					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P36					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 регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	Дефинирани процеси и управление, базирано на роли, за управление на публичните комуникации, осигуряващи точност, работни потоци за одобрение и ескалация при инциденти.
ISO/IEC 27002:2022	Контроли 5.10, 5.11, 5.35, 5.36	Регламентира използването, допустимата употреба, външната комуникация с органи/компетентни институции и докладването във връзка със съответствието.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Правила за използване на системи и комуникации, уведомления към потребителите и съхранение на одитни записи.
GDPR на ЕС	Членове 5, 25, 32, 33	Принципи за обработване на данни, защита на личните данни още при проектирането, сигурност на обработването и задължения за уведомяване при нарушения.
NIS2 на ЕС	Член 21	Мерки за управление на риска за киберсигурността, задължения при инциденти и публични съобщения, свързани с риска.
DORA на ЕС	Членове 9, 16	Управление на ИКТ риска и комуникационна стратегия за критични доставчици.
COBIT 2019	APO09, DSS05	Управление на споразуменията за услуги и комуникациите и практики за сигурна комуникация и управление на инциденти.

1. Цел

1.1 Настоящата политика установява задължителни правила и отговорности, уреждащи използването на социални медии и всички форми на външна комуникация от персонал, свързан с организацията.

1.2 Тя гарантира, че публичните послания — независимо дали са планирани или спонтанни — са точни, уважителни, сигурни, в съответствие с приложимите правни изисквания и съобразени с корпоративната идентичност.

1.3 Политиката има за цел да сведе до минимум рисковете, свързани с репутационни щети, регулаторни нарушения, изтичане на интелектуална собственост и неразрешено разкриване чрез публично достъпни канали.

1.4 Политиката също така насърчава отчетност и структурирано управление при всички форми на цифрова комуникация, които включват или засягат организацията.

2. Обхват

2.1 Настоящата политика се прилага за всички служители, външни изпълнители, стажанти и представители на трети страни, които:

2.1.1 комуникират от името на организацията, официално или неформално;

2.1.2 посочват или създават впечатление за принадлежност към организацията в публична среда;

2.1.3 използват лични или корпоративни акаунти за участие в публични дискусии, свързани с организацията.

2.2 Обхванатите комуникационни канали включват, но не се ограничават до:

2.2.1 платформи за социални медии (напр. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook);

2.2.2 блогове, уикита, форуми и публични дискусионни платформи;

2.2.3 електронна поща или директни съобщения до външни страни (напр. клиенти, регулатори, медии);

2.2.4 интервюта за пресата, участия в дискусионни панели или записани медийни изяви;

2.2.5 участие в онлайн общности, в които се споменава организацията.

2.3 Настоящата политика урежда както съдържание в реално време, така и предварително планирано съдържание и се прилага за всички устройства и акаунти (лични или корпоративни), използвани за разпространение на комуникацията.

3. Цели

3.1 Да предотвратява случайното или умишленото разкриване на поверителна, чувствителна или регулирана информация чрез външни комуникационни канали.

3.2 Да гарантира, че официалните публични изявления и съдържанието в социалните медии са точни, разрешени и съгласувани с корпоративната идентичност, етичните принципи и стратегическите комуникационни послания.

3.3 Да предотвратява репутационни щети и да осигурява последователност на посланията между вътрешните звена и външните платформи.

3.4 Да осигурява съответствие с приложимите правни задължения, свързани с публични изявления, включително, но не само, GDPR, NIS2, DORA и секторно-специфични правила за комуникация.

3.5 Да определя ясни отговорности, допустими случаи на използване и правила за прилагане за целия персонал, ангажиран с публично видими дейности.

4. Роли и отговорности

4.1 Директор „Маркетинг“ или „Комуникации“ / Ръководител „Връзки с обществеността“

4.1.1 Одобрява всички официални фирмени послания за външно публикуване.

4.1.2 Поддържа графици за съдържанието в социалните медии и указания за последователно прилагане на корпоративната идентичност.

4.1.3 Следи онлайн споменаванията и медийното отразяване, свързани с организацията.

4.2 Директор по информационна сигурност (CISO) / екипи по ИТ и информационна сигурност

4.2.1 Следи цифровите платформи за индикатори за изтичане на данни, представяне под чужда самоличност или опити за фишинг.

4.2.2 Координира действията с екипите за реагиране при инциденти при атаки или нарушения, свързани със социални медии.

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

9. Прилагане и съответствие

9.1 Настоящата политика е задължителна за целия обхванат персонал и трети страни. Неспазването ѝ може да доведе до:

9.1.1 официални предупреждения;

9.1.2 временно или постоянно отнемане на достъп до платформи или системи;

9.1.3 дисциплинарни мерки, включително прекратяване;

9.1.4 съдебни производства, ако външната комуникация доведе до репутационни щети, нарушение на сигурността на данните или регулаторно несъответствие.

9.2 Дисциплинарни мерки

9.2.1 Вътрешни нарушения (напр. изтичане на поверителни данни, клеветнически твърдения срещу организацията) водят до намеса на Човешки ресурси (ЧР), формално разследване и документиране в досието на служителя.

9.2.2 Когато е приложимо, правният отдел предприема гражданскоправни средства за защита или уведомява компетентните органи за престъпна дейност (напр. представяне под чужда самоличност, изтичане на вътрешна информация за сделки).

9.3 Мониторинг на съответствието

9.3.1 Екипите по сигурност и комуникации трябва да извършват текущ мониторинг на:

9.3.1.1 споменавания на бранда в основните платформи;

9.3.1.2 неофициално използване на фирмени изображения или търговски марки;

9.3.1.3 известни рискове (напр. недоволни служители, опити за представяне под чужда самоличност).

9.3.2 Мониторингът трябва да се извършва в съответствие със законите и регулациите относно поверителността на служителите, като всички маркирани случаи се потвърждават чрез човешки преглед.

9.4 Докладване чрез механизъм за подаване на сигнали за нарушения и неправомерно използване

9.4.1 Всеки служител, който подозира нарушение на настоящата политика, следва да го докладва на екипа по информационна сигурност, правния отдел или анонимно чрез портала за подаване на сигнали.

9.4.2 Ответни действия срещу податели на сигнали са строго забранени и подлежат на незабавни дисциплинарни мерки.

10. Преглед и актуализация на изискванията

10.1 Настоящата политика трябва да се преглежда ежегодно или по-рано, ако:

10.1.1 има съществени промени в регулаторните изисквания (напр. нови законодателни актове на ЕС относно цифровите комуникации);

10.1.2 бъдат въведени нови социални платформи или комуникационни канали;

10.1.3 има значим инцидент или повтарящи се нарушения, които сочат пропуски в процесите;

10.1.4 има структурна промяна или промяна в ръководството на функциите по PR, правни въпроси или сигурност.

10.2 Прегледът трябва да се извършва съвместно от:

10.2.1 ръководителя на маркетинг / PR;

10.2.2 CISO или ръководителя по риска за сигурността;

10.2.3 длъжностните лица по правни въпроси и съответствие.

10.3 Актуализациите трябва да бъдат документирани в Регистъра на промените в политиките и комуникирани чрез вътрешните канали за осведоменост. При съществени промени целият засегнат персонал трябва повторно да предостави потвърждение за запознаване с политиката.

11. Свързани политики и връзки

11.1 Настоящата политика се поддържа от и е взаимосвързана със следните компоненти на Системата за управление на информационната сигурност (СУИС) на организацията:

11.1.1 P1 – Политика за информационна сигурност: Установява общите принципи за защита на информацията, включително гарантиране, че комуникациите не водят до неоторизирано разкриване.

11.1.2 P3 – Политика за допустима употреба: Определя допустимото поведение при използване на цифрови платформи и технологии, което пряко урежда личното и професионалното използване на социални канали.

11.1.3 P6 – Политика за управление на риска: Осигурява рамката за оценка на риска при заплахи, свързани с публичната комуникация и репутационната експозиция.

11.1.4 P8 – Политика за информираност и обучение по информационна сигурност: Установява задължителни програми за осведоменост, които обучават персонала на практики за сигурна комуникация и заплахи от социално инженерство.

11.1.5 P13 – Политика за класификация и етикетиране на данни: Насочва персонала какво представлява Ограничена или Поверителна информация, която не трябва да се разкрива външно.

11.1.6 P30 – Политика за реагиране при инциденти: Определя как да се обработват инциденти, свързани с публична комуникация, включително изтичане на данни, представяне под чужда самоличност и регулаторни нарушения.

11.1.7 P33 – Политика за одит и мониторинг на съответствието: Урегулира одитните процеси, които валидират контролите за социални медии, системите за мониторинг и съответствието с политиките за външна комуникация.

12. Референтни стандарти и рамки

12.1 ISO/IEC 27001:

12.1.1 Клауза 8.1 – Оперативно планиране и контрол: Изисква дефинирани процеси и управление, базирано на роли, за управление на публичните комуникации, като осигурява точност, работни потоци за одобрение и ескалация на инциденти, свързани с данни или репутационен риск.

12.2 ISO/IEC 27002:2022:

12.2.1 Контрол 5.10 – Използване на информация: Регулира разрешеното и етично разпространение на вътрешни или външни комуникации.

12.2.2 Контрол 5.11 – Допустимо използване на корпоративни активи: Подсилва допустимите практики за споделяне на съдържание чрез корпоративни активи или лични акаунти.

12.2.3 Контрол 5.35 – Контакт с органи: Изисква структурирана и разрешена външна комуникация с регулаторни органи и публични институции.

12.2.4 Контрол 5.36 – Съответствие с политики и стандарти: Изисква последователно прилагане на вътрешните политики във всички комуникационни сценарии.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Правила за поведение: Изисква формални правила за използване на системи и комуникации, включително стандарти за публично разкриване.

12.3.2 AC-8 – Уведомление за използване на системата: Подпомага задължителни откази от отговорност и предупреждения за съдържание във външно насочени платформи.

12.3.3 AU-12 – Съхранение на одитни записи: Прилага се за запазването на журнали и история на комуникациите за преглед при инциденти и за целите на одита.

12.4 GDPR на ЕС (2016/679):

12.4.1 Член 5 – Принципи на обработването на данни: Забранява неоторизираното споделяне на лични данни чрез публична комуникация.

12.4.2 Член 25 – Защита на данните още при проектиране и по подразбиране: Изисква предпазни мерки за поверителност в комуникационните инструменти и работните процеси за съдържание.

12.4.3 Член 32 – Сигурност на обработването: Прилага криптиране, контрол на достъпа и процеси по одобрение на съдържание.

12.4.4 Член 33 – Уведомяване при нарушение: Налага своевременно оповестяване на изтичания на лични данни чрез публични канали.

12.5 Директива NIS2 на ЕС (2022/2555):

12.5.1 Член 21 – Мерки за управление на риска за киберсигурността: Включва комуникационни протоколи и задължения при инциденти и публични съобщения, свързани с риска.

12.6 DORA на ЕС (2022/2554):

12.6.1 Член 9 – Управление на ИКТ риска: Прилага се за външно предизвикани комуникационни рискове, като представяне под чужда самоличност, дезинформация и репутационни смущения.

12.6.2 Член 16 – Комуникационна стратегия: Изисква критичните финансови доставчици или доставчици на услуги да управляват комуникационните рискове и реакциите в кризисни сценарии.

12.7 COBIT 2019:

12.7.1 APO09 – Управлявани споразумения за услуги и комуникация: Изисква структурирано управление на вътрешните и външните комуникации.

12.7.2 DSS05 – Управление на услугите по сигурност: Осигурява комуникационните дейности да не въвеждат допълнителен риск и да не подкопават процесите по обработване на инциденти.