					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P39					Заглавие на документа: **Политика за координирано разкриване на уязвимости**							
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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
GDPR на ЕС	Art. 32(1)(d)	
NIS2 на ЕС	Art. 21(2)(e)	
DORA на ЕС	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Цел

1.1 Да установи формален процес за приемане, обработване и оповестяване на информация за уязвимости, засягащи системите или услугите на организацията, в съответствие с изискванията на член 21, параграф 2, буква „е“ от NIS2 относно обработването и оповестяването на уязвимости.

1.2 Да насърчава външни изследователи по сигурността, партньори и потребители да докладват уязвимости по отговорен начин чрез координирано оповестяване на уязвимости (CVD), както и да определя начина, по който организацията комуникира информация за уязвимости със заинтересованите страни.

2. Обхват

2.1 Тази политика се прилага за всички мрежови и информационни системи, притежавани или експлоатирани от организацията, както и за всички установени уязвимости в тези системи.

2.2 Тя обхваща вътрешните екипи (сигурност, ИТ, разработка) и всички външни страни, които докладват уязвимости (напр. изследователи, клиенти, доставчици). Политиката урежда също комуникацията с продуктови доставчици или външни доставчици на услуги, когато техни компоненти са засегнати от уязвимостта.

3. Цели

3.1 Да осигури своевременно откриване и отстраняване на уязвимости в сигурността чрез използване както на вътрешни оценки, така и на външни оповестявания.

3.2 Да предостави ясни указания на външните податели на сигнали за безопасно и законосъобразно подаване на информация за уязвимости, както и на организацията за ефективно реагиране и отстраняване.

3.3 Да осигури съответствие с изискванията на NIS2 и най-добрите практики в индустрията (ISO/IEC 29147 и ISO/IEC 30111) за координирано оповестяване на уязвимости с цел повишаване на сигурността на цялостната екосистема.

4. Роли и отговорности

4.1 Екип за реагиране при уязвимости (VRT): определен екип, ръководен от директора по информационна сигурност (CISO) или ръководителя по управление на уязвимостите, който приема и триажира сигналите за уязвимости, оценява риска и въздействието и координира отстраняването и публичното оповестяване.

4.2 Екипи по ИТ и разработка: работят съвместно с VRT за валидиране на докладваните уязвимости, разработване и тестване на корекции по сигурността или мерки за смекчаване и внедряване на корекции. При необходимост предоставят технически подробности за съобщения за сигурност.

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

9. Мониторинг и одит

9.1 VRT поддържа регистър за оповестяване на уязвимости, който проследява всеки сигнал от получаването му до приключването. Този регистър се преглежда ежемесечно, за да се гарантира своевременен напредък по отворените случаи. Просрочените случаи се ескалират.

9.2 Вътрешният одит или независим оценител по сигурността ежегодно преглежда ефективността на процеса по обработване на уязвимости — например чрез проверка, че извадка от случаи е обработена съгласно политиката (потвърдени, отстранени и оповестени своевременно). Проверява се и дали публично достъпният канал за оповестяване функционира ефективно (напр. дали тестови имейли се получават и обработват).

9.3 Показателите за уязвимости (обем по степен на сериозност, срокове за отстраняване и др.) се обобщават на тримесечна база и се представят на комитета по управление на киберсигурността с цел актуализиране на оценките на риска.

10. Преглед и поддръжка

10.1 Тази политика подлежи на преглед най-малко веднъж годишно. Допълнително всяка значима промяна в ИТ средата на организацията (напр. пускане на нова услуга с достъп от интернет) или съществено регулаторно развитие (напр. нови нормативни актове на ЕС относно оповестяването на продуктови уязвимости) води до извънреден преглед.

10.2 Актуализациите на политиката включват обратна връзка от външни податели на сигнали и поуки от вътрешни анализи след инцидент. Съществените промени се одобряват от CISO, комуникират се до всички служители и се публикуват в онлайн хранилището за политики по сигурност на организацията с оглед на прозрачност.

11. Свързани политики и връзки

11.1 P01 – Политика за информационна сигурност. Определя управленския мандат за обработване и оповестяване на уязвимости.

11.2 P19 – Политика за управление на уязвимости и корекции. Определя вътрешния процес за отстраняване, свързан с приемането по CVD.

11.3 P24 – Политика за сигурна разработка. Осигурява корекции и укрепване на SDLC въз основа на докладвани проблеми.

11.4 P25 – Политика за изисквания за сигурност на приложенията. Гарантира, че продуктите имат подготвени за оповестяване изисквания за сигурност.

11.5 P30 – Политика за реагиране при инциденти. Обхваща случаи на активна експлоатация на оповестени уязвимости.

11.6 P31 – Политика за събиране на доказателства и форензика. Осигурява запазване на артефакти, свързани с докладвани/експлоатирани дефекти.

11.7 P26 – Политика за сигурност на трети страни и доставчици. Координира оповестявания, засягащи компоненти на доставчици.

11.8 P37 – Политика по правни въпроси и регулаторно съответствие. Урежда уведомяването, формулировките за безопасна правна рамка и публикуването.

12. Референтни стандарти и рамки

12.1 Директива NIS2 (ЕС 2022/2555), член 21, параграф 2, буква „е“ (сигурност при разработката и обработване и оповестяване на уязвимости)

12.2 Регламент за изпълнение (ЕС) 2024/2690 на Комисията, приложение, раздел 6.10 (технически изисквания относно процесите за обработване и оповестяване на уязвимости)

12.3 Технически указания на ENISA относно мерките за управление на риска за киберсигурността – раздел за обработване и оповестяване на уязвимости

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (контрол A.5.7 относно разузнаване за заплахи и оповестяване на уязвимости; контрол A.8.28 относно сигурна разработка)

12.5 ISO/IEC 29147:2018 (указания за оповестяване на уязвимости) и ISO/IEC 30111:2019 (указания за процесите по обработване на уязвимости)