					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P22S					Заглавие на документа: **Политика за регистриране и мониторинг**							
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	Оперативни контроли, включително регистриране
ISO/IEC 27002:2022	Контроли 8.15, 8.16, 8.17	Регистриране на събития, защита на журналите и мониторинг
NIST SP 800-53 Rev.5	AU-2 до AU-12, SI-4	Съдържание и преглед на одитни журнали, съхранение, откриване на аномалии, предупреждения
GDPR на ЕС	Членове 5(1)(f), 32, 33	Поверителност и цялостност на данните, технически мерки и уведомяване при нарушение
NIS2 на ЕС	Членове 21(2)(d), 23	Механизми за регистриране за откриване на аномалии и докладване на инциденти в рамките на 24 часа
DORA на ЕС	Членове 10, 15	Оперативна устойчивост, мониторинг и регистриране при доставчици на услуги
COBIT 2019	DSS01.03, DSS05.02	Проследимост на дейностите и защита чрез регистриране и мониторинг

1. Цел

1.1 Настоящата политика установява задължителни контроли за регистриране и мониторинг с цел осигуряване на сигурността, отчетността и оперативната цялост на ИТ системите на организацията.

1.2 Тя определя видовете събития, които подлежат на регистриране, начина на съхранение на журналите, реда за техния преглед и отговорностите на персонала и доставчиците на услуги.

1.3 Регистрирането и мониторингът подпомагат откриването на заплахи, регулаторното съответствие, реагирането при инциденти и форензичния анализ.

1.4 Настоящата политика позволява на организацията да изпълнява изискванията за оперативни контроли на ISO/IEC 27001 и подпомага готовността за одит, доверието на клиентите и съответствието с GDPR, NIS2 и DORA.

2. Обхват

2.1 Настоящата политика се прилага за всички системи и потребители в организацията, включително:

2.1.1 работни станции, преносими компютри, сървъри, защитни стени, комутатори, маршрутизатори и безжични точки за достъп

2.1.2 облачни услуги, използвани за бизнес операции (напр. електронна поща, съхранение на файлове, резервни копия, инструменти за сътрудничество)

2.1.3 функции за регистриране в антивирусен софтуер, приложения, операционни системи и мрежово оборудване

2.1.4 всички служители, външни изпълнители и доставчици на управлявани услуги (MSP), които използват или администрират системи

2.1.5 всяко място, на което се използват ИТ системи на дружеството, включително дистанционни, хибридни или BYOD среди

2.2 Политиката се прилага и за журнали, генерирани от услуги на трети страни, когато организацията има административен достъп или договорни права за одит.

3. Цели

3.1 Да се осигури регистриране на системна дейност, включително автентикация, промени в конфигурацията, достъп до чувствителни данни и предупреждения за сигурност

3.2 Да се поддържат защитени и точни журнали за откриване на нарушения на политиката, системни грешки или неоторизирани действия

3.3 Да се осигури своевременен преглед на журналите при инциденти, разследвания и одити

3.4 Да се поддържа синхронизация на времето с цел осигуряване на цялостност и корелация на журналните данни

3.5 Да се защитят журналите от подправяне, загуба или преждевременно изтриване

3.6 Да се изпълнят правните и регулаторните задължения за отчетност на системите, проследимост и реакция при нарушение на сигурността

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява настоящата политика и осигурява нейното прилагане във всички бизнес системи

4.1.2 Преглежда предупреждения с висока критичност и съществени одитни констатации, докладвани от ИТ или от функциите по защита на личните данни

4.1.3 Одобрява изключения, когато регистрирането или срокът за съхранение не могат да бъдат технически приложени

4.2 Доставчик на ИТ поддръжка / вътрешна ИТ функция

4.2.1 Внедрява и конфигурира регистриране за операционни системи, мрежови устройства, антивирусни инструменти и ключови приложения

4.2.2 Осигурява журналите да се съхраняват, архивират и защитават от промяна

4.2.3 Преглежда журналите по график и разследва подозрителна или неоторизирана дейност

4.2.4 Поддържа системи за предупреждение, които сигнализират за аномално поведение или индикатори за компрометиране

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

9. Преглед и актуализация на изискванията

9.1 Годишен преглед

9.1.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно от Управителя с подкрепата на доставчика на ИТ поддръжка и Координатора по поверителността.

9.2 Основания за преглед

9.2.1 Извънредни прегледи трябва да се извършват в отговор на:

9.2.1.1 констатации, свързани с журналите, от вътрешни или външни одити

9.2.1.2 инциденти по сигурността, при които журналите са липсвали, били са повредени или са били недостатъчни

9.2.1.3 съществени промени в ИТ инфраструктурата (напр. миграция към облачни платформи за регистриране)

9.2.1.4 промени в правните или регулаторните задължения (напр. GDPR, NIS2, DORA)

9.3 Управление на версиите

9.3.1 Всички промени по настоящата политика трябва да се регистрират с номер на версия, дата и обобщение на промените

9.3.2 Предходните версии трябва да се архивират и съхраняват за минимум 3 години

9.3.3 Актуализираните политики трябва да бъдат комуникирани на засегнатите заинтересовани страни, особено на лицата с достъп на системно ниво

10. Свързани политики и връзки

10.1 Настоящата политика пряко подпомага и се подпомага от следните SME политики по информационна сигурност:

10.1.1 P17S – Политика за защита на данните и поверителност: Осигурява журналните данни, съдържащи лична информация, да се управляват с мерки за цялостност, срокове за съхранение и контрол на достъпа в съответствие с изискванията на GDPR.

10.1.2 P21S – Политика за мрежова сигурност: Осигурява основата за събиране на журнали, свързани със защитни стени, безжичен достъп, VPN и мониторинг на сегментацията.

10.1.3 P24S – Политика за сигурна разработка: Осигурява журналите на приложенията (напр. за опити за вписване, грешки и изключения) да бъдат заложени в проектирането и експлоатацията на софтуера.

10.1.4 P30S – Политика за реагиране при инциденти: Разчита на точни и пълни журнални данни за откриване, анализ и реагиране на събития по информационната сигурност.

10.1.5 P23S – Политика за синхронизация на времето: Осигурява последователни и проследими времеви маркери във всички системи, което позволява корелация на журналите по време на разследвания.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Изисква внедряване на оперативни контроли за смекчаване на рисковете за информационната сигурност, включително регистриране.

11.2 ISO/IEC 27002

11.2.1 Контрол 8.15 – Изисква регистриране на събития за подпомагане на откриването на аномалии и отчетността.

11.2.2 Контрол 8.16 – Изисква защита на журналите от подправяне и неоторизиран достъп.

11.2.3 Контрол 8.17 – Изисква мониторинг на системите за необичайна дейност и потвърждаване на ефективността на контролите за мониторинг.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 до AU-12 – Обхващат съдържанието на одитните журнали, прегледа, съхранението и автоматизираните предупреждения.

11.3.2 SI-4 – Изисква откриване на системни аномалии и докладване на подозрителни събития.

11.4 GDPR на ЕС

11.4.1 Член 5(1)(f) – Изисква цялостност и поверителност на личните данни, което включва регистриране на достъпа.

11.4.2 Член 32 – Изисква технически и организационни мерки за осигуряване на сигурност, включително регистриране и мониторинг.

11.4.3 Член 33 – Изисква своевременно уведомяване при нарушение, подкрепено с журнали, които позволяват анализ на първопричините.

11.5 Директива NIS2 на ЕС

11.5.1 Член 21(2)(d) – Изисква механизми за регистриране, които откриват аномалии и подпомагат разследванията на инциденти.

11.5.2 Член 23 – Изисква докладване на инциденти в рамките на 24 часа, което зависи от точни и своевременни журнални данни.

11.6 DORA на ЕС

11.6.1 Член 10 – Изисква цифрова оперативна устойчивост, включително проследимост на инциденти, свързани с ИКТ, чрез регистриране.

11.6.2 Член 15 – Налага мониторинг на доставчиците на услуги, включително права за достъп до журнали и техния преглед.

11.7 COBIT 2019

11.7.1 DSS01.03 – Изисква проследимост на системната дейност чрез регистриране и мониторинг.

11.7.2 DSS05.02 – Разглежда регистрирането като ключов контрол за защита срещу зловреден софтуер и друга неоторизирана дейност.