					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P36S					Заглавие на документа: **Политика за социалните медии и външните комуникации**							
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 регулаторни изисквания

Стандарт/регулация	**Клауза/член**	**Коментар**
ISO/IEC 27001:2022	Клаузи 5.1, 5.2, 6.1, 8	Ръководство, управление на риска и оперативен контрол върху външните комуникации
ISO/IEC 27002:2022	Контроли 5.10, 5.11	Допустима употреба и информационна сигурност при комуникация
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Правила за поведение, одит, докладване на инциденти и управление на публично достъпно съдържание и достъп
GDPR на ЕС	Членове 5, 32, 33	Принципи за защита на данните, сигурност и уведомяване при нарушение, засягащо публична комуникация
NIS2 на ЕС	Член 21(2)(e), 21(2)(f)	Политики за използване на системи и управление на риска във веригата на доставки/публичните комуникации
DORA на ЕС	Член 14(4)	Задължения за комуникация след инциденти

1. Цел

1.1. Настоящата политика установява задължителни правила за всички публично достъпни комуникации, включително използването на социални медии, взаимодействието с медиите и външното цифрово съдържание, когато се споменава дружеството, неговият персонал, клиенти, системи или вътрешни практики.

1.2. Политиката подпомага защитата на репутацията на дружеството, поддържането на правно и регулаторно съответствие и намаляването на риска от изтичане на информация, дезинформация или инциденти по сигурността.

1.3. Тя дава възможност на служителите и партньорите да участват позитивно и отговорно в онлайн дискусии, като същевременно избягват случайно разкриване на информация или невярно представяне.

1.4. Политиката подпомага готовността на SME за сертифициране по ISO/IEC 27001, като урежда контрола върху информацията, предоставяна на обществеността или на външни заинтересовани страни.

2. Обхват

2.1. Настоящата политика се прилага за всички лица, свързани с организацията, включително:

2.1.1. Служители и външни изпълнители

2.1.2. Лица на свободна практика, консултанти и доставчици от трети страни

2.1.3. Стажанти или служители на непълно работно време, участващи в обслужване на клиенти или със системен достъп

2.2. Политиката се прилага за всички форми на външна комуникация, в които се споменава организацията, включително:

2.2.1. Публикации в социалните медии (LinkedIn, Twitter/X, TikTok, Instagram, Facebook и др.)

2.2.2. Публикации в блогове, онлайн форуми, клиентски отзиви и дискусионни теми

2.2.3. Публични участия (напр. конференции, уебинари, подкасти)

2.2.4. Имейли или съобщения до журналисти, представители на държавни институции или инфлуенсъри

2.2.5. Публично споделени екранни снимки, снимки или видеоклипове от работна среда

2.3. Политиката се прилага и когато такава комуникация е извършена:

2.3.1. От лични устройства или профили

2.3.2. Извън обичайното работно време

2.3.3. Без злонамерено намерение — дори случайни или направени „между другото“ изказвания попадат в обхвата, ако се отнасят до дружеството

3. Цели

3.1. Защита на репутацията: Предотвратяване на увреждане на имиджа на дружеството чрез неоторизирана или неподходяща публична комуникация

3.2. Сигурност на данните: Предотвратяване на непреднамерено разкриване на чувствителни данни, вътрешни системи или клиентски детайли чрез социални медии или публични канали

3.3. Правно и регулаторно съответствие: Осигуряване, че цялото публично съдържание, отнасящо се до дружеството, е в съответствие с приложимите изисквания за защита на данните и законодателството в областта на бизнес комуникациите

3.4. Професионално поведение: Насърчаване на отговорно участие в онлайн дискусии и медийни изяви, включително чрез лични профили

3.5. Готовност при инциденти: Осигуряване на ясни и приложими стъпки при случайно разкриване на информация или нарушения на политиката

4. Роли и отговорности

4.1. Управител (GM)

4.1.1. Притежава отговорността за тази политика и я одобрява

4.1.2. Преглежда и одобрява всички публични изявления, взаимодействия с медиите или интервюта

4.1.3. Осигурява политиката да бъде ясно комуникирана на всички служители и трети страни

4.1.4. Разследва и предприема действия по всички нарушения на тази политика в координация с процедурите за реагиране при инциденти

4.2. Определен служител или ръководител „Комуникации“ (ако е определен)

4.2.1. Подпомага GM чрез преглед на съдържание преди външно публикуване (напр. публикации в блогове, теми за публични изяви)

4.2.2. Поддържа регистър на одобрените медийни активности или публикации в социалните медии с висок риск

4.2.3. Следи известните онлайн споменавания на дружеството за репутационни рискове или рискове по сигурността, доколкото ресурсите позволяват

[... 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. Годишен преглед

9.1.1. Настоящата политика трябва да се преглежда поне веднъж годишно от Управителя (GM)

9.1.2. Прегледът трябва да осигури съответствие с актуализираните правни задължения, тенденциите в комуникацията в индустрията и вътрешните промени в дейността

9.2. Прегледи при настъпване на събитие

9.2.1. Настоящата политика трябва да бъде актуализирана незабавно след:

9.2.1.1. Значим инцидент в социалните медии или репутационен проблем

9.2.1.2. Смяна на доставчици от трети страни, които управляват комуникации

9.2.1.3. Ново законодателство или регулаторни задължения, свързани с онлайн комуникация, медии или брандинг

9.3. Документиране на промените

9.3.1. Всички актуализации трябва да бъдат документирани, включително дата на редакция, обобщение на промените и одобрение от GM

9.3.2. Трябва да се поддържа история на версиите за целите на одит и сертификация

9.4. Разпространение на актуализациите

9.4.1. Всички служители и външни изпълнители трябва да бъдат уведомявани за всички промени в политиката

9.4.2. Актуализираните версии трябва да бъдат споделяни по имейл или чрез вътрешни портали

9.4.3. Всеки доставчик на публични комуникации трябва да потвърди актуализираните условия, преди да продължи работа

10. Свързани политики и връзки

10.1. Настоящата политика се прилага в координация със следните политики на SME:

10.1.1. P3S – Политика за допустима употреба: Определя допустимото поведение при използване на комуникационни платформи, включително достъп до социални медии по време на работно време

10.1.2. P8S – Политика за информираност и обучение по информационна сигурност: Осигурява обучение на служителите за разпознаване на рисковете от прекомерно споделяне, фишинг или репутационни заплахи онлайн

10.1.3. P17S – Политика за защита на данните и поверителност: Осигурява личните данни и клиентските данни да не се споделят във външни комуникации в съответствие с GDPR и други правни изисквания

10.1.4. P30S – Политика за реагиране при инциденти: Урегулира реакцията при случайно публично разкриване, онлайн заплахи или репутационни атаки вследствие на неправомерно използване на социални медии

10.1.5. P37S – Политика за правно и регулаторно съответствие: Установява по-широките правни и договорни задължения на организацията при публично споделяне на съдържание

10.2. Тези политики трябва да се прилагат съвместно, за да се поддържа сигурно, професионално и законосъобразно външно присъствие.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 5.1 – Лидерство и ангажираност: Изисква надзор от ръководството върху репутационните и информационните рискове

11.1.2. Клауза 6.1 – Управление на риска: Включва рискови експозиции, свързани с комуникацията

11.1.3. Клауза 8.1 – Оперативен контрол: Обхваща правилата за външно комуникиране на информация

11.2. ISO/IEC 27002

11.2.1. Контрол 5.10 – Допустима употреба на информация и активи

11.2.2. Контрол 5.11 – Информационна сигурност при комуникация

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Правила за поведение: Регулира подходящото поведение при използване на информационни ресурси

11.3.2. AU-7 – Намаляване на одитните данни и генериране на отчети: Подпомага наблюдението на публичното използване на системи

11.3.3. IR-6 – Докладване на инциденти: Налага реакция при нарушения, свързани с репутацията и комуникацията

11.3.4. AC-22 – Публично достъпно съдържание: Осигурява контрол върху външните публикации и достъпа

11.4. GDPR на ЕС (2016/679)

11.4.1. Член 5 – Принципи, свързани с обработването на лични данни (точност, цялостност, отчетност)

11.4.2. Член 32 – Сигурност на обработването: Изисква предпазни мерки при публично споделяне

11.4.3. Член 33 – Уведомяване при нарушение: Прилага се, ако лични данни са разкрити чрез външна комуникация

11.5. Директива NIS2 на ЕС (2022/2555)

11.5.1. Член 21(2)(e) – Политики за използване на информационни системи, включително комуникационни платформи

11.5.2. Член 21(2)(f) – Политики за управление на киберрискове във веригата на доставки и в публични платформи

11.6. DORA на ЕС (2022/2554)

11.6.1. Член 14(4) – Задължения за комуникация към клиенти, трети страни и органи след оперативни инциденти

11.7. COBIT 2019

11.7.1. APO09 – Управление на споразумения за услуги: Обхваща надзора върху доставчици и трети страни, свързани с комуникации

11.7.2. DSS05 – Управление на услугите по сигурността: Включва защита на публично достъпни цифрови активи

11.7.3. EDM03 – Осигуряване на оптимизацията на риска: Подчертава управлението на репутационни рискове и рискове по съответствието, свързани с комуникацията