни услуги, за да се гарантират сигурността, поверителността и възможността за одит на обработването на лични данни.

11.4.2 Член 32 – Сигурност на обработването: Подпомага прилагането на криптиране, контрол на достъпа, регистриране и други мерки за защита в облачни среди.

11.4.3 Глава V – Международни трансфери на данни: Налага законосъобразно прехвърляне на данни извън ЕС/ЕИП чрез защитни механизми като стандартни договорни клаузи (SCC) или решения за адекватно ниво на защита.

11.5 Директива NIS2 на ЕС (2022/2555):

11.5.1 Член 21(2)(f, i): Изисква организациите да управляват рисковете от външни доставчици на облачни услуги и да осигуряват цялостта на цифровата верига на доставки чрез договорни и технически мерки.

11.6 EU DORA (2022/2554):

11.6.1 Член 5(2) – Управление на ИКТ риска: Изисква интегриране на риска от ИКТ трети страни, включително облачни услуги, в цялостното управление на риска.

11.6.2 Член 28 – Надзор върху критични външни доставчици на ИКТ услуги: Изисква финансовите субекти да наблюдават, контролират и докладват зависимостите от доставчици на облачни услуги, рисковия профил и устойчивостта.

11.7 COBIT 2019:

11.7.1 BAI04 – Управление на наличността и капацитета: Осигурява облачните услуги да бъдат устойчиви, наблюдавани и да отговарят на определените критерии за резултатност.

11.7.2 DSS01 – Управление на операциите: Подпомага оперативната интеграция, обработването на инциденти и базовите конфигурации в платформи, хоствани в облака.

11.7.3 DSS05 – Управление на услугите по сигурност: Насочва внедряването на специфични за облачната среда контроли за сигурност, мониторинг и предотвратяване на инциденти в цифровите услуги.