					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P05					Заглавие на документа: **Политика за управление на промените**							
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	Клаузи 6.1, 5.	Обхваща действия по третиране на риска, контрол на достъпа и управление на промените
ISO/IEC 27002:2022	Контрол 8.	Прилага структуриран процес за управление на промените
NIST SP 800-53 Rev.5	CM-2 до CM-14	Контроли за управление на конфигурацията
EU GDPR	Членове 32(1)(b–d), 25; Съображение 78	Технически и организационни мерки за сигурността на системите и данните по време на промени
EU NIS2	Член 21(2)(a, b, d, e)	Изисква управление на риска при промени в ИКТ
EU DORA	Членове 5, 8, 12	Регламентира оперативния и ИКТ риска, както и докладването на инциденти
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA	Структурирани изисквания за ефективност, съответствие и управление на ИТ промените

1. Цел

1.1. Настоящата политика установява формална рамка за иницииране, оценяване, одобряване, внедряване и преглед на промени в информационните системи, инфраструктурата, приложенията и свързаните с тях процеси на организацията.

1.2. Тя гарантира, че всички промени се изпълняват по контролиран начин и с възможност за одит, като се свежда до минимум рискът от прекъсване, компрометиране на сигурността или регулаторно несъответствие.

1.3. Тя подпомага ISO/IEC 27001:2022, Приложение A, Контрол 8.32 чрез прилагане на сигурни, документирани и съобразени с риска практики за управление на промените.

1.4. Политиката също така осигурява проследимост на решенията, свързани с промените, и подпомага оперативната устойчивост при планирани или аварийни промени.

2. Обхват

2.1. Настоящата политика се прилага за всички промени, засягащи системи, данни и среди в рамките на обхвата на СУИС, включително:

2.1.1. ИТ инфраструктура (локална, облачна, хибридна)

2.1.2. Продукционни, предпродукционни и среди за аварийно възстановяване

2.1.3. Бизнес приложения, услуги, програмни интерфейси на приложения (API) и интеграции

2.1.4. Конфигурационни настройки, прилагане на корекции, софтуерни издания и миграции на системи

2.1.5. Аварийни корекции и проектни или планирани промени

2.2. Тя урежда промените, инициирани от:

2.2.1. Вътрешен персонал (ИТ операции, разработчици, собственици на системи)

2.2.2. Външни доставчици, доставчици на управлявани услуги (MSP) и външни изпълнители

2.2.3. Проектни екипи по време на внедряване на системи, надграждания или преходи на услуги

2.3. Настоящата политика не се прилага за:

2.3.1. временни тестови и развойни среди без достъп до продукционни данни

2.3.2. лични потребителски конфигурации (уредени в Политиката за допустима употреба)

2.3.3. промени по системи извън границите на контрол на организацията, освен ако засягат интегрирани активи или задължения по съответствие

3. Цели

3.1. Да се гарантира, че всички промени се преглеждат, одобряват, тестват и документират преди изпълнение.

3.2. Да се поддържат наличността на системите, цялостта на данните и непрекъсваемостта на услугите по време на и след дейностите по промяна.

3.3. Да се изискват определени класификации на промените, планове за връщане към предходно състояние и оценки на риска за всички видове промени.

3.4. Да се осигури прозрачно вземане на решения и ескалация чрез структурирано управление.

3.5. Да се подпомогне готовността за одит чрез проследими записи за промените и прегледи след внедряване.

3.6. Да се прилага разделение на задълженията и да се намалява рискът от неоторизирани или конфликтни промени в критични системи.

4. Роли и отговорности

4.1. Висше ръководство

4.1.1. Утвърждава Политиката за управление на промените и осигурява съгласуваност със стратегическите цели и регулаторните задължения.

4.1.2. Одобрява програми за промени с високо въздействие или с междудепартаментен обхват като част от управленския надзор.

4.1.3. Осигурява необходимите ресурси и бюджет за инструменти за контрол на промените и обучение на персонала.

4.2. Консултативен съвет по промените

4.2.1. Преглежда и одобрява стандартни и съществени промени, като гарантира подходяща оценка на риска, въздействието и зависимостите.

4.2.2. Валидира плановете за връщане към предходно състояние, резултатите от тестове, комуникацията със заинтересованите страни и графиците.

4.2.3. Състои се от собственици на системи, представители на информационната сигурност, ИТ операции, бизнес ръководители и представители по съответствието.

4.2.4. Може да делегира решения за промени с нисък риск или аварийни промени при документирани условия.

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

9. Преглед и актуализиране

9.1. Основания и периодичност за преглед

9.1.1. Настоящата политика трябва да се преглежда ежегодно или при:

9.1.1.1. Съществени промени в ИТ средата или инфраструктурата

9.1.1.2. Значими инциденти, свързани с неуспешни или неоторизирани промени

9.1.1.3. Регулаторни промени или нови правни задължения, свързани с промените

9.1.1.4. Внедряване на нови инструменти или платформи за управление на промените

9.2. Процес за преглед на Политиката за управление на промените

9.2.1. Мениджърът по промените ръководи процеса по преглед в сътрудничество с:

9.2.1.1. ИТ, сигурност и операции

9.2.1.2. Вътрешен одит и управление на риска

9.2.1.3. Представители на Консултативния съвет по промените

9.2.2. Актуализациите трябва да бъдат прегледани и одобрени от Висшето ръководство и Ръководния комитет на СУИС.

9.2.3. Преиздадените версии трябва да се проследяват в Регистъра на документите и да се комуникират на засегнатите страни, с повторно потвърждение при необходимост.

9.3. Контрол на документи и управление на версиите

9.3.1. Всички версии трябва да включват:

9.3.1.1. Идентификатор на политиката, заглавие и ниво на класификация

9.3.1.2. Собственик и хронология на промените

9.3.1.3. Регистър на промените и дата на влизане в сила

9.3.1.4. Орган по одобрение

9.3.2. Архивираните версии трябва да се съхраняват в съответствие с Политиката за съхранение на документи (минимум 3 години).

10. Свързани политики и взаимовръзки

10.1. Настоящата политика е пряко свързана със следните политики и подпомага тяхното прилагане:

10.1.1. P1 – Политика за информационна сигурност: Установява изискването за формални контроли за сигурност и отговорности на ниво процес, включително управление на промените.

10.1.2. P2 – Политика за роли и отговорности в управлението: Определя правомощията за одобрение и разделението на задълженията, свързани с разрешаването и надзора на промените.

10.1.3. P4 – Политика за контрол на достъпа: Гарантира, че разрешенията за достъп на лицата, които внедряват и преглеждат промени, следват принципа на минимално необходимите привилегии.

10.1.4. P6 – Политика за управление на риска: Осигурява всички промени да подлежат на подходяща оценка на риска и стратегии за смекчаване.

10.1.5. P33 – Политика за мониторинг на одита и съответствието: Регламентира валидирането и одитния преглед на записите и нарушенията, свързани с управлението на промените.

10.2. Тези политики съвместно осигуряват защитим, проследим и сигурен жизнен цикъл на управление на промените в рамките на СУИС.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001:2022

11.1.1. Клауза 6.1 – Действия за адресиране на рискове и възможности: Настоящата политика подпомага идентифицирането, оценяването и контрола на рисковете, свързани с промените.

11.1.2. Клауза 5.15 – Контрол на достъпа: Осигурява достъпът по време на промени да бъде контролиран и проследим.

11.1.3. Приложение A, Контрол 8.32 – Управление на промените: Настоящата политика изцяло прилага изискването за управление на промените в съоръженията и системите за обработка на информация по планиран и контролиран начин.

11.2. ISO/IEC 27002:2022 – Контрол 8

11.2.1. Подсилва прилагането на структуриран процес за управление на промените, включително класификация на промените, одобрение, тестване, връщане към предходно състояние и документиране.

11.3. NIST SP 800-53 Rev.5

11.3.1. Семейство CM (CM-1 до CM-14): Настоящата политика е тясно съгласувана с контролите за управление на конфигурацията, включително базови конфигурации (CM-2), контрол на промените в конфигурацията (CM-3), анализ на въздействието върху сигурността (CM-4) и ограничения на достъпа (CM-5).

11.3.2. Семейство AU (AU-2, AU-6, AU-12): Механизмите за регистриране и одит, посочени в настоящата политика, подпомагат проследимостта на събитията и прегледа на съответствието за дейности, свързани с промени.

11.3.3. RA-3, RA-5: Оценките на риска, обусловени от промените, и сканиранията за уязвимости са вградени в процеса по оценка на промените.

11.3.4. PM-11 (Определяне на мисията/бизнес процесите): Осигурява непрекъсваемостта на бизнеса и оперативните цели да бъдат запазени по време на промените.

11.4. EU GDPR (2016/679)

11.4.1. Член 32(1)(b–d): Настоящата политика подпомага изискването за подходящи технически и организационни мерки за гарантиране на сигурността на данните, особено по време на системни промени.

11.4.2. Член 25 – Защита на данните на етапа на проектиране и по подразбиране: Осигурява промените, засягащи лични данни, да интегрират защита на личните данни и сигурност в проектирането и внедряването.

11.4.3. Съображение 78: Изисква администраторите на данни да прилагат механизми, като политики за контрол на промените, за осигуряване на постоянна поверителност, цялостност и устойчивост на системите за обработване.

11.5. Директива NIS2 на ЕС (2022/2555)

11.5.1. Член 21(2)(a, b, d, e): Изисква технически и организационни мерки за управление на ИКТ рисковете, включително тези, произтичащи от системни промени, актуализации на софтуер и промени по инфраструктурата.

11.6. EU DORA (2022/2554)

11.6.1. Член 5 – Рамка за управление и вътрешен контрол: Настоящата политика прилага принципи за управление на оперативния риск, свързан с промени и актуализации в ИКТ.

11.6.2. Член 8 – Рамка за управление на ИКТ риска: Изисква финансовите субекти да управляват всички промени, засягащи ИКТ системите, чрез структурирани процеси за управление на промените, отразени в изискванията на настоящата политика за класификация, тестване, връщане към предходно състояние и документиране.

11.6.3. Член 12 – Докладване на инциденти: Осигурява неуспешните промени, водещи до прекъсвания в ИКТ, да бъдат проследими, документирани и докладвани, когато е приложимо.

11.7. COBIT 2019

11.7.1. BAI06 – Управлявани ИТ промени: Настоящата политика пряко изпълнява целите на BAI06 чрез установяване на структурирани работни потоци за одобрение на промени, оценка на въздействието, комуникация и тестване.

11.7.2. BAI02 – Управлявано дефиниране на изискванията и BAI03 – Управлявана идентификация и разработване на решения: Осигуряват промените, продиктувани от бизнеса, да бъдат преглеждани и внедрявани по сигурен начин.

11.7.3. DSS01 – Управлявани операции: Подпомага текущата цялостност на системите по време на изпълнение на промените.

11.7.4. MEA01 и MEA03 – Мониторинг, оценяване и преценка на резултатността и съответствието: Осигурява непрекъснат надзор върху ефективността и прилагането на политиката за управление на промените.