					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P30					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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8.1, Клауза 9	Структурирани процеси за управление на риска и реагиране при инциденти
ISO/IEC 27002:2022	Контроли 5.25–5.27	Роли, докладване, реагиране и подобрение при инциденти
NIST SP 800-53 Rev.5	IR-1 до IR-9	Цялостен жизнен цикъл на реагиране при инциденти
GDPR на ЕС	Член 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Срокове за уведомяване при нарушения, докладване и комуникация със субектите на данни
NIS2 на ЕС	Член 23(1)–(4)	Уведомяване на националния компетентен орган и структурирано докладване
DORA на ЕС	Член 17(1)–(3)	Докладване на значими инциденти, свързани с ИКТ, за финансови субекти
COBIT 2019	DSS02, DSS04, MEA	Определя, наблюдава и оценява управлението на инциденти, непрекъсваемостта и оценяването

1. Цел

1.1 Настоящата политика установява формална рамка за идентифициране, докладване, анализ, ограничаване, реагиране, възстановяване и оценка след инцидент на инциденти по информационната сигурност, засягащи организацията.

1.2 Тя осигурява своевременно, координирано и ефективно реагиране с цел минимизиране на оперативните прекъсвания, финансовите загуби, репутационните щети и регулаторното несъответствие.

1.3 Политиката подпомага и непрекъснатото подобряване на киберустойчивостта на организацията чрез извлечени поуки и интегриране на констатациите след инцидент в управлението, инструментите и програмите за обучение.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички лица, включително служители, външни изпълнители, консултанти и външни доставчици на услуги

2.1.2 Всички информационни системи, приложения, инфраструктура, мрежи и данни, независимо дали са локални, в облака или в хибридна среда

2.1.3 Всички видове инциденти по сигурността, включително, но не само:

2.1.3.1 Неоторизиран достъп или ескалация на привилегии

2.1.3.2 Атаки със зловреден софтуер и ransomware

2.1.3.3 Атаки за отказ на услуга (DoS/DDoS)

2.1.3.4 Загуба, изтичане или извличане на данни

2.1.3.5 Неправомерни действия от вътрешни лица или нарушения на политиката

2.1.3.6 Нарушения на физическата сигурност, засягащи цифрови активи

2.2 Политиката обхваща откриването, триажа, разследването, ескалацията, ограничаването, обработването на доказателства, уведомяването, възстановяването и анализа на първопричините.

3. Цели

3.1 Да установи повтаряема и мащабируема способност за реагиране при инциденти, която позволява бързо откриване, класифициране и смекчаване на инциденти по сигурността.

3.2 Да минимизира въздействието върху дейността от събития по сигурността чрез структурирани процедури за ограничаване, отстраняване и възстановяване на системите.

3.3 Да гарантира, че докладването и реагирането при инциденти са съобразени с правните, регулаторните и договорните изисквания, по-специално тези относно сроковете за уведомяване при нарушения и обработването на доказателства.

3.4 Да подпомага прозрачността и отчетността чрез надлежно регистриране, документиране и проследяване на показатели за всички инциденти по сигурността.

3.5 Да насърчава непрекъснатото подобрение чрез прегледи след инцидент, коригиращи действия и обучение на заинтересованите страни.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за рамката за реагиране при инциденти, осигурява прилагането на политиката и упражнява надзор върху координацията на инцидентите в цялата организация.

4.1.2 Изпълнява ролята на основна точка за контакт с регулаторите, висшето ръководство и външния правен консултант при значими инциденти.

4.2 Координатор по реагиране при инциденти

4.2.1 Координира междуфункционалните екипи за реагиране, управлява работните потоци и проследява статуса на ограничаването и възстановяването.

4.2.2 Инициира и ръководи прегледите след инцидент (PIR) и гарантира, че коригиращите действия се регистрират и изпълняват.

[... 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 най-малко веднъж годишно и да се актуализира при необходимост, за да включва:

9.1.1 Промени в ландшафта на заплахите, типовете инциденти или векторите на атака

9.1.2 Извлечени поуки от съществени инциденти, предотвратени инциденти или регулаторни констатации

9.1.3 Актуализации на приложимите закони и регулации (напр. GDPR, DORA, NIS2)

9.1.4 Обратна връзка от учения за реагиране при инциденти и прегледи след инцидент

9.2 CISO отговаря за инициирането и координирането на процеса по преглед в консултация със:

9.2.1.1 Правен консултант и DPO

9.2.1.2 SOC и ИТ операции

9.2.1.3 Екипите по непрекъсваемост на дейността и управление на риска

9.2.1.4 Изпълнителното ръководство

9.3 Промените в политиката трябва да бъдат:

9.3.1 Документирани в хранилище с управление на версиите

9.3.2 Комуникирани към всички засегнати екипи и отразени в обучението за осведоменост

9.3.3 Валидирани чрез tabletop или практически учения за реагиране при инциденти в рамките на три месеца от одобрението

9.4 Спешните актуализации, породени от нововъзникващи заплахи, одитни констатации или нововъведени правни задължения, трябва да бъдат въведени незабавно и отразени в историята на версиите на политиката.

10. Свързани политики и връзки

10.1 Настоящата политика се подпомага от и зависи от следните организационни политики:

10.1.1 P1 – Политика за информационна сигурност: Установява общото изискване за дейност, основана на риска, и готовност за инциденти.

10.1.2 P5 – Политика за управление на промените: Гарантира, че дейностите по ограничаване и възстановяване, свързани с инфраструктура или услуги, следват формални процедури.

10.1.3 P13 – Политика за класификация и етикетиране на данни: Подпомага класификацията на тежестта на инцидентите въз основа на чувствителността на данните.

10.1.4 P15 – Политика за архивиране и възстановяване: Осигурява възстановяване след ransomware или разрушителни атаки с гарантиране на целостта.

10.1.5 P18 – Политика за криптографски контроли: Определя мерки за криптиране, които намаляват въздействието на инциденти и риска от експозиция на данни.

10.1.6 P22 – Политика за регистриране и наблюдение: Осигурява основната видимост върху събитията, алармирането и съхранението на журнали, необходими за ефективно откриване и форензичен анализ.

10.1.7 P29 – Политика за тестови данни и тестова среда: Гарантира, че инцидентите, засягащи непроизводствени системи, също се обработват по структуриран и сигурен начин.

10.1.8 P33 – Политика за мониторинг на одита и съответствието: Валидира готовността за инциденти и ефективността на реагирането чрез структурирани одити и оценки на съответствието.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001: Клауза 8.1 – Оперативно планиране и контрол: Структурирани процеси за управление на рисковете и планиране на реагирането при инциденти.

11.2 ISO/IEC 27002:2022 – Контроли 5.25–5.27: Отговорности за управление на инциденти, докладване, реагиране, комуникация и подобрение.

11.3 NIST SP 800-53 Rev.5: IR-1 до IR-9, AU-6, PL-2: Цялостни изисквания за жизнения цикъл на реагиране при инциденти, одит и планиране на сигурността.

11.4 GDPR на ЕС: Член 33/34: Задължения за докладване към надзорните органи и изисквания за уведомяване на субектите на данни (с определени изключения).

11.5 Директива NIS2 на ЕС (2022/2555): Член 23: Задължително национално докладване, включително междинни и окончателни задължения за докладване.

11.6 DORA на ЕС (2022/2554): Член 17: Изисквания към финансовите институции за докладване на ИКТ инциденти към компетентните органи.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Управление на инциденти по услуги и непрекъсваемост, както и наблюдение на резултатността/съответствието.