					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P30S					Заглавие на документа: **Политика за реагиране при инциденти**							
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 регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1, 6.3, 8	Управление на инциденти, непрекъснато подобрение, оперативен контрол
ISO/IEC 27002:2022	Контроли 5.24, 5.25	Откриване на инциденти, готовност, извличане на поуки
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Обработване и мониторинг на инциденти, докладване
GDPR на ЕС	Член 33	Изисквания за уведомяване при нарушения
NIS2 на ЕС	Член 23	Задължително докладване на киберинциденти
DORA на ЕС	Член 17	Управление на ИКТ инциденти
COBIT 2019	DSS02, DSS04	Управление на услуги и инциденти, както и непрекъсваемост

1. Цел

1.1. Настоящата политика определя начина, по който организацията открива, докладва и реагира при инциденти по информационна сигурност, засягащи нейните цифрови системи, данни или услуги.

1.2. Политиката подпомага организацията да сведе до минимум щетите, да защити данните на клиентите и да изпълни приложимите регулаторни изисквания, включително изискването на GDPR за уведомяване при нарушение в 72-часов срок.

1.3. Политиката осигурява ясно разпределение на отговорностите, стъпките за комуникация и последващите действия след инцидент, включително в малки организации без собствен екип по сигурност.

2. Обхват

2.1. Настоящата политика се прилага за:

2.1.1. Всички служители, външни изпълнители и външни доставчици на ИТ услуги.

2.1.2. Всички системи и услуги, управлявани от дружеството, включително уебсайтове, облачни платформи, мобилни устройства, лаптопи и акаунти за електронна поща.

2.1.3. Всички видове инциденти, включително:

2.1.3.1. Неоторизиран достъп до данни или системи.

2.1.3.2. Инфекции със зловреден софтуер или рансъмуер.

2.1.3.3. Опити за фишинг или социално инженерство.

2.1.3.4. Недостъпност на системи поради кибератаки или неправомерна употреба.

2.1.3.5. Случайно разкриване или изтриване на чувствителна информация.

2.1.3.6. Загуба или кражба на служебни устройства или носители за съхранение.

3. Цели

3.1. Да се установи ясен процес за разпознаване и ескалиране на инциденти по сигурността.

3.2. Да се гарантира, че инцидентите се докладват, регистрират и по тях се предприемат действия в предварително определени срокове.

3.3. Да се осигури бързо ограничаване на щетите, възстановяване на данни и възстановяване на услуги.

3.4. Да се гарантира, че засегнатите страни (напр. клиенти, регулатори) се уведомяват, когато това се изисква по закон.

3.5. Да се предотврати повторна поява чрез анализ на първопричините, коригиращи действия и подобряване на политиката.

3.6. Да се даде възможност на МСП да изпълняват изискванията за сертифициране по ISO/IEC 27001 и да демонстрират отчетност по време на одити.

4. Роли и отговорности

4.1. Управител

4.1.1. Отговаря за настоящата политика и осигурява нейното прилагане.

4.1.2. Упражнява надзор върху дейностите по реагиране при инциденти и одобрява уведомленията до регулатори или клиенти.

4.1.3. Преглежда докладите след инцидент и гарантира, че при необходимост се извършват актуализации на политиките.

4.1.4. Може да делегира координационни задължения, но запазва отчетността.

4.2. Доставчик на ИТ поддръжка / системен администратор (вътрешен или външен)

4.2.1. Открива и разследва потенциални инциденти по сигурността.

4.2.2. Изпълнява действия по ограничаване и възстановяване (напр. деактивиране на достъп, възстановяване от резервни копия).

4.2.3. Уведомява Управителя за всички потвърдени или предполагаеми инциденти в рамките на 1 час от установяването им.

4.2.4. Поддържа регистър на инцидентите с времеви маркери, оценка на въздействието и предприетите действия по реагиране.

[... 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. Планиран преглед

9.1.1. Настоящата политика се преглежда най-малко веднъж на всеки 12 месеца от Управителя, за да се гарантира:

9.1.1.1. Съответствие с контролите на ISO/IEC 27001:2022.

9.1.1.2. Способност за реакция спрямо нови заплахи, рискове и инциденти.

9.1.1.3. Продължаващо съответствие със законовите и договорните задължения (напр. GDPR, DORA).

9.2. Събития, задействащи преглед

9.2.1. Политиката се преглежда и актуализира също и след:

9.2.1.1. Всеки инцидент с висока степен на сериозност или регулаторно уведомяване.

9.2.1.2. Въвеждане на нова ИТ инфраструктура или промени в системите.

9.2.1.3. Промени в правните изисквания, свързани с нарушения на сигурността.

9.3. Документиране и разпространение на прегледа

9.3.1. Всички прегледи и промени се документират в журнал на промените по политиката.

9.3.2. Актуализираните версии се разпространяват до всички служители, доставчици и доставчици на ИТ поддръжка, участващи в дейности по сигурност или експлоатация на системи.

9.3.3. Доказателства за осведомеността на служителите (напр. протоколи от срещи или потвърждения по електронна поща) трябва да се съхраняват с оглед на готовност за одит.

10. Свързани политики и връзки

10.1. Настоящата политика се прилага координирано със следните политики за МСП:

10.1.1. P1S – Политика за информационна сигурност: Определя общите изисквания за поддържане на поверителност, цялостност и наличност по време на операциите, включително обработването на инциденти.

10.1.2. P2S – Политика за роли и отговорности в управлението: Установява структурите на правомощия и отчетност за откриване, докладване и ескалация на инциденти.

10.1.3. P4S – Политика за контрол на достъпа: Осигурява незабавно отнемане на права за достъп по време на действия по реагиране при инцидент.

10.1.4. P8S – Политика за информираност и обучение по информационна сигурност: Гарантира, че всички служители могат ефективно да идентифицират и докладват инциденти по сигурността.

10.1.5. P17S – Политика за защита на данните и поверителност: Насочва процедурите за правно уведомяване при нарушение съгласно GDPR и подпомага регулаторното съответствие по време на инциденти.

10.1.6. P22S – Политика за регистриране и мониторинг: Осигурява необходимите инструменти и видимост за откриване, анализ и одит на събития по сигурността.

10.1.7. P31S – Политика за събиране на доказателства и компютърна криминалистика: Подпомага разследването и правната обоснованост на действията, свързани с инциденти, чрез насоки за правилно боравене с доказателства.

10.2. Тези политики съвместно установяват оперативната рамка на МСП за откриване, реагиране и възстановяване след инциденти по информационна сигурност.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 6.1 – Изисква планиране на третирането на риска, включително подготовка за инциденти.

11.1.2. Клауза 6.3 – Подкрепя непрекъснатото подобрение чрез извличане на поуки от събития по сигурността.

11.1.3. Клауза 8.1 – Подчертава необходимостта от оперативен контрол за управление на инциденти и прекъсвания.

11.2. ISO/IEC 27002

11.2.1. Контрол 5.24 – Изисква структуриран подход за докладване, оценяване и реагиране при инциденти по информационна сигурност.

11.2.2. Контрол 5.25 – Фокусира се върху извличането на поуки от инциденти с цел подобряване на бъдещата готовност и устойчивостта на системите.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Определя процедури за обработване на инциденти, включително ограничаване и възстановяване.

11.3.2. IR-5 – Установява изисквания за мониторинг и анализ на инциденти.

11.3.3. IR-6 – Въвежда задължителни протоколи за вътрешно и външно докладване на инциденти.

11.4. GDPR на ЕС

11.4.1. Член 33 – Изисква докладване на нарушения на сигурността на личните данни до регулаторите в 72-часов срок, с подробности за обхвата и смекчаващите мерки.

11.5. Директива NIS2 на ЕС (2022/2555)

11.5.1. Член 23 – Изисква съществените и важните субекти да уведомяват компетентните органи за значими инциденти, като използват стандартизирани формати за докладване.

11.6. Регламент DORA на ЕС (2022/2554)

11.6.1. Член 17 – Изисква финансовите субекти да класифицират, докладват и проследяват инциденти и прекъсвания, свързани с ИКТ.

11.7. COBIT 2019

11.7.1. DSS02 – Управление на заявки за услуги и инциденти: Дава насоки за ефективно обработване на оперативни инциденти и инциденти по сигурността в съответствие с целите на управлението.

11.7.2. DSS04 – Управление на непрекъсваемостта: Свързва реагирането при инциденти с по-широките стратегии за непрекъсваемост и възстановяване.