

ПОЛІТИКА

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ

[НАЗВА КОМПАНІЇ]

18 серпня 2026 року

Затверджено	[наказ / рішення, дата, номер]
Власник документа	[маркетинг / комунікації / HR / юридичний відділ]
Відповідальна особа	[ПІБ, посада, контакт]
Дата набрання чинності	[дд.мм.рррр]
Наступний перегляд	[дд.мм.рррр або не рідше одного разу на рік]

Статус: шаблон для адаптації та затвердження всередині компанії

ПЕРЕД ЗАТВЕРДЖЕННЯМ

Заповніть усі поля у квадратних дужках, внесіть перелік офіційних акаунтів і затверджених каналів комунікації, а також погодьте документ із відповідальними за HR, інформаційну безпеку, комунікації та юридичні питання. Цей шаблон не замінює індивідуальної юридичної консультації.

Зміст

1. Мета, сфера дії та статус документа
2. Що вважається соціальними мережами
3. Основні принципи
4. Офіційне використання соціальних мереж
5. Особисте використання працівниками
6. Вимоги до змісту публікацій
7. Спеціальні правила в умовах війни
8. Персональні дані, конфіденційність та інтелектуальна власність
9. Мова, реклама та доступність контенту
10. Кібербезпека та управління доступами
11. Використання в робочий час і питання приватності
12. Реагування на помилки, кризи та злам акаунтів
13. Повідомлення про порушення та відповідальність
14. Прикінцеві положення

Додаток 1. Швидкий чекліст перед публікацією

Додаток 2. Матриця погодження контенту

Додаток 3. Підтвердження ознайомлення працівника

Нормативна та методична основа

1. Мета, сфера дії та статус документа

Соціальні мережі дають змогу працівникам і компаніям спілкуватися з клієнтами, партнерами, професійними спільнотами, друзями та родиною. Водночас необережна публікація може спричинити витік конфіденційної інформації, порушення прав інших осіб, репутаційну шкоду, кіберінцидент або юридичну відповідальність.

Ця Політика встановлює правила офіційного використання соціальних мереж від імені [НАЗВА КОМПАНІЇ] (далі — Компанія), а також правила особистого використання соціальних мереж працівниками у випадках, коли таке використання пов'язане з Компанією, її клієнтами, партнерами, працівниками або службовою інформацією.

Політика поширюється на штатних працівників, керівників, стажерів, підрядників, консультантів і інших осіб, які отримали доступ до офіційних акаунтів або можуть діяти від імені Компанії. Для підрядників відповідні вимоги мають бути включені до договорів або окремих зобов'язань про конфіденційність.

У разі суперечності між цією Політикою, законодавством України, трудовим або цивільно-правовим договором, колективним договором чи іншими обов'язковими внутрішніми документами застосовуються норми вищої юридичної сили та спеціальні правила, що регулюють конкретну ситуацію.

2. Що вважається соціальними мережами

Для цілей цієї Політики поняття «соціальні мережі» використовується широко та охоплює публічні й напівпублічні цифрові платформи, месенджери, сервіси спільнот, майданчики для публікації контенту та спільного доступу до матеріалів. Перелік не є вичерпним.

Категорія	Актуальні приклади
Соціальні платформи	Facebook, Instagram, LinkedIn, TikTok, X, Threads, Bluesky, Snapchat.
Відео, стрими та аудіо	YouTube, Twitch, Vimeo, Spotify, Apple Podcasts, SoundCloud та інші подкаст-платформи.
Месенджери та спільноти	Telegram, Viber, WhatsApp, Signal, Messenger, Discord, а також публічні канали, чати й групи у цих сервісах.
Блоги, форуми та авторські платформи	Reddit, Medium, Substack, WordPress, Blogger та тематичні форуми.
Візуальні та довідкові платформи	Pinterest, Google Business Profile / Google Maps, сервіси відгуків, маркетплейси та каталоги.
Спільна робота і поширення файлів	Google Workspace / Drive / Docs, Microsoft 365 / OneDrive / SharePoint, Dropbox, Notion, Miro, Figma, Canva та інші сервіси, якщо матеріал доступний зовнішнім особам або може бути поширений за посиланням.

ВАЖЛИВО

Офіційні акаунти та службові комунікації не повинні вестися через ресурси, використання яких заборонене або обмежене законодавством України, санкційними рішеннями чи внутрішніми правилами безпеки Компанії. Для службової роботи використовуються лише затверджені Компанією платформи.

3. Основні принципи

- **Законність.** Дотримуйтеся законодавства України, правил платформи, договорів і внутрішніх документів Компанії.
- **Відповідальність.** Пам'ятайте, що публікація може бути скопійована, заархівована, процитована або поширена навіть після видалення.
- **Точність.** Перевіряйте факти, цифри, імена, дати, посилання та джерела. Помилки виправляйте відкрито й оперативно.
- **Повага.** Не допускайте погроз, цькування, дискримінаційних висловлювань, мови ворожнечі, приниження гідності або навмисного переслідування.
- **Конфіденційність.** Не публікуйте службову, комерційну, клієнтську або персональну інформацію без належної правової підстави та дозволу.
- **Безпека.** Захищайте акаунти, перевіряйте посилання, не передавайте паролі і негайно повідомляйте про підозрілі дії.
- **Прозорість.** Чітко розмежовуйте офіційну позицію Компанії, особисту думку працівника та рекламний або партнерський контент.
- **Професійне судження.** Якщо законність, безпечність або доречність публікації викликає сумнів — зупиніться й зверніться до [ВІДПОВІДАЛЬНОЇ ОСОБИ / ВІДДІЛУ].

4. Офіційне використання соціальних мереж

4.1. Власність і повноваження

Усі офіційні акаунти, сторінки, канали, спільноти, рекламні кабінети, підписники, контакти, листування, статистика, контент, доменні імена та інші цифрові активи, створені або придбані для Компанії, належать Компанії або використовуються нею на законних підставах.

Створювати офіційні акаунти, публікувати від імені Компанії, відповідати медіа, запускати рекламу або робити публічні заяви можуть лише особи, яким це прямо доручено посадовою інструкцією, наказом, договором або письмовим погодженням.

Особистий номер телефону, особиста електронна пошта чи особистий акаунт працівника не повинні бути єдиним засобом відновлення доступу до корпоративного акаунта. Компанія має зберігати актуальний реєстр власників, адміністраторів і способів відновлення доступу.

4.2. Перелік офіційних акаунтів

Платформа	Посилання / @username	Власник процесу	Адміністратори
[платформа]	[посилання]	[відділ / ПІБ]	[ПІБ / роль]
[платформа]	[посилання]	[відділ / ПІБ]	[ПІБ / роль]
[платформа]	[посилання]	[відділ / ПІБ]	[ПІБ / роль]
[платформа]	[посилання]	[відділ / ПІБ]	[ПІБ / роль]
[платформа]	[посилання]	[відділ / ПІБ]	[ПІБ / роль]
[платформа]	[посилання]	[відділ / ПІБ]	[ПІБ / роль]

4.3. Погодження та публікація

- Дотримуйтеся затвердженої комунікаційної стратегії, брендбуку, tone of voice, контент-плану та матриці погодження.
- Перед публікацією перевірте текст, візуали, субтитри, посилання, згадки, теги, геолокацію, авторські права та наявність потрібних згод.
- Фінансові результати, юридичні спори, кадрові рішення, кризові події, політичні заяви, питання безпеки та інша чутлива інформація публікуються лише після окремого погодження.
- Публікації від імені Компанії мають зберігатися у корпоративному архіві або системі планування контенту разом із фінальною версією матеріалів і даними про погодження.
- Коментарі та приватні повідомлення обробляються відповідно до затверджених сценаріїв. Не обіцяйте клієнту те, що не уповноважені виконати.

4.4. Модерація та взаємодія

Компанія може модерувати коментарі на власних ресурсах за оприлюдненими правилами спільноти. Допускається приховування або видалення спаму, шахрайства, незаконного контенту, погроз, розкриття персональних даних, мови ворожнечі та інших матеріалів, що порушують правила платформи чи закон. Обґрунтована критика не видаляється лише через її негативний характер.

У конфліктних ситуаціях не вступайте в емоційні суперечки. Зафіксуйте повідомлення, передайте його відповідальній особі та продовжуйте комунікацію за погодженим сценарієм.

5. Особисте використання працівниками

Компанія поважає право працівників на приватне життя, свободу висловлювань і особисте користування соціальними мережами поза межами виконання трудових обов'язків. Працівник не зобов'язаний публікувати, поширювати або підтримувати контент Компанії зі свого особистого акаунта, якщо інше прямо не передбачено його роботою та законною домовленістю.

Водночас особистий акаунт не звільняє від обов'язків щодо нерозголошення конфіденційної інформації, захисту персональних даних, дотримання авторських прав і недопущення неправдивого представлення себе як офіційного речника Компанії.

- Якщо Ви згадуєте місце роботи або професійно коментуєте тему, пов'язану з діяльністю Компанії, чітко зазначайте, що висловлюєте особисту думку, якщо інше не входить до Ваших повноважень.
- Рекомендоване застереження: «Це моя особиста думка, яка може не збігатися з позицією [НАЗВА КОМПАНІЇ]». Саме застереження не виправдовує порушення закону або розголошення таємниці.
- Не використовуйте логотип, фірмовий стиль, службове посвідчення, форму, офіс або інші ознаки Компанії для особистої реклами, політичної агітації, збору коштів чи підтримки сторонніх товарів без дозволу.
- Не створюйте враження, що особистий профіль, канал або проєкт належить Компанії чи офіційно нею схвалений.
- Не публікуйте скриншоти службових чатів, внутрішніх листів, робочих зустрічей, CRM, таск-менеджерів, аналітики або документів навіть із закритих груп без дозволу.
- Робочий конфлікт варто спочатку вирішувати через керівника, HR, процедуру повідомлення про порушення або інший внутрішній механізм. Це не обмежує право особи законно звертатися до державних органів, профспілки, адвоката чи повідомляти про правопорушення.

6. Вимоги до змісту публікацій

6.1. Заборонений або обмежений контент

- завідомо неправдива інформація, сфабриковані цитати, маніпулятивні монтажі або неперевірені чутки, що можуть зашкодити Компанії чи третім особам;
- погрози, заклики до насильства, переслідування, мобінг, булінг, сексуальні домагання, дискримінаційні висловлювання або мова ворожнечі;
- наклепницькі твердження, образи, приниження честі, гідності чи ділової репутації;
- контент, який порушує авторські, суміжні, торговельні або інші права інтелектуальної власності;
- персональні дані, медична інформація, документи, адреси, контакти, банківські реквізити, паролі або інші дані без належної правової підстави;
- комерційна таємниця, фінансові прогнози, непублічні договори, переговори, ціни, клієнтські бази, внутрішні звіти, стратегії, плани запусків і юридичні матеріали;
- прихована реклама, замовчування істотного комерційного зв'язку, фальшиві відгуки або штучне введення аудиторії в оману;
- контент від імені Компанії, створений або істотно змінений за допомогою ШІ, якщо він містить неперевірені факти, вигадані джерела, неправдиве зображення реальної особи або несанкціоновану імітацію голосу чи зовнішності.

6.2. Чесність, виправлення та джерела

Використовуйте першоджерела, офіційні повідомлення або надійні медіа. У разі помилки не намагайтеся приховати її так, щоб аудиторія була введена в оману: виправте публікацію, додайте уточнення або опублікуйте спростування залежно від масштабу помилки.

Не видавайте припущення за факт. Якщо інформація є попередньою, прогнозною, рекламною, партнерською або створеною на основі обмежених даних — позначте це зрозуміло для аудиторії.

7. Спеціальні правила в умовах війни

ПРАВИЛО БЕЗПЕКИ

Не публікуйте інформацію, яка може допомогти ворогу встановити місце, час, маршрут, склад або наслідки дій Сил оборони, екстрених служб, критичної інфраструктури чи працівників Компанії. Навіть звичайне фото може містити геолокацію, номер будинку, орієнтири або метадані.

- Не публікуйте в реальному часі фото, відео або текстові описи переміщення, розташування чи ідентифікації військових підрозділів, техніки, озброєння, блокпостів, складів або логістичних маршрутів.
- Не показуйте роботу ППО, місця її розміщення, траєкторії ракет або дронів, точні точки влучань, орієнтири чи панорами, що дають змогу визначити координати.
- Не транслюйте наживо місце обстрілу, рятувальної операції або наслідки атаки до оприлюднення інформації уповноваженими державними органами та без дозволу відповідальної особи.
- Не публікуйте деталі про стан і вразливості об'єктів критичної інфраструктури, енергосистеми, зв'язку, водопостачання, виробництва чи укриттів, якщо це створює ризик безпеці.
- Перед публікацією матеріалів із військовими, пораненими, загиблими, полоненими, зниклими безвісти або їхніми родинами перевіряйте законність, етичність, наявність згод і правила уповноважених органів.
- Для повідомлень про війну використовуйте офіційні джерела: Генеральний штаб ЗСУ, Міністерство оборони, ДСНС, СБУ, органи місцевої влади та інші уповноважені органи. Не поширюйте анонімні «інсайди» без перевірки.
- Не додавайте геолокацію та перевіряйте, чи не містять файли метаданих, які розкривають місце зйомки. За потреби публікацію відкладають до усунення ризику.
- Під час повітряної тривоги, евакуації або іншої небезпеки пріоритетом є життя і безпека, а не створення контенту.

Несанкціоноване поширення окремих відомостей про переміщення зброї, військових формувань або їх розташування в умовах воєнного чи надзвичайного стану може мати ознаки кримінального правопорушення. У разі сумніву публікацію слід зупинити та передати на перевірку.

8. Персональні дані, конфіденційність та інтелектуальна власність

8.1. Персональні дані

Не публікуйте персональні дані без визначеної мети, належної правової підстави та дотримання принципу мінімізації. Навіть інформація, яка окремо здається незначною, у поєднанні з іншими даними може ідентифікувати людину або створити для неї ризик.

- ПІБ разом із номером телефону, електронною адресою, адресою проживання, датою народження, документами або фінансовими реквізитами;
- дані про здоров'я, інвалідність, лікування, біометрію, сімейні обставини або інші чутливі відомості;
- фото і відео працівників, клієнтів, відвідувачів або дітей, якщо немає належної підстави, повідомлення та, коли потрібно, згоди;
- списки учасників, реєстраційні форми, резюме, записи дзвінків, скриншоти листування або дані з CRM;

Працівники, які мають доступ до персональних даних у зв'язку з роботою, зобов'язані не розголошувати їх і використовувати лише в межах наданих повноважень.

8.2. Конфіденційна інформація та комерційна таємниця

До конфіденційної інформації можуть належати неопублічні фінансові дані, ціни, умови договорів, пропозиції, клієнтські бази, технічні рішення, вихідні файли, паролі, ключі доступу, внутрішні правила, аналітика, плани маркетингу, майбутні продукти, кадрові рішення, юридичні спори та переговори. Конкретний перелік визначається договорами і внутрішніми документами Компанії.

Якщо Ви не впевнені, чи є інформація публічною, вважайте її неопублічною до підтвердження відповідальною особою.

8.3. Авторське право, бренди та контент третіх осіб

- Використовуйте лише контент, який створено Компанією, ліцензовано, придбано, надано з дозволу або правомірно використовується на іншій підставі.
- Зазначення автора саме по собі не завжди дає право копіювати фото, музику, відео, текст, дизайн або програмний код.
- Перевіряйте умови стоків, музичних бібліотек, шаблонів, шрифтів, генеративних сервісів та матеріалів із відкритими ліцензіями.
- Не завантажуйте конфіденційні матеріали Компанії або клієнтів до зовнішніх ШІ-сервісів, якщо це не дозволено окремою політикою та договором із постачальником.
- Торговельні марки, логотипи партнерів і клієнтів використовуються лише у погодженому контексті та форматі.

9. Мова, реклама та доступність контенту

9.1. Мова офіційних сторінок

Офіційні сторінки та публічна інформація Компанії, орієнтована на споживачів в Україні, ведуться українською мовою відповідно до вимог законодавства. Інші мовні версії можуть додаватися для міжнародних аудиторій, експорту, партнерів або конкретних кампаній, але не повинні погіршувати доступність української версії там, де вона є обов'язковою.

Мовою реклами в Україні є державна мова з урахуванням передбачених законом винятків, зокрема для об'єктів права інтелектуальної власності. Перед запуском іншомовної кампанії перевірте цільову територію, аудиторію та юридичні вимоги.

9.2. Рекламний і партнерський контент

Реклама, спонсорство, бартер, партнерські посилання, подарунки, амбасадорство та інші комерційні відносини мають бути позначені зрозуміло для аудиторії. Не маскуйте рекламу під незалежну рекомендацію або особистий досвід, якщо існує матеріальна зацікавленість.

Працівник не має права приймати винагороду за рекомендацію товарів, послуг або партнерів від імені Компанії без погодження та врегулювання потенційного конфлікту інтересів.

9.3. Доступність

- Додавайте субтитри до відео та перевіряйте їхню точність.
- За можливості додавайте альтернативний текст до зображень і зрозумілі описи посилань.
- Не покладайтеся лише на колір для передачі важливої інформації; забезпечуйте читабельний контраст і достатній розмір тексту.
- Не використовуйте надмірно миготливий контент, який може бути небезпечним для чутливих користувачів.

10. Кібербезпека та управління доступами

10.1. Обов'язкові заходи

- Увімкніть багатофакторну автентифікацію для всіх корпоративних акаунтів. Перевага надається застосунку-автентифікатору або фізичному ключу безпеки, якщо платформа це підтримує.
- Використовуйте унікальні складні паролі та затверджений менеджер паролів. Заборонено передавати паролі у відкритому вигляді через чати, електронну пошту або таблиці.
- Реєструйте корпоративні акаунти на службову електронну пошту та корпоративний номер або інший контрольований Компанією спосіб відновлення.
- Надавайте мінімально необхідні ролі. Не передавайте повні права адміністратора, якщо достатньо ролі редактора, рекламодавця або аналітика.
- Регулярно перевіряйте активні сесії, підключені застосунки, резервні коди, способи відновлення та список адміністраторів.

- Не переходьте за підозрілими посиланнями та не вводьте пароль після переходу з повідомлення без перевірки домену. Запити «терміново підтвердити сторінку» часто є фішингом.
- На особистих пристроях, з яких дозволено працювати з корпоративними акаунтами, мають бути встановлені блокування екрана, актуальні оновлення та засоби захисту, визначені Компанією.
- Конфіденційна інформація передається лише через затверджені Компанією системи. Звичайний чат у месенджері не вважається автоматично захищеним каналом.

10.2. Зміна ролі або припинення співпраці

У день зміни обов'язків або завершення співпраці Компанія має відкликати непотрібні доступи, змінити спільні секрети, перевірити способи відновлення та зафіксувати передачу цифрових активів. Працівник зобов'язаний передати всі матеріали, резервні коди та іншу інформацію, необхідну для безперервної роботи.

11. Використання в робочий час і питання приватності

Особисте користування соціальними мережами у робочий час допускається в межах, установлених правилами внутрішнього трудового розпорядку, якщо воно не перешкоджає роботі, не створює ризиків безпеки та не суперечить законним розпорядженням роботодавця. Перерви та неробочий час регулюються окремо.

Не використовуйте службову електронну адресу для реєстрації особистих профілів, підписок або сервісів, якщо це не дозволено Компанією.

Корпоративні пристрої, мережі, пошта та акаунти призначені насамперед для роботи. Компанія може вести технічні журнали, контролювати безпеку та перевіряти використання корпоративних систем лише на законній підставі, у пропорційний спосіб і після належного інформування працівників. Ця Політика не надає Компанії автоматичного права вимагати пароль від особистого акаунта або отримувати доступ до приватного листування без законної підстави.

Публічно доступний контент може стати відомим колегам, клієнтам або партнерам незалежно від налаштувань приватності. Водночас рішення щодо працівника не повинні ґрунтуватися на дискримінації, законній приватній активності або реалізації права повідомляти про порушення.

12. Реагування на помилки, кризи та злам акаунтів

12.1. Помилка у публікації

- Не приховуйте помилку і не сперечайтесь з аудиторією від імені Компанії без погодження.
- Зробіть скриншот, збережіть посилання та зафіксуйте час публікації.
- Негайно повідомте [КЕРІВНИКА / КОМУНІКАЦІЇ / ЮРИСТА] і виконуйте погоджений план: редагування, видалення, уточнення, спростування або вибачення.
- Якщо помилка стосується персональних даних, безпеки, військової інформації чи конфіденційних матеріалів, додатково повідомте [ВІДПОВІДАЛЬНОГО ЗА ЗАХИСТ ДАНИХ / ІНФОРМАЦІЙНУ БЕЗПЕКУ].

12.2. Підозра на злам або шахрайство

- Не видаляйте докази до їх фіксації, якщо це не потрібно для негайного припинення шкоди.
- Завершіть сторонні сесії, змініть пароль, перевірте способи відновлення та підключені застосунки з безпечного пристрою.
- Повідомте відповідальну особу та платформу. За потреби попередьте аудиторію лише через перевірений канал.
- Не сплачуйте викуп і не ведіть самостійні переговори зі зловмисником від імені Компанії.

12.3. Кризова комунікація

Під час кризової події право публічно коментувати ситуацію мають лише визначені речники. Інші працівники передають запити медіа та публічні звернення на [КОНТАКТ]. За потреби Компанія тимчасово зупиняє заплановані публікації та рекламу, щоб уникнути недоречної автоматичної комунікації.

13. Повідомлення про порушення та відповідальність

13.1. Куди повідомляти

Комунікації / маркетинг	[ПІБ, e-mail, телефон]
HR / трудові питання	[ПІБ, e-mail, телефон]
Інформаційна безпека	[ПІБ, e-mail, телефон / канал інцидентів]
Юридичні питання / персональні дані	[ПІБ, e-mail, телефон]
Конфіденційне повідомлення про порушення	[канал / форма / e-mail]

13.2. Заборона переслідування

Заборонено переслідувати, погрожувати або застосовувати негативні заходи до особи лише через добросовісне повідомлення про можливе порушення цієї Політики, участь у перевірці або законне звернення до уповноважених органів.

13.3. Наслідки порушення

Порушення розглядаються з урахуванням обставин, наслідків, умислу, повторності та вимог законодавства. До працівника можуть застосовуватися передбачені законом і внутрішніми документами заходи, включно з навчанням, обмеженням доступу, вимогою усунути порушення, дисциплінарною відповідальністю у порядку, встановленому трудовим законодавством, а також матеріальною, цивільною, адміністративною чи кримінальною відповідальністю за наявності правових підстав.

Формулювання цієї Політики не є самостійною підставою для звільнення або іншого стягнення поза процедурою, установлену законодавством і трудовими документами.

14. Прикінцеві положення

- Політика набирає чинності з дати, визначеної у наказі або рішенні про її затвердження.
- Працівники ознайомлюються з Політикою під підпис або в інший спосіб, який дає змогу підтвердити факт ознайомлення.
- Політика переглядається не рідше одного разу на рік, а також після суттєвих змін законодавства, платформ, структури Компанії або кіберінцидентів.
- Поточна версія зберігається за адресою: [ПОСИЛАННЯ НА ВНУТРІШНІЙ РЕСУРС]. Застарілі копії мають бути вилучені з використання або чітко позначені.
- Питання, не врегульовані цією Політикою, вирішуються відповідно до законодавства України, договорів та інших внутрішніх документів Компанії.

Додаток 1. Швидкий чекліст перед публікацією

✓	Перевірка	Контрольне запитання
☐	Повноваження	Чи маю я право публікувати це від імені Компанії?

✓	Перевірка	Контрольне запитання
☐	Факти	Чи перевірені імена, дати, цифри, цитати, посилання та джерела?
☐	Конфіденційність	Чи немає тут внутрішніх документів, цін, планів, чатів, клієнтських даних або паролів?
☐	Персональні дані	Чи є законна підстава та потрібні згоди на фото, відео, імена й інші дані?
☐	Військова безпека	Чи не розкриває матеріал місце, час, маршрут, ППО, військових, критичну інфраструктуру або наслідки атаки?
☐	Авторські права	Чи маємо право використовувати фото, музику, відео, шрифт, дизайн і логотипи?
☐	Мова та реклама	Чи відповідає мова вимогам для України? Чи позначено рекламу або партнерство?
☐	Безпека	Чи не веде посилання на підозрілий ресурс? Чи вимкнено зайву геолокацію та видалено небезпечні метадані?
☐	Тон	Чи сказав/ла б я це так само людині особисто? Чи немає приниження, погроз або дискримінації?
☐	Погодження	Чи отримано всі потрібні погодження і чи збережено фінальну версію?

Додаток 2. Матриця погодження контенту

Компанія може змінити цю матрицю відповідно до своєї структури. Позначення «обов'язково» означає письмове або зафіксоване в робочій системі погодження до публікації.

Тип контенту	Основний погоджувач	Додатковий погоджувач	Особливі умови
Звичайний контент за контент-планом	SMM / комунікації	—	У межах затверджених рубрик
Новий продукт, ціни, акція	Маркетинг / власник продукту	Юрист — за потреби	Перевірити умови та мову реклами
Кейс або відгук клієнта	Акаунт / власник клієнта	Юрист / DPO — за потреби	Дозвіл на бренд і персональні дані
Фінансові результати, інвестиції	Керівник / фінанси	Юрист / комунікації	Лише підтверджені неопублічні дані після дозволу
Кадрова інформація, фото працівника	HR / комунікації	Юрист / DPO — за потреби	Підстава для використання даних
Політична, суспільно чутлива тема	Керівник / комунікації	Юрист	Оцінка репутаційного ризику
Війна, обстріли, військові	Керівник комунікацій	Безпека / юрист	Лише офіційні джерела, перевірка геолокації
Кризова заява або інцидент	Уповноважений речник	Керівник / юрист / безпека	Один узгоджений центр комунікації
ШІ-згенерований реалістичний контент	Креативний керівник	Юрист / власник бренду	Перевірка фактів, прав і ризику введення в оману

Додаток 3. Підтвердження ознайомлення працівника

ПІБ працівника

Посада / підрозділ

Дата отримання Політики

Версія Політики 1.0

Я підтверджую, що:

- отримав/ла доступ до Політики використання соціальних мереж [НАЗВА КОМПАНІЇ];
- прочитав/ла документ у повному обсязі, мав/ла можливість поставити запитання та розумію встановлені вимоги;
- зобов'язуюся дотримуватися Політики в межах, що відповідають законодавству, моєму договору та посадовим обов'язкам;
- розумію обов'язок негайно повідомляти про втрату доступу, злам акаунта, витік конфіденційної інформації або інший інцидент.

Підпис працівника

Дата

ПІБ друкованими літерами

Підпис представника Компанії (за потреби)

Нормативна та методична основа

Документ адаптовано для українських реалій станом на 18 липня 2026 року. Під час затвердження та кожного наступного перегляду необхідно перевіряти актуальність законодавства й внутрішніх процедур.

- [Закон України «Про захист персональних даних» № 2297-VI](#)
- [Закон України «Про авторське право і суміжні права» № 2811-IX](#)
- [Закон України «Про забезпечення функціонування української мови як державної» № 2704-VIII](#)
- [Закон України «Про рекламу» № 270/96-ВР](#)
- [Кримінальний кодекс України, зокрема стаття 114-2](#)
- [Рекомендації CERT-UA щодо захисту облікових записів і двоетапної автентифікації](#)
- [Рекомендації Кіберполіції щодо безпеки в соціальних мережах](#)
- [Digital 2026: Ukraine — огляд актуального цифрового середовища і платформ](#)

ЮРИДИЧНЕ ЗАСТЕРЕЖЕННЯ

Цей документ є універсальним корпоративним шаблоном. Вимоги до конкретної компанії залежать від сфери діяльності, форми власності, категорій даних, типів працівників, договірних зобов'язань, регульованого ринку та фактичних процесів моніторингу. Перед затвердженням рекомендована юридична перевірка.