					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P32					Заглавие на документа: **Политика за непрекъсваемост на дейността и аварийно 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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	
ISO/IEC 27002:2022	Контроли 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 до CP-11	
NIST SP 800-34 Rev.1	Планиране при извънредни ситуации	Рамка
ISO 22301:2019		Изисквания към системата за управление на непрекъсваемостта на дейността
GDPR на ЕС	Член 32	
Директива NIS2 на ЕС	Член 21(2)(f)	
DORA на ЕС	Член 10	
COBIT 2019	DSS	

1. Цел

1.1. Настоящата политика определя задължителните контроли и отговорности за осигуряване на способността на организацията да поддържа или възстановява критични бизнес операции и поддържащи ИКТ услуги по време на и след прекъсващ инцидент.

1.2. Политиката има за цел да защитава живота, оперативната стабилност, правните задължения, ангажиментите към клиентите и репутацията на организацията чрез изграждане на устойчивост посредством проактивно планиране и валидирани способности за възстановяване.

1.3. Настоящата политика осигурява основата на рамката на организацията за управление на непрекъсваемостта на дейността (BCM) и аварийното възстановяване (DR), като гарантира съответствие с приложимите регулаторни, договорни и отраслови изисквания.

2. Обхват

2.1. Настоящата политика се прилага за всички организационни единици, информационни системи, бизнес процеси, персонал и услуги, предоставяни от трети страни, които са класифицирани като критични или съществени въз основа на резултатите от анализа на въздействието върху бизнеса (BIA).

2.2. Политиката обхваща:

2.2.1. Прекъсвания, причинени от природни или предизвикани от човека събития, включително кибератаки, откази на инфраструктура, недостъпност на центрове за данни, пандемии и прекъсвания в услугите на доставчици

2.2.2. Планиране, тестване и непрекъснато усъвършенстване на плановете за непрекъсваемост на дейността (BCP) и плановете за аварийно възстановяване (DRP)

2.2.3. Роли и отговорности за аварийно реагиране, координация на възстановяването и ескалация на инциденти

2.3. Всички служители с отговорности по непрекъсваемостта или възстановяването, включително ИТ, собственици на бизнес процеси, кризисни мениджъри и доставчици, са длъжни да спазват разпоредбите на настоящата политика.

3. Цели

3.1. Да се осигури непрекъсваемост на бизнес операциите и услугите чрез предварително определени и тествани процедури, като се минимизира оперативното, репутационното и правното въздействие.

3.2. Да се възстановяват ИКТ услугите в рамките на определените целеви стойности за време за възстановяване (RTO) и целеви точки за възстановяване (RPO), съгласувани с нивата на толеранс към риск на бизнеса.

3.3. Да се определи отговорността за планирането, изпълнението и управлението на непрекъсваемостта на дейността и аварийното възстановяване в рамките на цялата организация.

3.4. Да се гарантира, че способностите за непрекъсваемост се тестват, поддържат и усъвършенстват регулярно въз основа на реалистични сценарии и одитни констатации.

3.5. Да се изпълнят задълженията за съответствие по ISO, NIST, GDPR, DORA и NIS2, като се подкрепя надлежната грижа по отношение на оперативната устойчивост и наличността.

4. Роли и отговорности

4.1. Изпълнително ръководство

4.1.1. Одобрява Политиката за непрекъсваемост на дейността и аварийно възстановяване и осигурява стратегическо съгласуване.

4.1.2. Осигурява бюджет и ресурси в подкрепа на непрекъсваемостта на дейността, аварийното реагиране и ученията за възстановяване.

4.2. Ръководител по непрекъсваемост на дейността (BCM Lead)

4.2.1. Отговаря за разработването и поддържането на BCP на организационно ниво и за координацията на тестовете за непрекъсваемост.

4.2.2. Поддържа графика за BIA, координира обучението и гарантира, че документацията отговаря на изискванията за съответствие.

[... 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. Настоящата политика трябва да се преглежда ежегодно от Ръководителя по непрекъсваемост на дейността и директора по информационна сигурност, за да се гарантира съгласуваност с:

9.1.1. Промени в бизнес операциите, критичните системи или инфраструктурата

9.1.2. Извлечени поуки от инциденти, одити, настолни учения или тестове за аварийно възстановяване

9.1.3. Актуализирани регулаторни или договорни задължения (напр. DORA, GDPR, клиентски изисквания за RTO/RPO)

9.1.4. Промени в апетита към риск на организацията или стратегията за непрекъсваемост

9.2. Прегледите трябва да включват:

9.2.1. Валидиране на приложимостта на плановете и данните за контакт

9.2.2. Повторна оценка на RTO, RPO и категоризацията по нива на възстановяване

9.2.3. Оценка на капацитета на услугите за резервно копиране и аварийно възстановяване

9.2.4. Обратна връзка от заинтересовани страни, изпълнили скорошни планове или тестове за възстановяване

9.3. Всички промени в политиките трябва да бъдат:

9.3.1. Под управление на версиите с документирана обосновка и потвърждение от заинтересованите страни

9.3.2. Комуникирани към ключовия персонал и екипите с актуализирани отговорности

9.3.3. Отразени в актуализирани обучения, материали за осведоменост и оперативни процедури

9.4. Извънредни междинни актуализации трябва да се издават при съществена организационна промяна, правно изискване или критична констатация, която прави текущите планове или политиката неприложими.

10. Свързани политики и връзки

10.1. Настоящата политика се прилага съвместно със следните ключови документи:

10.1.1. P1 – Политика за информационна сигурност: Установява изискването за устойчиви, базирани на риска операции при всякакви условия.

10.1.2. P5 – Политика за управление на промените: Гарантира, че всички промени в конфигурацията или инфраструктурата, свързани с възстановяване, следват документирани и одобрени работни потоци.

10.1.3. P14 – Политика за съхранение на данни и унищожаване: Регламентира жизнения цикъл на носителите за резервни копия и възстановените данни, използвани при дейности по непрекъсваемост.

10.1.4. P15 – Политика за архивиране и възстановяване: Прилага контроли относно честотата на архивиране, сигурността и проверката на възстановяването.

10.1.5. P18 – Политика за криптографски контроли: Гарантира, че процесите по възстановяване поддържат стандартите за криптиране и поверителност.

10.1.6. P22 – Политика за регистриране и мониторинг: Подпомага откриването и ескалацията на събития, влияещи върху непрекъсваемостта.

10.1.7. P30 – Политика за реагиране при инциденти: Определя процесите по ограничаване, ескалация и анализ на първопричините, съгласувани с тригерите за непрекъсваемост.

10.1.8. P33 – Политика за мониторинг на одита и съответствието: Валидира целостта и ефективността на практиките за непрекъсваемост и възстановяване в системите и процесите.

11. Референтни стандарти и рамки

11.1. Настоящата политика е съгласувана с международно признати стандарти за непрекъсваемост на дейността и аварийно възстановяване и подпомага доказването на съответствие, устойчивостта и правното съответствие.

11.2. ISO/IEC 27002

11.2.1. Приложение A, Контрол 5.29 – Информационна сигурност по време на прекъсване: Изисква непрекъснатост на контролите за сигурност при неблагоприятни условия.

11.2.2. Приложение A, Контрол 5.30 – ИКТ готовност за непрекъсваемост на дейността: Изисква подготовка, тестване и валидиране на способностите за възстановяване на ИКТ.

11.3. ISO 22301:2019 – Системи за управление на непрекъсваемостта на дейността

11.3.1. Осигурява рамката за установяване, внедряване и поддържане на практики по BCM, съгласувани с организационните цели и праговете на риск.

11.4. NIST SP 800-34 Rev.1 – Ръководство за планиране при извънредни ситуации

11.4.1. Описва добри практики в индустрията за планове при извънредни ситуации за ИТ системи, включително разработване на стратегия за непрекъсваемост, анализ на въздействието и тестване на планове.

11.5. GDPR на ЕС (2016/679)

11.5.1. Член 32 – Сигурност на обработването: Изисква устойчивост на системите за обработване и своевременно възстановяване на наличността и достъпа до лични данни след инцидент.

11.6. Директива NIS2 на ЕС (2022/2555)

11.6.1. Член 21(2)(f): Изисква мерки за непрекъсваемост на дейността и управление при кризи в подкрепа на сигурността на мрежовите и информационните системи.

11.7. DORA на ЕС (2022/2554)

11.7.1. Член 10 – ИКТ непрекъсваемост на дейността: Изисква финансовите субекти да разработват и тестват планове за непрекъсваемост на ИКТ, включително базирани на риска RTO/RPO и възможности за превключване при отказ.

11.8. COBIT 2019

11.8.1. DSS04 – Управление на непрекъсваемостта: Обхваща всички аспекти на планирането на непрекъсваемостта, включително идентифициране на заплахи, анализ на въздействието, стратегия за възстановяване и редовно тестване.