					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P38					Заглавие на документа: **Политика за сигурни комуникации и многофакторно удостоверяване**							
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	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
EU GDPR	Art. 32(1)(b)	
EU NIS2	Art. 21(2)(j)	
EU DORA	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Цел

1.1 Да се определят изискванията за използване на многофакторно удостоверяване или решения за непрекъсната автентикация при достъп до системи в съответствие с член 21, параграф 2, буква „й“ от NIS2.

1.2 Да се установят контроли за защитени гласови, видео, текстови и аварийни комуникации с цел защита на поверителността и целостта на информацията.

2. Обхват

2.1 Тази политика се прилага за всички механизми за автентикация и комуникационни системи (гласови обаждания, решения за видеоконференции, съобщения и системи за аварийно уведомяване), използвани от организацията.

2.2 Тя обхваща всички служители, външни изпълнители и други външни страни, които използват комуникационните канали на организацията или осъществяват достъп до нейните мрежови и информационни системи.

3. Цели

3.1 Да се гарантира, че достъп до системите получават само надлежно удостоверени потребители, като се намалява рискът от неоторизиран достъп чрез внедряване на многофакторно удостоверяване (MFA).

3.2 Да се гарантира, че вътрешните и аварийните комуникации се предават чрез сигурни методи (напр. криптирани канали), като се предотвратяват подслушване и подправяне.

3.3 Да се осигури съответствие с изискванията на NIS2 за силна автентикация и сигурни комуникации, като се повишава общата киберустойчивост.

4. Роли и отговорности

4.1 Директор „Информационна сигурност“ (CISO) / екипите по ИТ и сигурност: определят и поддържат механизмите за многофакторно удостоверяване (MFA) и инструментите за сигурна комуникация; осигуряват техническото прилагане на тази политика.

4.2 ИТ администратори: внедряват многофакторно удостоверяване (MFA) за приложимите системи и конфигурират одобрените платформи за сигурна комуникация; наблюдават съответствието.

[... 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 Екипите по ИТ и сигурност трябва да извършват непрекъснат мониторинг на журналите за автентикация за опити за вписване само с един фактор или за аномални неуспешни опити при многофакторно удостоверяване (MFA). Журналите на системите за сигурна комуникация (когато е приложимо) трябва да се наблюдават за опити за неоторизиран достъп или промени в конфигурацията.

9.2 Вътрешният одит извършва ежегоден преглед на спазването на изискванията за внедряване на многофакторно удостоверяване (MFA), като потвърждава, че всички критични системи го прилагат, и проверява, че за чувствителни комуникации се използват единствено одобрени сигурни канали. Констатациите се докладват на ръководството заедно с препоръки.

10. Преглед и поддръжка

10.1 Тази политика подлежи на преглед най-малко веднъж годишно, както и при всеки съществен инцидент по сигурността или новоидентифициран риск, свързан с автентикацията или комуникациите (напр. нови вектори на заплаха срещу многофакторното удостоверяване (MFA), установено използване на несигурни комуникации).

10.2 При необходимост се извършват актуализации с цел отразяване на развитието на технологиите (напр. внедряване на по-надеждни решения за непрекъсната автентикация) или осигуряване на съответствие с актуализирани регулаторни насоки (като бъдещи препоръки на ENISA относно сигурните комуникации).

11. Свързани политики и връзки

11.1 P01 – Политика за информационна сигурност. Определя мерките за защита на автентикацията и комуникациите в цялата организация.

11.2 P04 – Политика за контрол на достъпа. Установява управлението на правата за достъп, което многофакторното удостоверяване (MFA) по P38 прилага.

11.3 P11 – Политика за управление на потребителски акаунти и привилегии. Обвързва многофакторното удостоверяване (MFA) с жизнения цикъл на привилегирования достъп.

11.4 P18 – Политика за криптографски контроли. Определя одобрените криптографски средства и управлението на ключове за сигурни комуникации.

11.5 P21 – Политика за мрежова сигурност. Защитава транспортните канали, използвани за глас, видео и съобщения.

11.6 P22 – Политика за регистриране и мониторинг. Осигурява мониторинг на събитията по автентикация и използването на сигурни канали.

11.7 P32 – Политика за непрекъсваемост на дейността и аварийно възстановяване. Защитава аварийните комуникации по време на кризи.

11.8 P08 – Политика за информираност и обучение по информационна сигурност. Обучава потребителите относно многофакторното удостоверяване (MFA) и добрите практики при използване на комуникационни канали.

12. Препратки

12.1 Директива NIS2 (ЕС 2022/2555), член 21, параграф 2, буква „й“ (използване на многофакторно удостоверяване и защитени комуникации)

12.2 Регламент за изпълнение (ЕС) 2024/2690 на Комисията, приложение, раздел 11 (изисквания за контрол на достъпа, включително многофакторно удостоверяване (MFA) за привилегировани акаунти)

12.3 ISO/IEC 27001:2022 и ISO/IEC 27002: