					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P27S					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**

Съответствие със стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	
ISO/IEC 27002:2022	Контроли 5.23–5.25	
NIST SP 800-53 Rev.5	AC-20, SC-12, SC-13, SR-5	
GDPR на ЕС	Членове 28, 32 и глава V	
NIS2 на ЕС	Член 21(2)(f), (i)	
DORA на ЕС	Членове 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Цел

1.1 Настоящата политика определя условията и начина за сигурно използване на облачни услуги в организацията. Тя гарантира, че данните, обработвани или съхранявани в облачна среда, са защитени, достъпът до тях е контролиран, а рисковете се управляват по подходящ начин.

1.2 Политиката подпомага МСП при изпълнение на законовите задължения и очакванията на клиентите относно защитата на чувствителна информация, предотвратяването на изтичане на данни и ефективното управление на рисковете, свързани с облачните услуги, без необходимост от инфраструктура от мащаба на голямо предприятие.

1.3 Настоящата политика подпомага сертифицирането по ISO/IEC 27001, съответствието с GDPR и доверието по веригата на доставки чрез последователно управление на всички външни облачни услуги.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички облачни услуги, използвани за съхранение, обработване или пренос на фирмени данни

2.1.2 Всички служители, външни изпълнители и доставчици на услуги, които използват облачни инструменти от името на организацията

2.1.3 Безплатни и платени облачни решения, включително платформи за електронна поща, споделяне на документи, SaaS решения, платформи за архивиране, решения за видеоконференции и клиентски платформи

2.1.4 Всички устройства (настолни компютри, мобилни устройства, таблети), чрез които се осъществява достъп до фирмена информация посредством облачни приложения

2.2 Това включва, без да се ограничава до:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Облачни инструменти за архивиране и аварийно възстановяване

2.2.5 Споделени папки или приложения, използвани за фактуриране, управление на проекти или комуникация с клиенти

3. Цели

3.1 Да се предотвратява неоторизираното или високорисково използване на неодобрени облачни услуги.

3.2 Да се гарантира, че чувствителните или регулираните данни, съхранявани в облака, са защитени чрез подходящи технически и административни контроли.

3.3 Да се определят ясни роли за одобряване, конфигуриране, наблюдение и извеждане от експлоатация на облачни услуги.

3.4 Да се контролират потоците от данни и да се прилагат изискванията за съхранение, изтриване и поверителност по отношение на информацията, съхранявана в облака.

3.5 Да се намали зависимостта от лични акаунти или непроследявани инструменти, като се изисква одобрение за всички облачни системи, използвани за служебни цели.

3.6 Да се изпълняват изискванията на ISO/IEC 27001:2022, GDPR, NIS2 и DORA относно управлението на външни зависимости, свързани с облачни услуги.

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява използването на всички нови облачни услуги

4.1.2 Преглежда рисковете, свързани с доставчиците на облачни услуги и видовете услуги

4.1.3 Осигурява прилагането на политиката и упражнява надзор върху решенията за изключения

4.2 Външен доставчик на ИТ услуги или техническа поддръжка

4.2.1 Оценява и внедрява сигурна конфигурация за облачните услуги

4.2.2 Конфигурира акаунти, контроли за достъп и резервни копия

4.2.3 Следи съответствието с изискванията за пароли, MFA и настройки 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

9.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно от Управителя, в координация с външния доставчик на ИТ услуги.

9.2 Официален преглед трябва да се извършва и:

9.2.1 След инцидент по сигурността, свързан с облачни услуги (напр. нарушение или загуба на данни)

9.2.2 При въвеждане на нова съществена облачна платформа

9.2.3 При промяна в правните или регулаторните изисквания (напр. актуализации на GDPR, NIS2, DORA)

9.2.4 Ако дейностите по мониторинг установят неправилна употреба или нови рискове

9.3 Управителят трябва да гарантира, че:

9.3.1 Регистърът на облачните услуги се актуализира с новите услуги и услугите, изведени от употреба

9.3.2 Правните изисквания и изискванията за поверителност продължават да се изпълняват

9.3.3 Всички промени се комуникират на съответните потребители и заинтересовани страни

9.4 Архивните версии трябва да се съхраняват сигурно, а старите версии на политиката да се обработват съгласно P14S – Политика за съхранение на данни и унищожаване на организацията.

10. Свързани политики и зависимости

10.1 Настоящата политика трябва да се прилага съвместно със следните политики по информационна сигурност, съобразени с нуждите на МСП:

10.1.1 P2S – Политика за роли и отговорности в управлението: Определя отговорностите за одобряване на облачни услуги и управление на взаимоотношенията с доставчици.

10.1.2 P4S – Политика за контрол на достъпа: Подпомага сигурното вписване, управлението на сесиите и практиките по отнемане на достъп, изисквани за облачните платформи.

10.1.3 P14S – Политика за съхранение на данни и унищожаване: Определя как данните в облачна среда се архивират, съхраняват и изтриват в съответствие със законовите задължения.

10.1.4 P17S – Политика за защита на данните и поверителност: Гарантира, че всички лични данни, съхранявани в облачни услуги, се обработват в съответствие с принципите на GDPR.

10.1.5 P30S – Политика за реагиране при инциденти: Осигурява структурирани процедури за реагиране при инциденти по сигурността, свързани с облачни услуги, включително събиране на доказателства и външно уведомяване.

10.2 Заедно тези политики гарантират, че използването на облачни услуги е сигурно, съответства на приложимите изисквания и е оперативно устойчиво.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква организациите да внедрят оперативни контроли за обработване на данни, включително контроли, свързани с облачни системи.

11.2 ISO/IEC 27002

11.2.1 Контрол 5.23 – Изисква управление на използването на облачни услуги и SaaS решения от трети страни.

11.2.2 Контрол 5.24 – Изисква определена политика за използване на облачни услуги, съобразена с риска и регулаторните изисквания.

11.2.3 Контрол 5.25 – Изисква организациите да гарантират, че контролите за сигурност в облачни среди отговарят на организационните потребности.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-20 – Изисква официални политики за използване на външни системи, включително облачни услуги.

11.3.2 SC-12, SC-13 – Обхващат криптирането на данни при пренос и на данни в покой в облачни среди.

11.3.3 SR-5 – Обхваща контролите за риск, свързани с облачни услуги и трети страни по веригата на доставки.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 28 – Изисква доставчиците на облачни услуги, действащи като обработващи лични данни, да спазват обвързващи договорни задължения.

11.4.2 Член 32 – Изисква технически и организационни мерки за обработване на данни в облачна среда.

11.4.3 Глава V – Забранява неоторизирани международни трансфери на лични данни, съхранявани в облака.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(f), (i) – Изисква съществени и важни субекти да прилагат подходящи политики за сигурност на облачните услуги и контрол по веригата на доставки.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 5(2) – Изисква финансовите МСП да интегрират сигурността на облачните услуги в своите рамки за управление на риска, свързан с ИКТ.

11.6.2 Член 28 – Установява правила за надзор върху критични външни доставчици на ИКТ услуги, включително доставчици на облачни услуги.

11.7 COBIT 2019

11.7.1 DSS01 – „Управление на операциите“ разглежда оперативната цялост на облачните услуги.

11.7.2 DSS05 – „Управление на услугите по сигурност“ включва специфични за облака мерки за защита и мониторинг.

11.7.3 BAI04 – „Управление на наличността и капацитета“ осигурява непрекъсваемост на дейността и производителност в облачни среди.