					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P36S					Tytuł dokumentu: **Polityka mediów społecznościowych i komunikacji zewnętrznej**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	Zdefiniowane procesy i nadzór oparty na rolach dla zarządzania komunikacją publiczną, zapewniające poprawność, ścieżki akceptacji oraz eskalację incydentów.
ISO/IEC 27002:2022	Środki kontrolne 5.10, 5.11, 5.35, 5.36	Reguluje wykorzystanie informacji, dopuszczalne użytkowanie oraz kontakty zewnętrzne i komunikację z organami, a także raportowanie zgodności.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Zasady korzystania z systemów i komunikacji, powiadomienia dla użytkowników oraz przechowywanie zapisów audytowych.
RODO	Artykuły 5, 25, 32, 33	Zasady przetwarzania danych, ochrona danych w fazie projektowania, bezpieczeństwo przetwarzania oraz wymogi zgłaszania naruszeń.
Dyrektywa NIS2	Artykuł 21	Środki zarządzania ryzykiem cyberbezpieczeństwa, obowiązki dotyczące incydentów oraz publicznego komunikowania kwestii związanych z ryzykiem.
Rozporządzenie DORA	Artykuły 9, 16	Zarządzanie ryzykiem ICT oraz strategia komunikacji dla dostawców krytycznych.
COBIT 2019	APO09, DSS05	Nadzór nad uzgodnieniami dotyczącymi usług i komunikacji oraz bezpieczne praktyki komunikacyjne i obsługa incydentów.

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe zasady i odpowiedzialności regulujące korzystanie z mediów społecznościowych oraz wszelkich form komunikacji zewnętrznej przez osoby powiązane z organizacją.

1.2 Zapewnia, że przekaz publiczny — niezależnie od tego, czy jest planowany, czy spontaniczny — jest poprawny, zgodny z zasadami szacunku, bezpieczny, zgodny z prawem oraz spójny z marką organizacji.

1.3 Celem polityki jest ograniczenie ryzyk związanych ze szkodą reputacyjną, naruszeniem wymogów regulacyjnych, ujawnieniem własności intelektualnej oraz nieuprawnionym ujawnieniem informacji za pośrednictwem kanałów publicznych.

1.4 Polityka dodatkowo wspiera rozliczalność i uporządkowany nadzór nad wszystkimi formami komunikacji cyfrowej dotyczącej organizacji lub wywierającej na nią wpływ.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich pracowników, kontraktorów, stażystów oraz przedstawicieli stron trzecich, którzy:

2.1.1 Komunikują się w imieniu organizacji, oficjalnie lub nieformalnie

2.1.2 Odwołują się do organizacji lub sugerują z nią związek w przestrzeni publicznej

2.1.3 Korzystają z kont prywatnych lub służbowych do udziału w publicznych dyskusjach dotyczących organizacji

2.2 Zakres objętych kanałów komunikacji obejmuje między innymi:

2.2.1 Platformy mediów społecznościowych (np. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Blogi, wiki, fora i publiczne tablice dyskusyjne

2.2.3 Wiadomości e-mail lub wiadomości bezpośrednie kierowane do podmiotów zewnętrznych (np. klientów, organów regulacyjnych, mediów)

2.2.4 Wywiady prasowe, panele dyskusyjne lub utrwalone wystąpienia medialne

2.2.5 Udział w społecznościach internetowych, w których pojawia się odniesienie do organizacji

2.3 Niniejsza polityka reguluje zarówno treści publikowane w czasie rzeczywistym, jak i wcześniej zaplanowane, oraz ma zastosowanie do wszystkich urządzeń i kont (prywatnych lub służbowych) wykorzystywanych do rozpowszechniania komunikacji.

3. Cele

3.1 Zapobieganie przypadkowemu lub celowemu ujawnieniu informacji poufnych, wrażliwych lub objętych regulacjami za pośrednictwem kanałów komunikacji zewnętrznej.

3.2 Zapewnienie, że oficjalne oświadczenia publiczne i treści publikowane w mediach społecznościowych są poprawne, autoryzowane i zgodne z identyfikacją marki organizacji, zasadami etyki oraz strategicznym przekazem.

3.3 Zapobieganie szkodzie reputacyjnej i zapewnienie spójności komunikatów pomiędzy działami wewnętrznymi oraz platformami zewnętrznymi.

3.4 Zapewnienie zgodności z obowiązującymi wymogami prawnymi dotyczącymi wypowiedzi publicznych, w tym między innymi z RODO, NIS2, DORA oraz sektorowymi zasadami komunikacji.

3.5 Określenie jasnych odpowiedzialności, dopuszczalnych przypadków użycia oraz zasad egzekwowania postanowień wobec całego personelu prowadzącego działania publiczne.

4. Role i odpowiedzialności

4.1 Dyrektor ds. marketingu lub komunikacji / kierownik PR

4.1.1 Zatwierdza wszystkie oficjalne komunikaty organizacji przeznaczone do publikacji zewnętrznej

4.1.2 Utrzymuje harmonogramy treści w mediach społecznościowych oraz wytyczne zapewniające spójność marki

4.1.3 Monitoruje wzmianki internetowe i ekspozycję medialną dotyczącą organizacji

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO) / zespół bezpieczeństwa

4.2.1 Monitoruje platformy cyfrowe pod kątem wskaźników ujawnienia danych, podszywania się lub prób phishingu

4.2.2 Koordynuje działania z zespołami reagowania na incydenty w przypadku ataków lub naruszeń związanych z mediami społecznościowymi

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Egzekwowanie polityki i zgodność

9.1 Niniejsza polityka jest obowiązkowa dla całego personelu objętego zakresem oraz stron trzecich. Nieprzestrzeganie jej postanowień może skutkować:

9.1.1 Formalnymi ostrzeżeniami

9.1.2 Tymczasowym lub trwałym cofnięciem dostępu do platform lub systemów

9.1.3 Środkami dyscyplinarnymi, w tym zakończeniem współpracy

9.1.4 Podjęciem działań prawnych, jeżeli komunikacja zewnętrzna skutkuje szkodą reputacyjną, naruszeniem ochrony danych osobowych lub niezgodnością regulacyjną

9.2 Środki dyscyplinarne

9.2.1 Naruszenia wewnętrzne (np. ujawnienie danych poufnych, zniesławienie organizacji) skutkują zaangażowaniem HR, formalnym postępowaniem wyjaśniającym oraz udokumentowaniem w aktach pracowniczych.

9.2.2 W stosownych przypadkach dział prawny podejmie środki cywilnoprawne lub powiadomi właściwe organy o działalności przestępczej (np. podszywanie się, ujawnienia związane z wykorzystywaniem informacji poufnych).

9.3 Monitorowanie zgodności

9.3.1 Zespoły bezpieczeństwa i komunikacji muszą prowadzić bieżące monitorowanie:

9.3.1.1 Wzmianek o marce na głównych platformach

9.3.1.2 Nieoficjalnego wykorzystania materiałów graficznych organizacji lub znaków towarowych

9.3.1.3 Znanych ryzyk (np. niezadowolonych pracowników, prób podszywania się)

9.3.2 Monitorowanie musi być zgodne z przepisami i regulacjami dotyczącymi prywatności pracowników, a wszystkie oznaczone przypadki muszą być weryfikowane przez człowieka.

9.4 Mechanizm zgłaszania nieprawidłowości i zgłaszanie nadużyć

9.4.1 Każdy pracownik podejrzewający naruszenie niniejszej polityki jest zachęcany do zgłoszenia tego faktu do zespołu ds. bezpieczeństwa informacji, działu prawnego lub anonimowo za pośrednictwem portalu dla sygnalistów.

9.4.2 Działania odwetowe wobec sygnalistów są bezwzględnie zabronione i będą skutkować natychmiastowym zastosowaniem środków dyscyplinarnych.

10. Wymagania dotyczące przeglądu i aktualizacji

10.1 Niniejsza polityka musi podlegać corocznemu przeglądowi lub wcześniej, jeżeli:

10.1.1 Nastąpią istotne zmiany wymagań regulacyjnych (np. nowe przepisy UE dotyczące komunikacji cyfrowej)

10.1.2 Zostaną przyjęte nowe platformy społecznościowe lub kanały komunikacji

10.1.3 Wystąpi istotny incydent lub powtarzające się naruszenia wskazujące na luki procesowe

10.1.4 Nastąpi zmiana strukturalna lub kadrowa w funkcjach PR, prawnej lub bezpieczeństwa

10.2 Przegląd musi być przeprowadzany wspólnie przez:

10.2.1 Szefa marketingu / PR

10.2.2 CISO lub osobę odpowiedzialną za ryzyko bezpieczeństwa

10.2.3 Kierownika działu prawnego i zgodności

10.3 Aktualizacje muszą być dokumentowane w Rejestrze zmian polityki i komunikowane za pośrednictwem wewnętrznych kanałów budowania świadomości. W przypadku istotnych zmian cały personel objęty zmianą musi ponownie potwierdzić zapoznanie się z polityką.

11. Powiązane polityki i zależności

11.1 Niniejsza polityka jest wspierana przez następujące elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) organizacji i pozostaje z nimi w powiązaniu:

11.1.1 P1 – Polityka bezpieczeństwa informacji: ustanawia nadrzędne zasady ochrony informacji, w tym zapewnienie, że komunikacja nie prowadzi do nieuprawnionego ujawnienia.

11.1.2 P3 – Polityka dopuszczalnego użytkowania: definiuje dopuszczalne zachowania dotyczące platform cyfrowych i technologii, które bezpośrednio regulują prywatne i zawodowe korzystanie z kanałów społecznościowych.

11.1.3 P6 – Polityka zarządzania ryzykiem: zapewnia ramy zarządzania ryzykiem do oceny zagrożeń związanych z komunikacją publiczną i ekspozycją reputacyjną.

11.1.4 P8 – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: ustanawia programy podnoszenia świadomości, które edukują personel w zakresie bezpiecznych praktyk komunikacyjnych i zagrożeń socjotechnicznych.

11.1.5 P13 – Polityka klasyfikacji i oznaczania informacji: wskazuje personelowi, co stanowi informacje zastrzeżone lub poufne, które nie mogą być ujawniane na zewnątrz.

11.1.6 P30 – Polityka reagowania na incydenty: definiuje sposób postępowania z incydentami związanymi z komunikacją publiczną, w tym wyciekami danych, podszywaniem się i naruszeniami regulacyjnymi.

11.1.7 P33 – Polityka audytu i monitorowania zgodności: reguluje procesy audytowe weryfikujące środki kontrolne dotyczące mediów społecznościowych, systemy monitorowania oraz zgodność z politykami komunikacji zewnętrznej.

12. Normy i ramy odniesienia

12.1 ISO/IEC 27001:2022

12.1.1 Klauzula 8.1 – Planowanie i nadzór operacyjny: wymaga zdefiniowanych procesów i nadzoru opartego na rolach dla zarządzania komunikacją publiczną, zapewniających poprawność, ścieżki akceptacji oraz eskalację incydentów związanych z ryzykiem dla danych lub reputacji.

12.2 ISO/IEC 27002:2022

12.2.1 Środek kontrolny 5.10 – Wykorzystanie informacji: reguluje autoryzowane i etyczne rozpowszechnianie komunikacji wewnętrznej lub zewnętrznej.

12.2.2 Środek kontrolny 5.11 – Dopuszczalne użytkowanie aktywów organizacji: wzmacnia dopuszczalne praktyki udostępniania treści przy użyciu korporacyjnych aktywów IT lub kont prywatnych.

12.2.3 Środek kontrolny 5.35 – Kontakty z organami: wymaga uporządkowanej i autoryzowanej komunikacji zewnętrznej z organami regulacyjnymi i instytucjami publicznymi.

12.2.4 Środek kontrolny 5.36 – Zgodność z politykami i normami: wymaga spójnego stosowania polityk wewnętrznych we wszystkich scenariuszach komunikacyjnych.

12.3 NIST SP 800-53 Rev.5

12.3.1 PL-4 – Zasady zachowania: wymaga formalnych zasad korzystania z systemów i komunikacji, w tym standardów ujawnień publicznych.

12.3.2 AC-8 – Powiadomienie o korzystaniu z systemu: wspiera obowiązkowe zastrzeżenia i ostrzeżenia dotyczące treści na platformach zewnętrznych.

12.3.3 AU-12 – Retencja zapisów audytowych: ma zastosowanie do zachowania logów i historii komunikacji na potrzeby przeglądu incydentów i audytu.

12.4 RODO (2016/679)

12.4.1 Artykuł 5 – Zasady przetwarzania danych: zakazuje nieuprawnionego udostępniania danych osobowych za pośrednictwem komunikacji publicznej.

12.4.2 Artykuł 25 – Ochrona danych w fazie projektowania i domyślna ochrona danych: wymaga środków ochrony prywatności w narzędziach komunikacyjnych i przepływach pracy dotyczących treści.

12.4.3 Artykuł 32 – Bezpieczeństwo przetwarzania: obejmuje szyfrowanie, kontrolę dostępu i procesy zatwierdzania treści.

12.4.4 Artykuł 33 – Zgłoszenie naruszenia: wymaga terminowego zgłaszania wycieków danych osobowych za pośrednictwem kanałów publicznych.

12.5 Dyrektywa UE NIS2 (2022/2555)

12.5.1 Artykuł 21 – Środki zarządzania ryzykiem cyberbezpieczeństwa: obejmuje protokoły komunikacyjne i obowiązki podczas incydentów oraz publicznego komunikowania ryzyka.

12.6 Rozporządzenie DORA (2022/2554)

12.6.1 Artykuł 9 – Zarządzanie ryzykiem ICT: ma zastosowanie do ryzyk komunikacyjnych wywołanych zewnętrznie, takich jak podszywanie się, dezinformacja i zakłócenia reputacyjne.

12.6.2 Artykuł 16 – Strategia komunikacji: wymaga, aby krytyczni dostawcy finansowi lub usługowi zarządzali ryzykiem komunikacyjnym i reakcją w scenariuszach kryzysowych.

12.7 COBIT 2019

12.7.1 APO09 – Zarządzane uzgodnienia usługowe i komunikacja: wymaga uporządkowanego nadzoru nad komunikacją wewnętrzną i zewnętrzną.

12.7.2 DSS05 – Zarządzanie usługami bezpieczeństwa: zapewnia, że działania komunikacyjne nie wprowadzają dodatkowego ryzyka ani nie osłabiają procesów obsługi incydentów.