					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P32S					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 регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1, 6.3, 8	
ISO/IEC 27002:2022	Контроли 5.29, 5	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
GDPR на ЕС	Членове 32, 33	
NIS2 на ЕС	Член 21(2)(f)	
DORA на ЕС	Член 10	
COBIT 2019	DSS	

1. Цел

1.1 Настоящата политика гарантира, че организацията е в състояние да поддържа непрекъсваемост на дейността и да възстановява съществени ИТ услуги по време на и след прекъсващи събития, като прекъсване на електрозахранването, кибератаки, ransomware инфекции или откази на системи.

1.2 Тя определя ясна рамка за планиране на непрекъсваемостта на дейността и аварийното възстановяване (BC/DR), съобразена с нуждите на МСП без собствен ИТ екип.

1.3 Настоящата политика подпомага организацията да изпълнява приложимите задължителни изисквания по ISO/IEC 27001:2022, GDPR, NIS2, DORA и COBIT 2019, като същевременно изгражда оперативна устойчивост и доверие у клиентите.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 всички системи и услуги от критично значение за бизнеса (напр. електронна поща, облачно съхранение, платформи за фактуриране, клиентски записи)

2.1.2 всички служители и външни доставчици на ИТ услуги, отговорни за готовността и изпълнението на BC/DR

2.1.3 всички видове прекъсвания, включително киберинциденти, отказ на хардуер, прекъсване на електрозахранването, наводнение и недостъпност на офиса

2.2 Политиката обхваща:

2.2.1 управление на резервните копия

2.2.2 планиране на непрекъсваемостта на дейността (BCP)

2.2.3 дейности по аварийно възстановяване

2.2.4 обучение на персонала и тестване

2.2.5 процедури за правна и регулаторна реакция

3. Цели

3.1 Да защитава способността на организацията да предоставя ключови услуги въпреки непланирани прекъсвания.

3.2 Да осигурява своевременно възстановяване на системи и данни в съответствие с предварително определените целеви стойности за време за възстановяване (RTO).

3.3 Да гарантира, че целият персонал може да следва процедурите за непрекъсваемост по време на кризи при минимално объркване.

3.4 Да поддържа съответствие с изискванията за защита на данните и оперативна устойчивост, включително член 32 от GDPR и член 21 от NIS2.

3.5 Да установи практическа и подлежаща на тестване стратегия за непрекъсваемост и възстановяване, подходяща за МСП.

4. Роли и отговорности

4.1 Управител (GM)

4.1.1 Носи отговорност за процеса по BC/DR и за настоящата политика

4.1.2 Одобрява Плана за непрекъсваемост на дейността (BCP)

4.1.3 Координира реагирането при инциденти и вътрешната комуникация по време на прекъсвания

4.1.4 Извършва регулаторни уведомления, когато се изискват (напр. уведомления за нарушения по GDPR)

4.2 Доставчик на ИТ услуги / системен администратор

4.2.1 Поддържа и тества резервните копия

4.2.2 Изпълнява процедурите за аварийно възстановяване при активиране

4.2.3 Документира всички действия по възстановяване и събитията, свързани с възстановяването на системите

4.2.4 Докладва незабавно на GM за критични ИТ инциденти

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

9. Преглед и актуализация

9.1 Годишен преглед на политиката и плана

9.1.1 Управителят (GM) трябва да гарантира, че настоящата политика и свързаният с нея План за непрекъсваемост на дейността (BCP) се преглеждат формално поне веднъж годишно.

9.1.2 Прегледът трябва да включва:

9.1.2.1 оценка на нови или възникващи рискове

9.1.2.2 повторно валидиране на RTO/RPO

9.1.2.3 проверка на информацията за доставчици и контакти

9.1.2.4 съгласуване с промени в ИТ системите, правните задължения или дейността

9.2 Актуализации, задействани от събития

9.2.1 Настоящата политика трябва да се актуализира и при:

9.2.1.1 съществени инциденти или прекъсвания, особено ако целите не са били постигнати

9.2.1.2 нови правни или регулаторни задължения (напр. изменения по DORA)

9.2.1.3 промени в критични системи, облачни платформи или персонал

9.2.1.4 констатации от годишните тестове на BCP/DR

9.3 Процес за контрол на промените

9.3.1 Всички промени трябва да бъдат одобрени от GM

9.3.2 Трябва да се поддържа регистър на историята на версиите, включващ дата, описание на промяната и одобряващия

9.3.3 Актуализираната политика трябва да бъде повторно разпространена до целия относим персонал, включително доставчика на ИТ услуги и ръководителите на отдели

9.4 Документиране на извлечените поуки

9.4.1 След тестове или реални прекъсвания документираните извлечени поуки трябва да се използват при бъдещи преработки

9.4.2 Тези прегледи трябва да включват и оценки на представянето на доставчиците и проверки за адекватност на реакцията

10. Свързани политики и връзки

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

10.1.1 P1S – Политика за информационна сигурност: Определя общите цели по сигурността, които практиките за непрекъсваемост и възстановяване трябва да подкрепят.

10.1.2 P4S – Политика за контрол на достъпа: Осигурява възможност за аварийно отнемане или възстановяване на потребителски достъп при сценарии на прекъсване на дейността.

10.1.3 P6S – Политика за управление на риска: Формира основата за идентифициране, оценяване и приоритизиране на рисковете, свързани с непрекъсваемостта.

10.1.4 P8S – Политика за информираност и обучение по информационна сигурност: Гарантира, че служителите са подготвени да действат при прекъсвания и разбират BCP.

10.1.5 P15S – Политика за архивиране и възстановяване: Определя конкретни технически процедури за защита на наличността на данните и тяхното възстановяване.

10.1.6 P17S – Политика за защита на данните и поверителност: Гарантира, че планирането на непрекъсваемостта спазва изискванията за защита на личните данни и съответства на GDPR по време на и след инциденти.

10.1.7 P22S – Политика за регистриране и мониторинг: Подпомага откриването на събития, които могат да задействат процесите по BC/DR, и осигурява форензични одитни следи след прекъсване.

10.1.8 P30S – Политика за реагиране при инциденти: Непосредствено предхожда активирането на процеса по възстановяване при киберинциденти или оперативни инциденти.

10.1.9 P31S – Политика за събиране на доказателства и форензика: Гарантира, че цифровите доказателства се събират по време на сценарии на непрекъсваемост за нуждите на съответствието, застраховането или разследването.

10.2 Тези политики формират съгласувана и подготвена за одит рамка за устойчивост, отчетност и непрекъсваемост на контрола във всички дейности на МСП.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:

11.1.1 Клауза 6.1 – Изисква планиране и третиране, базирани на риска, включително непрекъсваемост на дейността и възстановяване.

11.1.2 Клауза 6.3 – Подчертава непрекъснатото подобрение след прекъсвания.

11.1.3 Клауза 8.1 – Изисква оперативни контроли, които включват документирани мерки за непрекъсваемост.

11.2 ISO/IEC 27002:

11.2.1 Контрол 5.29 – Изисква създаване и поддържане на механизми за непрекъсваемост на дейността.

11.2.2 Контрол 5.30 – Изисква тестване и преглед на тези механизми.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Определя изисквания за планиране при извънредни ситуации.

11.3.2 CP-4 – Изисква обучение по непрекъсваемост за персонала на организацията.

11.3.3 CP-6 – Обхваща изискванията за алтернативно място за съхранение.

11.3.4 CP-7 – Регламентира очакванията за алтернативна среда за обработка.

11.4 GDPR на ЕС:

11.4.1 Член 32 – Изисква мерки за осигуряване на постоянна наличност и устойчивост на системите и услугите за обработване.

11.4.2 Член 33 – Поражда задължения за уведомяване при нарушения, когато отказ в непрекъсваемостта води до компрометиране на лични данни.

11.5 Директива (ЕС) NIS2 (2022/2555):

11.5.1 Член 21(2)(f) – Изисква планиране на непрекъсваемостта и способности за управление на кризи като условие за готовност по отношение на киберрисковете.

11.6 Регламент (ЕС) DORA (2022/2554):

11.6.1 Член 10 – Изисква внедряване на тестване за цифрова оперативна устойчивост и способности за възстановяване, особено за МСП във финансовия сектор.

11.7 COBIT 2019:

11.7.1 DSS04 – Управление на непрекъсваемостта: Предоставя насоки за корпоративно управление относно поддържането и валидирането на оперативната устойчивост, включително собственост, тестване, интеграция на доставчици и прегледи след събития.