					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P15					Заглавие на документа: **Политика за архивиране 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**

Съгласуваност с приложимите стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1.3, 8.	Третиране на риска, планиране и оперативни контроли за архивиране
ISO/IEC 27002:2022	Контроли 8.13, 5.28, 5.	Управление на архивирането, сигурно унищожаване
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Изисквания за архивиране на системи, възстановяване и сигурно изчистване на носители
GDPR на ЕС	Член 32, Съображение 49	Възстановяване и наличност на лични данни, непрекъсваемост на дейността
NIS2 на ЕС	Член 21(2)(c-e)	Контроли за архивиране и непрекъсваемост в подкрепа на устойчивостта
DORA на ЕС	Членове 10, 11	Изисквания за архивиране, възстановяване и тестване във финансовия сектор
COBIT 2019	DSS01, DSS04, MEA	Операции по архивиране, непрекъсваемост и наблюдение на съответствието

1. Цел

1.1 Целта на тази политика е да определи задължителните изисквания за архивиране и възстановяване на данни, системи и приложения с цел подпомагане на оперативната устойчивост, целостта на данните и непрекъсваемостта на дейността.

1.2 Политиката установява стандартизирана рамка за:

1.2.1 Защита на организационните данни от загуба вследствие на изтриване, повреда, отказ или кибератаки

1.2.2 Определяне на очакванията за възстановяване чрез ясни параметри RTO (Recovery Time Objective) и RPO (Recovery Point Objective)

1.2.3 Интегриране на операциите по архивиране в по-широката рамка на СУИС и плановете за непрекъсваемост на дейността (BCP/DRP)

1.2.4 Осигуряване на съответствие с приложимите закони и секторни регулации относно наличността и възстановимостта

1.3 Политиката въвежда контроли по ISO/IEC 27001:2022, свързани със сигурното унищожаване на данни (5.28), устойчивостта (5.29) и оперативното възстановяване (8.13), и е съгласувана с добрите практики по ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA и NIS2.

2. Обхват

2.1 Тази политика се прилага за:

2.1.1 Всички критични за бизнеса и оперативни системи в обхвата на СУИС

2.1.2 Всички структурирани и неструктурирани служебни данни, включително бази данни, файлове, електронна поща и конфигурации

2.1.3 Всички среди — локални, облачни, хибридни и отдалечени/външни среди за съхранение

2.1.4 Всички лица, отговорни за управлението, изпълнението, проверката или възстановяването на процесите по архивиране

2.2 Политиката се прилага също за:

2.2.1 Носителите и инфраструктурата за архивиране, включително физически ленти, виртуални устройства, моментни снимки на дискове и облачни решения за архивиране

2.2.2 Външни доставчици на услуги, ангажирани да хостват, управляват или обработват архивите на организацията

2.2.3 Архивиране на журнали, конфигурации, одитна следа и оперативна документация, критични за непрекъсваемостта

2.3 Системите, изрично изключени от архивиране, трябва да бъдат документирани, за тях да е извършена оценка на риска и да бъдат формално одобрени от мениджъра на СУИС и собственика на системата.

3. Цели

3.1 Да се гарантира, че всички критични системи и данни се архивират надеждно с достатъчна честота, резервираност и мерки за сигурност.

3.2 Да се осигурят механизми за възстановяване, които отговарят на определените цели за RTO и RPO в съответствие с анализите на въздействието върху бизнеса.

3.3 Да се поддържа пълна документация на процедурите за архивиране, сроковете за съхранение, ролите и използваните технологии.

3.4 Да се валидира ефективността на контролите при операциите по архивиране чрез систематично тестване на възстановяването, регистриране на откази и проследяване на коригиращите действия.

3.5 Да се защитават архивните данни от неоторизиран достъп, промяна или унищожаване през целия им жизнен цикъл.

3.6 Да се осигури съответствие с:

3.6.1 Изискванията за оперативни контроли и контроли за непрекъсваемост по ISO/IEC 27001

3.6.2 Семействата CP и MP в NIST SP 800-53 за архивиране и сигурно изчистване

3.6.3 Член 32 и Съображение 49 от GDPR относно възстановяването на достъпа до лични данни

3.6.4 Член 10 от DORA и член 21 от NIS2 относно непрекъсваемостта и устойчивостта на ИКТ

3.7 Да се гарантира, че външните услуги за архивиране изпълняват договорните и регулаторните задължения по сигурност, включително по отношение на криптиране, унищожаване и протоколи за уведомяване.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява тази политика и гарантира, че критичните за бизнеса системи са адекватно защитени чрез одобрени практики за архивиране и възстановяване.

4.1.2 Носи отговорност за осигуряването на достатъчни ресурси за операциите по архивиране и за периодичния им преглед за регулаторно съответствие.

4.2 Директор по информационна сигурност (CISO)

4.2.1 Отговаря за тази политика и осигурява съгласуваността ѝ с по-широките рамки за информационна сигурност, управление на риска и непрекъсваемост на дейността.

4.2.2 Наблюдава интегрирането на процедурите за архивиране в BCP/DRP, реагирането при инциденти и планирането на устойчивостта.

4.2.3 Преглежда изключенията от архивиране и оценява предложенията за приемане на риск при изключване на критични системи.

[... 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 Тази политика трябва да се преглежда най-малко веднъж годишно или по-рано, ако е задействана от:

9.1.1 Промени в стратегията за непрекъсваемост на дейността или аварийно възстановяване

9.1.2 Нови регулаторни или правни задължения, които влияят върху честотата на архивиране или срока за съхранение на данни

9.1.3 Промени в архитектурата на системите, инструментите за архивиране или доставчиците на услуги

9.1.4 Значими инциденти или одитни констатации, свързани със загуба на данни или откази при възстановяване

9.2 Прегледът трябва да бъде координиран от CISO в сътрудничество с:

9.2.1 ИТ инфраструктура и операции

9.2.2 Вътрешен одит

9.2.3 Длъжностното лице по защита на данните (DPO)

9.2.4 Екипите по непрекъсваемост на дейността и аварийно възстановяване

9.3 Графиците за архивиране, списъците на включените системи, документацията за възстановяване и журналите за изключения трябва да се преглеждат паралелно, за да се гарантира:

9.3.1 Точност на обхвата на архивиране за всички критични активи

9.3.2 Съответствие с изискванията за RTO/RPO и срок на съхранение

9.3.3 Пълнота на журналите от тестове и докладите за инциденти

9.3.4 Отстраняване на предходно установени пропуски в контролите

9.4 Всички актуализации трябва:

9.4.1 Да бъдат под управление на версиите и съхранявани в хранилището за документация на СУИС

9.4.2 Да включват обобщение на промените и обосновка

9.4.3 Да бъдат одобрени от Изпълнителното ръководство

9.4.4 Да бъдат комуникирани до всички засегнати технически и бизнес служители

10. Свързани политики и връзки

10.1 Тази политика пряко подпомага и взаимодейства със следните свързани документи:

10.1.1 P6 - Политика за управление на риска: Определя приоритизацията, базирана на риска, за защитата на архивите на системи и услуги.

10.1.2 P12 - Политика за управление на активите: Гарантира, че системите, подлежащи на архивиране, са включени в инвентара и обвързани с проследяване по жизнения цикъл и класификация.

10.1.3 P13 - Политика за класификация и етикетиране на данни: Определя кои категории данни изискват архивиране, включително етикетиране на метаданни за приоритизация.

10.1.4 P14 - Политика за съхранение и унищожаване на данни: Координира срока за съхранение на архивите с регулаторните ограничения за съхранение и правилното унищожаване на носители с изтекъл срок.

10.1.5 P16 - Политика за маскиране на данни и псевдонимизация: Подпомага минимизирането на данните при архивиране на чувствителни набори от данни.

10.1.6 P30 - Политика за реагиране при инциденти: Активира се при откази на архивиране, проблеми с възстановяването или компрометиране на хранилища за архивни данни.

10.2 Тези взаимосвързани политики формират цялостна рамка, която гарантира, че управлението на архивирането е вградено в по-широката стратегия на организацията за СУИС и оперативна устойчивост.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:

11.1.1 Клауза 6.1.3 - План за третиране на риска: Подпомага приоритизацията на архивирането и планирането на възстановяването, базирани на риска.

11.1.2 Клауза 8.1 - Оперативно планиране и контрол: Интегрира контролите за възстановяване и непрекъсваемост като част от оперативните мерки за сигурност.

11.1.3 Приложение A, Контрол 5.28 - Сигурно унищожаване или повторна употреба на оборудване: Отнася се до сигурното изчистване на архивни носители.

11.1.4 Приложение A, Контрол 5.29 - Информационна сигурност по време на прекъсване: Осигурява възможности за възстановяване по време на инциденти или бедствия.

11.1.5 Приложение A, Контрол 8.13 - Архивиране на информация: Пряко се адресира чрез планирани, тествани и защитени операции по архивиране.

11.2 ISO/IEC 27002:2022 - Контроли 8.13, 5.28, 5.: Тези контроли затвърждават изискването за редовно архивиране, валидиране на целостта и планиране на възстановяването във всички ИТ среди.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Архивиране на системи: Установява цялостни процедури за архивиране, включително съхранение извън обекта и тестване на възстановяването.

11.3.2 CP-10 - Възстановяване и реституиране на системи: Изисква валидирани процедури за пълно или частично възстановяване, съобразени с целите за възстановяване.

11.3.3 MP-6 - Изчистване на носители: Осигурява сигурно обработване на изведени от употреба архивни носители.

11.3.4 SI-12 - Процедури за обработване на информация: Подсилва отговорностите по архивиране и възстановяване за чувствителни данни.

11.4 GDPR на ЕС (2016/679):

11.4.1 Член 32 - Сигурност на обработването: Изисква възможности за възстановяване и мерки за гарантиране на наличността на данните, особено на личните данни.

11.4.2 Съображение 49: Подкрепя мерките за непрекъсваемост на дейността и аварийно възстановяване, включително сигурно архивиране като част от организационната устойчивост.

11.5 Директива NIS2 на ЕС (2022/2555):

11.5.1 Член 21(2)(c-e): Изисква технически и организационни мерки, включително контроли за архивиране и непрекъсваемост, за осигуряване на устойчивост на услугите.

11.6 DORA на ЕС (2022/2554):

11.6.1 Член 10 - Непрекъсваемост на ИКТ дейността: Изисква финансовите субекти да разполагат с цялостно архивиране на данни, възстановяване и планиране на непрекъсваемостта.

11.6.2 Член 11 - Тестване на плановете за непрекъсваемост на ИКТ дейността: Подчертава валидирането на способността за възстановяване чрез редовно тестване.

11.7 COBIT 2019:

11.7.1 DSS01 - Управлявани операции: Подпомага надеждното предоставяне на услуги чрез защитена наличност на данните.

11.7.2 DSS04 - Управлявана непрекъсваемост: Определя стратегически и оперативни контроли за непрекъсваемост, включително проверени архиви.

11.7.3 MEA03 - Мониторинг, оценяване и преценка на съответствието: Изисква периодичен преглед на мерките за непрекъсваемост, включително ефективността на контролите за архивиране.