					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P05S					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**

Съответствие със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 6.1, 8	
ISO/IEC 27002:2022	Контрол 8	
NIST SP 800-53 Rev. 5	CM-2 до CM-5, CM-11	
EC NIS2	Член 21(2)(b)	
EC DORA	Членове 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Цел

1.1 Настоящата политика гарантира, че всички промени в ИТ системи, конфигурации, бизнес приложения или облачни услуги се планират, оценяват по отношение на риска, тестват и одобряват преди внедряване.

1.2 Целта е да се намалят оперативните прекъсвания, рисковете за сигурността и прекъсванията на услугите чрез въвеждане на опростен, но задължителен процес, приложим и за малки предприятия с ограничени ресурси.

1.3 Настоящата политика подпомага сертифицирането по ISO/IEC 27001:2022, като формализира начина, по който се управляват и документират техническите и оперативните промени.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 служители и ръководители на отдели, които инициират или изпълняват промени

2.1.2 външни доставчици на ИТ услуги, които управляват системи или софтуер

2.1.3 управителя, който носи цялостна отговорност за одобряването на промените

2.2 Политиката обхваща промени в:

2.2.1 софтуер (актуализации, корекции, нови приложения)

2.2.2 хардуер (подмяна, надграждане)

2.2.3 мрежови конфигурации и конфигурации на защитни стени

2.2.4 облачни услуги, права за достъп на потребители или интеграции с доставчици

2.2.5 критични промени в бизнес процеси, включващи информационни системи

2.3 В обхвата на тази политика попадат както планирани, така и аварийни промени.

3. Цели

3.1 Да се гарантира, че всички промени в ИТ и бизнес системи са разрешени, документирани и обратими при възникване на проблеми.

3.2 Да се предотвратят непланирани прекъсвания, загуба на данни или инциденти по сигурността, причинени от неконтролирани промени.

3.3 Да се определят опростени и повтаряеми процедури за заявяване, одобряване, тестване и връщане назад на промени.

3.4 Да се поддържа подлежащ на одит регистър на промените, който подпомага оперативната отчетност и съответствието с регулаторните изисквания.

3.5 Да се осигури вземане на решения въз основа на риска при съществени или чувствителни промени.

4. Роли и отговорности

4.1 Управител

4.1.1 Носи крайна отговорност за всички съществени промени.

4.1.2 Преглежда и одобрява нерутинни, критични или високорискови промени.

4.1.3 Преглежда регистъра на промените на тримесечна база или след значими инциденти.

4.2 ИТ поддръжка или външен доставчик на ИТ услуги

4.2.1 Изпълнява промени, включително актуализиране на конфигурации, прилагане на корекции и миграции на системи.

4.2.2 Поддържа основен регистър на промените, в който се записват датите, видовете промени, резултатите и одобряващите лица.

4.2.3 Тества промените преди внедряване и при необходимост прилага стъпки за връщане назад.

4.2.4 Уведомява засегнатите потребители преди и след съществени промени.

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

9. Изисквания за преглед и актуализиране

9.1 Годишен преглед

9.1.1 Настоящата политика трябва да се преглежда ежегодно от управителя или определено ИТ лице за контакт, за да се гарантира съответствие с текущите системи, работни процеси и регулаторни изисквания.

9.2 Междинни прегледи

9.2.1 Преглед трябва да се инициира и при:

9.2.1.1 инциденти по сигурността, причинени от неефективно управление на промените

9.2.1.2 внедряване на нови ИТ системи

9.2.1.3 промени в приложими стандарти като ISO, NIS2 или DORA

9.3 Документиране на актуализациите

9.3.1 Промените в тази политика трябва да бъдат версионирани и одобрени от управителя. За всяка версия трябва да се записват датата, обобщение на промените и одобряващото лице.

9.4 Комуникиране на политиката

9.4.1 Всички актуализации трябва да бъдат съобщавани на всички засегнати служители и външни доставчици. Документацията трябва да бъде актуализирана на всички места, където се поддържа като референтен документ (напр. портал за служители, споделени хранилища).

10. Свързани политики и връзки

10.1 Настоящата политика е тясно свързана със следните политики за МСП:

10.1.1 P2S – Политика за роли и отговорности по управлението: определя правомощията за одобряване на промени.

10.1.2 P4S – Политика за контрол на достъпа: гарантира, че промените в правата за достъп, произтичащи от промени, са документирани и внедрени правилно.

10.1.3 P7S – Политика за назначаване и освобождаване: координира промени, свързани със смяна на роли и предоставяне на достъп.

10.1.4 P15S – Политика за архивиране и възстановяване: гарантира, че могат да бъдат изпълнени стъпки за връщане назад и възстановяване, ако дадена промяна е неуспешна.

10.1.5 P30S – Политика за реагиране при инциденти: урежда начина, по който неуспешни или неразрешени промени се третират като инциденти по сигурността.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.1 – Планирането въз основа на риска трябва да включва дейностите по промени.

11.1.2 Клауза 8.1 – Оперативните контроли трябва да се прилагат последователно за дейностите, свързани с промени, за да се гарантира цялостта на услугите.

11.2 ISO/IEC 27002

11.2.1 Контрол 8.32 – Предоставя насоки за процеси по сигурно управление на промените, включително документиране, тестване и одобряване.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Базова конфигурация на системите преди промяна.

11.3.2 CM-3 – Контрол на промените в конфигурацията.

11.3.3 CM-4 – Анализ на въздействието върху сигурността.

11.3.4 CM-5 – Одобряване и документиране на промени.

11.3.5 CM-11 – Одит и наблюдение на промените.

11.4 Директива ЕС NIS2

11.4.1 Член 21(2)(b) – Изисква формални процедури за технически и организационни мерки за сигурност, включително управление на промените.

11.5 ЕС DORA

11.5.1 Членове 6(9) и 8(4)(b) – Изискват финансовите субекти да поддържат управление на промените и конфигурациите на ИКТ системите.

11.6 COBIT 2019

11.6.1 BAI06 – Управление на промените: подчертава планирането, оценката на риска и възможностите за връщане назад.

11.6.2 DSS01 – Управление на операциите: гарантира оперативната цялост по време на технически преходи и промени.