					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P15S					Заглавие на документа: **Политика за резервни копия и възстановяване**							
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	Контроли за резервни копия съгласно изискванията на СУИС
ISO/IEC 27002:2022	Контроли 5.29, 8.13	Добри практики за резервни копия и интеграция с управлението на непрекъсваемостта на дейността
NIST SP 800-53 Rev. 5	CP-9, MP-6	Резервни копия и защита на носителите
EC NIS2	Член 21(2)(c)	Устойчивост и непрекъсваемост чрез резервни копия
EC DORA	Член 10(1)	Непрекъсваемост на ИКТ – резервни копия за организации от финансовия сектор
COBIT 2019	BAI04.05, DSS04	Документиране и тестване на резервни копия, контрол на процесите
GDPR на ЕС	Членове 5(1)(f), 32(1)(c)	Цялостност, наличност и своевременно възстановяване на данни

1. Цел

1.1 Настоящата политика определя как организацията изпълнява и управлява резервните копия, за да осигури непрекъсваемост на дейността, да предпази от загуба на данни и да позволи своевременно възстановяване след инциденти.

1.2 Тя установява задължителни правила за архивиране, съхранение и възстановяване на системи и данни, особено в МСП без сложна ИТ инфраструктура.

1.3 Настоящата политика подпомага готовността за одит и сертифициране по ISO/IEC 27001, като гарантира, че основните контроли за резервни копия са въведени, прилагат се последователно и се преглеждат редовно.

1.4 Способността на организацията да се възстановява след технически откази, случайно изтриване или киберинциденти зависи от стриктното спазване на тази политика.

2. Обхват

2.1 Настоящата политика се прилага за всички бизнес системи и данни, включително:

2.1.1 Финансови записи, клиентска информация и данни на Човешки ресурси (ЧР)

2.1.2 Настолни компютри, лаптопи, сървъри и облачни приложения, използвани в дейността

2.1.3 Носители за резервни копия, като USB устройства, външни носители за съхранение или облачно базирани резервни копия

2.2 Тя се прилага и за всички лица, които отговарят за изпълнението или управлението на процесите по архивиране, включително:

2.2.1 Управителят (GM) или определено отговорно лице

2.2.2 Външни доставчици на ИТ поддръжка или консултанти

2.2.3 Всички служители, отговорни за записването на данни в одобрени местоположения

3. Цели

3.1 Да се гарантира, че всички критични бизнес данни и системи се архивират сигурно на подходящи интервали, определени според риска и оперативната необходимост.

3.2 Да се гарантира, че данните могат да бъдат възстановени своевременно и в пълен обем след прекъсвания.

3.3 Да се предотвратят неоторизиран достъп, манипулиране или загуба на данни от резервни копия чрез ефективни контроли за съхранение.

3.4 Да се определят ясно и да се прилагат роли и отговорности за внедряване и тестване на процедурите по архивиране.

3.5 Да се подпомогне съответствието с ISO/IEC 27001, GDPR и други регулаторни изисквания чрез структурирани и документирани практики за резервни копия.

4. Роли и отговорности

4.1 Управителят (GM)

4.1.1 Одобрява настоящата политика и осигурява нейното прилагане

4.1.2 Осигурява ресурси и определя отговорностите за дейностите по архивиране и възстановяване

4.1.3 Преглежда неуспешни архивирания, инциденти или отклонения от политиката

4.1.4 Ръководи годишните прегледи на политиката и осигурява готовност за одит

4.2 Външен доставчик на ИТ поддръжка (ако е приложимо)

4.2.1 Внедрява и управлява решения за архивиране (локални или облачно базирани)

4.2.2 Наблюдава успешното изпълнение на архивирането и планира тестове за възстановяване

4.2.3 Докладва неуспешни архивирания и инциденти директно на Управителя (GM)

4.2.4 Осигурява криптиране, ограничения на достъпа и правилно боравене с носителите за резервни копия

[... 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 поне веднъж годишно от Управителя (GM). Основанията за междинен преглед включват:

9.1.1 Съществени промени в системите или методите за съхранение

9.1.2 Въвеждане на нови облачни или ИТ платформи

9.1.3 Правни или регулаторни промени, засягащи възстановяването на данни

9.1.4 Констатации от одити или инциденти

9.2 Управителят (GM) отговаря за иницииране на прегледа, одобряването на промените и комуникирането на актуализациите.

9.3 Версиите на политиката трябва да се проследяват и архивират. Заменените версии трябва да бъдат с ограничен достъп, за да се избегне объркване по време на одити или събития по възстановяване на дейността.

10. Свързани политики и връзки

10.1 Настоящата политика е съгласувана със следните SME политики и зависи от тях:

10.1.1 P14S – Политика за съхранение и унищожаване на данни: Определя колко дълго данните от резервни копия трябва да се съхраняват и как да бъдат сигурно изтрити.

10.1.2 P13S – Политика за класификация и етикетиране на данни: Подпомага определянето на приоритета на данните, които трябва да бъдат архивирани, според нивата на класификация.

10.1.3 P30S – Политика за реагиране при инциденти: Обхваща процедурите при неуспешно архивиране или когато е необходимо възстановяване на данни след нарушение или прекъсване.

10.1.4 P2S – Политика за роли и отговорности в управлението: Определя ясни правомощия за надзор върху резервните копия и прилагане на политиката.

10.1.5 P17S – Политика за защита на данните и поверителност: Осигурява обработването на лични данни при резервни копия да е в съответствие с правните изисквания и изискванията за поверителност.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1: Оперативно планиране и контрол на системите за резервни копия като част от СУИС

11.2 ISO/IEC 27002

11.2.1 Контрол 8.13: Определя добри практики за планиране, наблюдение и възстановяване на резервни копия

11.2.2 Приложение A, Контрол 5.29: Интеграция на резервните копия с непрекъсваемостта на дейността и готовността за възстановяване

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (Планиране при извънредни обстоятелства): Определя структурирани стратегии за резервни копия за устойчивост на дейността

11.3.2 MP-6 (Защита на носителите): Изисква сигурно боравене и унищожаване на носители за резервни копия

11.4 GDPR на ЕС

11.4.1 Член 5(1)(f): Изисква цялостност и наличност на личните данни

11.4.2 Член 32(1)(c): Изисква възможност за своевременно възстановяване на достъпа до лични данни

11.5 Директива ЕС NIS2

11.5.1 Член 21(2)(c): Изисква резервни копия и възстановяване като част от планирането за устойчивост и непрекъсваемост

11.6 ЕС DORA

11.6.1 Член 10(1): Организациите от финансовия сектор трябва да осигурят резервни копия като част от мерките за непрекъсваемост на ИКТ

11.7 COBIT 2019

11.7.1 BAI04.05: Изисква документирани стратегии за резервни копия

11.7.2 DSS04.07: Подчертава рутинното тестване и контрола върху процесите по архивиране и възстановяване на данни