Dofinansowane przez Unię Europejską

sieć splot wartości

WZÓR

Zasady korzystania z kont, poczty i mediów społecznościowych organizacji

wzór dla małych organizacji pozarządowych

Opracowanie: Fundacja LegisLab

Stan prawny na dzień: wrzesień 2026 r.

Z komentarzem [FL1]: JAK KORZYSTAĆ Z WZORU. (1) Przed zawarciem umowy usuń tę kartę tytułową, stopkę z oznaczeniami projektu oraz wszystkie komentarze. (2) Uzupełnij pola w nawiasach kwadratowych [ ] – wskazówki w nawiasach usuń. (3) Postanowienia oznaczone [opcjonalnie] pozostaw albo usuń, zależnie od specyfiki organizacji.

Wzór ma charakter pomocniczy i nie stanowi porady prawnej. Przed wdrożeniem należy dostosować jego treść do wielkości organizacji, używanych narzędzi oraz sposobu współpracy z zarządem, pracownikami i wolontariuszami.

Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

Program finansowany jest przez Unię Europejską. Wyrażone opinie i poglądy są wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Komisji Europejskiej. Ani Unia Europejska, ani organ przyznający finansowanie nie mogą ponosić za nie odpowiedzialności.

Jak korzystać z wzoru

Ten materiał przygotowano dla małych organizacji pozarządowych: stowarzyszeń, fundacji, kół gospodyń wiejskich, ochotniczych straży pożarnych i grup działających głównie dzięki wolontariuszom. W takich organizacjach konta e-mail, strona internetowa i profile w mediach społecznościowych często zakłada i prowadzi jedna osoba, na własnym telefonie lub komputerze. Gdy ta osoba odchodzi, organizacja może stracić dostęp do swojej domeny, poczty czy profilu. Wzór pomaga temu zapobiec.

Co zawiera dokument

- **Zasady** (18 paragrafów) – gotowy tekst do przyjęcia przez zarząd.
- **Załącznik 1** – Rejestr kont i dostępów (bez haseł).
- **Załącznik 2** – Oświadczenie osoby korzystającej z kont organizacji.
- **Załącznik 3** – Karta wyłączenia dostępu, gdy ktoś kończy współpracę.
- **Załącznik 4** – Ściągawka „zasady na jednej stronie" dla zespołu i wolontariuszy.

Jak wdrożyć – 8 kroków

1. **Zrób spis kont.** Zanim przyjmiesz Zasady, uzupełnij Załącznik 1: jakie konta ma organizacja, na kogo są założone i kto ma dostęp.
2. **Wyznacz dwie osoby**: administratora głównego i zastępczego. Żadne ważne konto nie powinno zależeć od jednej osoby.
3. **Przenieś konta na organizację.** Zmień adresy odzyskiwania na adresy organizacji i dodaj drugiego administratora (np. do profilu w mediach społecznościowych, do panelu domeny i hostingu).
4. **Włącz weryfikację dwuetapową** na poczcie, w chmurze, w panelu domeny i hostingu, w mediach społecznościowych oraz w bankowości.
5. **Uzupełnij wzór.** Wpisz dane w polach oznaczonych [takim tłem]. Usuń postanowienia oznaczone [opcjonalnie], jeżeli nie dotyczą Twojej organizacji (np. wolontariuszy lub bankowości internetowej).
6. **Przyjmij Zasady uchwałą zarządu** albo zarządzeniem prezesa, zgodnie ze statutem. Przykład: „Zarząd [nazwa organizacji] uchwala Zasady korzystania z kont, poczty i mediów społecznościowych w brzmieniu stanowiącym załącznik do uchwały. Zasady wchodzą w życie z dniem [data]".
7. **Przekaż Zasady osobom z dostępem** i zbierz krótkie oświadczenia (Załącznik 2). Wolontariuszom wystarczy Załącznik 4 i potwierdzenie e-mailem.
8. **Ustaw przypomnienie** w kalendarzu: przegląd dostępów co 6 miesięcy oraz termin odnowienia domeny i hostingu.

Na co zwrócić uwagę

- Zasady dotyczą **kont organizacji**. Nie dają prawa wglądu w prywatne konta i prywatną korespondencję osób, które z nich korzystają.

Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

- Wzór nie służy do monitorowania treści korespondencji. Jeżeli organizacja zatrudnia pracowników i chce kontrolować pocztę służbową, musi spełnić odrębne wymogi (zob. art. 22^2 i 22^3 Kodeksu pracy) oraz zasady ochrony danych osobowych.
- Zasady **uzupełniają**, a nie zastępują politykę ochrony danych osobowych, procedurę reagowania na naruszenia, standardy ochrony małoletnich i klauzule informacyjne, które organizacja już stosuje. W tekście wpisz ich nazwy w miejscach oznaczonych [ ].
- Liczby podane we wzorze (długość hasła, terminy przeglądów, okresy przechowywania) to rozsądne wartości domyślne. Dostosuj je do swoich możliwości, ale nie obniżaj ich bez powodu.
- Przed zamieszczeniem gotowych Zasad w organizacji **usuń** kartę tytułową, tę instrukcję i stopkę z oznaczeniami projektu.

Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

Załącznik do [uchwały Zarządu nr … / zarządzenia Prezesa Zarządu nr …] z dnia [data]

ZASADY KORZYSTANIA Z KONT, POCZTY I MEDIÓW SPOŁECZNOŚCIOWYCH

[nazwa organizacji]

§ 1. Cel i zakres

1. Zasady określają, jak [nazwa organizacji] („Organizacja") zakłada, zabezpiecza i wykorzystuje swoje konta cyfrowe. Ich celem jest to, aby Organizacja nigdy nie traciła dostępu do własnych zasobów, a dane i wizerunek były bezpieczne.
2. Zasady dotyczą kont i narzędzi Organizacji, w szczególności:
   a) poczty e-mail w domenie [domena] oraz innych adresów używanych przez Organizację;
   b) domeny, hostingu i panelu strony internetowej;
   c) dysku w chmurze i wspólnych folderów;
   d) profili w mediach społecznościowych: [Facebook / Instagram / LinkedIn / YouTube / TikTok – wpisz właściwe];
   e) narzędzi do newslettera, ankiet, formularzy, komunikatorów i wideokonferencji;
   f) [opcjonalnie] bankowości elektronicznej i programu księgowego online – z zastrzeżeniem dodatkowych zasad banku i biura rachunkowego.
3. Zasady stosuje się do członków zarządu, pracowników, wolontariuszy, współpracowników oraz podmiotów zewnętrznych, którym Organizacja udostępniła dostęp („Użytkownicy").
4. Zasady nie dotyczą prywatnych kont Użytkowników. Organizacja nie żąda dostępu do prywatnych kont ani prywatnej korespondencji Użytkowników.

§ 2. Podstawowe pojęcia

- **Konto Organizacji** – konto, adres, profil lub panel utworzony dla Organizacji lub w jej imieniu, niezależnie od tego, kto je faktycznie założył.
- **Administrator** – osoba z pełnymi uprawnieniami do konta: może zmieniać ustawienia, dodawać i usuwać osoby oraz odzyskiwać dostęp.
- **Użytkownik** – osoba, której nadano dostęp do konta w określonym zakresie.
- **Weryfikacja dwuetapowa (2FA)** – dodatkowe potwierdzenie logowania, np. kodem z aplikacji lub kluczem sprzętowym, oprócz hasła.
- **Menedżer haseł** – program, który bezpiecznie przechowuje hasła i pomaga tworzyć długie, unikalne hasła.
- **Incydent** – każde zdarzenie, które zagraża bezpieczeństwu kont lub danych, np. utrata dostępu, przejęcie konta, kradzież urządzenia, kliknięcie w fałszywy link, wysłanie danych do niewłaściwej osoby.

§ 3. Własność kont i treści

1. Konta Organizacji, adresy, domeny, profile, treści i dane na nich zgromadzone należą do Organizacji, także wtedy, gdy konto założyła osoba fizyczna.

2. Konta Organizacji zakłada się na adres e-mail i numer telefonu Organizacji. Jeżeli serwis wymaga numeru telefonu lub adresu osoby prywatnej, wpisuje się to do Rejestru kont i wskazuje drugą osobę, która może odzyskać dostęp.
3. Użytkownik nie przenosi, nie sprzedaje, nie zmienia nazwy ani nie usuwa konta Organizacji bez zgody Zarządu.
4. Po zakończeniu współpracy Użytkownik nie zachowuje dostępu do kont Organizacji ani kopii jej danych, z wyjątkiem tych, do których ma prawo na podstawie odrębnych ustaleń.

§ 4. Administratorzy i rejestr kont

1. Zarząd wyznacza Administratora głównego: [imię i nazwisko, funkcja] oraz Administratora zastępczego: [imię i nazwisko, funkcja].
2. Przy każdym ważnym koncie są co najmniej dwie osoby, które mogą zmienić dane dostępowe lub administratora (jeśli narzędzie to umożliwia).
3. Administrator główny prowadzi Rejestr kont i dostępów (Załącznik 1). Rejestr zawiera nazwę narzędzia, adres konta, administratorów, osoby z dostępem, informację o 2FA oraz terminy odnowień i przeglądów. **Rejestr nie zawiera haseł.**
4. Rejestr przechowuje się w miejscu dostępnym dla Administratora głównego i zastępczego: [np. zamknięty folder w chmurze Organizacji].
5. Kody zapasowe do 2FA, klucze odzyskiwania i dane do odzyskania konta przechowuje się w bezpiecznym miejscu, osobno od Rejestru: [np. menedżer haseł Organizacji / zamknięta koperta w sejfie]. Dostęp do nich mają co najmniej dwie osoby wskazane przez Zarząd.

§ 5. Nadawanie i odbieranie uprawnień

1. Uprawnienia nadaje Administrator na podstawie decyzji Zarządu [lub koordynatora projektu].
2. Obowiązuje zasada minimum: Użytkownik dostaje tylko takie uprawnienia, jakie są mu potrzebne do zadań (np. rola redaktora zamiast administratora, podgląd zamiast edycji).
3. Każdy Użytkownik korzysta z własnego loginu. Nie używamy jednego wspólnego konta dla kilku osób. Jeżeli narzędzie nie pozwala na osobne konta, wymaga to zgody Administratora, wpisu do Rejestru i zmiany hasła przy każdej zmianie osób, które je znają.
4. Tam, gdzie to możliwe, uprawnienia nadaje się na czas określony (np. na czas projektu lub wydarzenia).
5. Przed nadaniem dostępu Użytkownik zapoznaje się z Zasadami i podpisuje oświadczenie (Załącznik 2). [opcjonalnie: dla wolontariuszy działających krótko wystarczy potwierdzenie e-mailem po otrzymaniu Załącznika 4.]

§ 6. Hasła i logowanie

1. Każde konto ma unikalne hasło, którego nie używamy w żadnym innym serwisie.
2. Hasło ma co najmniej 14 znaków. Najlepiej, gdy jest to fraza złożona z kilku niezwiązanych słów. Do tworzenia i przechowywania haseł zalecamy menedżer haseł.

3. Nie zmieniamy haseł „z automatu” co miesiąc. Hasło zmieniamy niezwłocznie, gdy: podejrzewamy, że je ktoś poznał; serwis zgłosił wyciek; osoba znająca hasło kończy współpracę; hasło przekazano niebezpiecznym kanałem.
4. Weryfikację dwuetapową włączamy na wszystkich kontach, które ją oferują. W pierwszej kolejności dotyczy to poczty e-mail, panelu domeny i hostingu, chmury, mediów społecznościowych oraz bankowości. Jeśli to możliwe, wybieramy aplikację uwierzytelniającą lub klucz sprzętowy zamiast kodów SMS.
5. Nie wolno: zapisywać haseł na kartkach przy komputerze, w niezabezpieczonych plikach, w wiadomościach e-mail ani w komunikatorach; podawać hasła ani kodów 2FA nikomu, kto o nie prosi (także osobie podającej się za pracownika serwisu, banku lub członka zarządu); zapamiętywać haseł w przeglądarce na cudzych lub wspólnych urządzeniach.
6. Jeżeli hasło musi zostać przekazane innej osobie, przekazujemy je innym kanałem niż adres konta (np. telefonicznie) i zmieniamy po użyciu.

§ 7. Urządzenia, z których korzystamy

1. Do kont Organizacji logujemy się z urządzeń, które mają: blokadę ekranu (PIN, hasło lub biometrię), aktualny system i przeglądarkę, włączone automatyczne aktualizacje oraz aktywne zabezpieczenie przed złośliwym oprogramowaniem.
2. Prywatne urządzenia można wykorzystywać do pracy dla Organizacji, pod warunkiem przestrzegania Zasad. [opcjonalnie: Organizacja udostępnia sprzęt służbowy: wpisz, jaki i komu.]
3. Na urządzeniach cudzych i publicznych (np. w bibliotece, na komputerze znajomego) nie logujemy się do kont Organizacji. Jeśli to się zdarzy, wylogowujemy się ze wszystkich sesji i zmieniamy hasło.
4. Pliki Organizacji przechowujemy w jej chmurze lub na dysku Organizacji. Jeśli pobraliśmy je na prywatne urządzenie, usuwamy je po zakończeniu zadania.
5. Utratę lub kradzież urządzenia, z którego korzystano z kont Organizacji, zgłaszamy jak incydent (§ 14).

§ 8. Poczta elektroniczna

1. Sprawy Organizacji prowadzimy z adresów organizacyjnych: [np. imię@domena lub funkcja@domena]. Wiadomości z adresów prywatnych przekazujemy niezwłocznie na adres Organizacji.
2. Adresy zbiorcze (np. kontakt@, biuro@) mają co najmniej dwie osoby odpowiedzialne. Sposób obsługi ustala Zarząd.
3. Przy wiadomościach do wielu osób, które się nie znają, używamy ukrytej kopii (UDW/BCC).
4. Załączniki z danymi osobowymi ograniczamy do niezbędnych. Plik zabezpieczamy hasłem przekazanym innym kanałem lub udostępniamy bezpieczny link z ograniczonym dostępem.
5. Nie ustawiamy automatycznego przekierowywania poczty Organizacji na prywatne adresy bez zgody Administratora.

6. Przed wysłaniem sprawdzamy adresata. Podpowiedzi autouzupełniania potrafią wstawić inny adres, niż zamierzaliśmy.

§ 9. Chmura, wspólne foldery i kopie zapasowe

1. Dokumenty Organizacji przechowujemy w: [nazwa narzędzia, np. wspólny dysk Organizacji], a nie na prywatnych kontach.
2. Struktura folderów: [np. Zarząd, Projekty, Finanse, Wolontariusze, Komunikacja]. Do folderów z danymi osobowymi i finansami dostęp mają tylko osoby, które go potrzebują.
3. Pliki udostępniamy wskazanym osobom, a nie „każdemu, kto ma link". Wyjątek stanowią dokumenty przeznaczone do publikacji.
4. Dostęp do folderu projektu cofamy po zakończeniu projektu lub roli danej osoby.
5. Kopię zapasową ważnych danych wykonujemy: [sposób i częstotliwość, np. raz w tygodniu na zewnętrzny dysk / automatycznie w usłudze]. Odpowiada za to: [imię i nazwisko]. Co [6] miesięcy sprawdzamy, czy da się odtworzyć wybrany plik z kopii.

§ 10. Strona internetowa, domena i media społecznościowe

1. Domena i hosting są zarejestrowane na Organizację jako właściciela, a nie na osobę prywatną. Terminy ich wygaśnięcia wpisujemy do Rejestru i kalendarza. Przypomnienie o odnowieniu ustawiamy co najmniej [60] dni wcześniej, na adres zbiorczy Organizacji.
2. Profile w mediach społecznościowych prowadzimy tak, aby co najmniej dwie osoby miały uprawnienia administratora. Korzystamy z funkcji ról i zarządzania stroną udostępnianych przez platformę, a nie z logowania na prywatne konto jednej osoby.
3. Prywatnych profili osób nie wykorzystujemy jako profilu Organizacji.
4. Publikować w imieniu Organizacji mogą: [role/osoby]. Treści zatwierdza: [osoba]. Treści szczególne (kryzysowe, dotyczące osób trzecich, dzieci lub osób w trudnej sytuacji, kontrowersyjne) zatwierdza Zarząd.
5. Komunikacja Organizacji jest rzetelna i kulturalna oraz zgodna z jej wartościami i politykami: [np. polityka równościowa, standardy ochrony małoletnich]. Komentarze naruszające te zasady (wulgarne, dyskryminujące, zawierające dane osobowe) ukrywamy lub usuwamy zgodnie z regulaminem platformy.
6. Na prywatnych profilach Użytkownicy nie występują w imieniu Organizacji i nie przedstawiają swoich opinii jako jej stanowiska.
7. Wiadomości prywatne na profilach przeglądają: [osoby]. Zgłoszenia dotyczące zagrożenia dobra dziecka lub naruszeń ochrony danych kierujemy zgodnie z odpowiednią procedurą Organizacji: [nazwa].
8. Aplikacje, wtyczki i narzędzia zewnętrzne powiązane z kontem (np. do planowania postów) włącza wyłącznie Administrator, po sprawdzeniu dostawcy. Nieużywane integracje usuwamy.

§ 11. Dane osobowe, wizerunek i prawa autorskie

1. Zdjęcia i nagrania z udziałem osób publikujemy zgodnie z zasadami stosowanymi w Organizacji: [nazwa dokumentu, np. klauzula informacyjna dla uczestników wydarzeń /

zgoda na wizerunek]. W przypadku małoletnich stosujemy dodatkowo [Standardy ochrony małoletnich].

2. Nie publikujemy danych uczestników (list, adresów, telefonów, zrzutów ekranu z formularzy), jeżeli nie ma do tego podstawy i potrzeby. Zrzuty ekranu i dokumenty przed publikacją anonimizujemy.
3. Publikujemy tylko te treści, do których Organizacja ma prawa: własne, objęte licencją lub dostępne na licencji otwartej, z podaniem wymaganych informacji o autorze i źródle.
4. Zasady uzupełniają [politykę ochrony danych osobowych Organizacji] i jej nie zastępują.

§ 12. Oznaczenia projektów i informacja o finansowaniu [opcjonalnie]

1. Jeżeli treść dotyczy projektu finansowanego ze środków zewnętrznych, stosujemy oznaczenia i wzmianki o finansowaniu wymagane w umowie i wytycznych danego projektu (logotypy, podpisy, klauzule).
2. Za sprawdzenie oznaczeń przed publikacją odpowiada: [osoba]. Przed publikacją korzystamy z krótkiej listy kontrolnej: logotypy, wymagany podpis, zgody na wizerunek, brak danych osobowych.

§ 13. Uważamy na oszustwa (phishing)

1. Typowe sygnały ostrzegawcze: pośpiech („konto zostanie zablokowane dzisiaj"), prośba o hasło, kod lub przelew, link prowadzący na nietypową stronę, nieoczekiwany załącznik, nagła zmiana numeru rachunku na fakturze, wiadomość „od prezesa" z prośbą o pilny przelew lub zakup kart podarunkowych, rzekome ostrzeżenie platformy społecznościowej o naruszeniu zasad.
2. Nie klikamy w podejrzane linki. Adres strony wpisujemy ręcznie albo korzystamy z zapisanej zakładki, a logujemy się tylko po sprawdzeniu domeny.
3. Prośby o zmianę rachunku bankowego lub pilny przelew potwierdzamy drugim kanałem, np. telefonicznie na znany nam numer.
4. Kodów 2FA, SMS, BLIK ani haseł nie podajemy nikomu.
5. Podejrzaną wiadomość zgłaszamy: [osoba/adres]. Jeśli kliknięto link lub podano dane, stosujemy § 14. Podejrzane wiadomości i strony można zgłosić do CERT Polska (incydent.cert.pl).

§ 14. Zgłaszanie incydentów

1. Użytkownik zgłasza Administratorowi niezwłocznie, w tym samym dniu: [telefon / e-mail do zgłoszeń] każdy incydent, w szczególności: utratę lub kradzież urządzenia; brak możliwości zalogowania się lub zmianę hasła, której nie dokonano; powiadomienie o logowaniu z nieznanego miejsca; kliknięcie w podejrzany link albo podanie hasła; wysłanie wiadomości do niewłaściwej osoby; wpisy na profilu, których nikt nie opublikował.
2. Pierwsze kroki: zmień hasło z bezpiecznego urządzenia; wyloguj wszystkie sesje; sprawdź przekierowania poczty, podłączone aplikacje i ustawienia 2FA; zrób zrzuty ekranu jako dowód; poinformuj osoby, które mogły otrzymać fałszywe wiadomości.

3. Jeśli incydent dotyczy danych osobowych, stosujemy [Procedurę reagowania na naruszenia ochrony danych osobowych]. Zarząd ocenia wtedy, czy zgłosić naruszenie Prezesowi UODO – co do zasady bez zbędnej zwłoki i w miarę możliwości nie później niż w ciągu 72 godzin od stwierdzenia naruszenia – oraz czy zawiadomić osoby, których dane dotyczą.
4. W razie przejęcia profilu w mediach społecznościowych Administrator korzysta z formularza pomocy platformy i informuje Zarząd.
5. Szybkie zgłoszenie błędu popełnionego w dobrej wierze nie skutkuje negatywnymi konsekwencjami. Zależy nam na szybkiej reakcji, a nie na szukaniu winnych.

§ 15. Zmiana osoby i zakończenie współpracy

1. Gdy Użytkownik kończy rolę (koniec projektu, rezygnacja, zmiana zarządu, koniec wolontariatu), Administrator odbiera mu dostęp najpóźniej [w dniu zakończenia współpracy / w ciągu 3 dni roboczych], zgodnie z Kartą wyłączenia dostępu (Załącznik 3).
2. Użytkownik: zwraca urządzenia i nośniki; przekazuje materiały i informacje o bieżących sprawach; usuwa dane Organizacji z prywatnych urządzeń; wskazuje integracje i powiązania kont, o których wie (bez konieczności przesyłania haseł).
3. Hasła wspólne zmieniamy. Telefon, adres e-mail i urządzenia 2FA przypisane do konta zastępujemy danymi Organizacji.
4. Skrzynkę e-mail osoby kończącej współpracę zamykamy po okresie [np. 3 miesięcy] z automatyczną odpowiedzią lub przekierowaniem na adres Organizacji. Przed zamknięciem osoba może usunąć lub zabrać swoją prywatną korespondencję. Dalsze przechowywanie treści ocenia się według zasad przechowywania dokumentów w Organizacji.
5. Po zmianie członków zarządu nowy Zarząd w ciągu [14] dni sprawdza Rejestr kont, zmienia administratorów, dostęp do poczty, domeny, bankowości i innych ważnych narzędzi oraz aktualizuje Rejestr. Dotyczy to także kont w systemach urzędowych, jeśli Organizacja z nich korzysta.
6. Profilu zaufanego ani innych środków identyfikacji elektronicznej osoby fizycznej nie udostępniamy innym. Do działania w imieniu Organizacji korzystamy z uprawnień, pełnomocnictw i funkcji dostępnych w danym systemie.

§ 16. Przegląd dostępów i kopii

1. Administrator co [6] miesięcy oraz po zakończeniu większego projektu sprawdza: aktualność listy osób z dostępem, administratorów, włączenie 2FA, dane do odzyskiwania kont, terminy domeny i hostingu, działanie kopii zapasowej, nieużywane konta (do zamknięcia).
2. Wynik przeglądu zapisuje w Rejestrze (data, podpis) i informuje Zarząd.
3. Raz w roku Zarząd omawia stan bezpieczeństwa kont i sprawdza, czy Zasady są aktualne.

§ 17. Odpowiedzialność i wprowadzenie nowych osób

1. Zarząd odpowiada za wdrożenie Zasad, Administrator za prowadzenie Rejestru i przeglądy, a Użytkownicy za ich przestrzeganie.
2. Nowa osoba przed otrzymaniem dostępu dostaje krótkie wprowadzenie i Załącznik 4.

3. Nieprzestrzeganie Zasad może skutkować ograniczeniem lub odebraniem dostępu. Wobec pracowników stosuje się przepisy prawa pracy, a wobec wolontariuszy i współpracowników postanowienia zawartych z nimi porozumień lub umów.

§ 18. Postanowienia końcowe

1. Zasady wchodzą w życie [data].
2. Zmiany Zasad wprowadza Zarząd. Użytkownicy są o nich informowani: [sposób].
3. Zasady są dostępne dla Użytkowników: [miejsce, np. wspólny folder].
4. W sprawach nieuregulowanych decyduje Zarząd.

Załącznik 1. Rejestr kont i dostępów

Rejestr prowadzi Administrator główny. **Nie wpisuj tu haseł ani kodów.** Dodaj tyle wierszy, ile masz kont. Pierwsze dwa wiersze to przykłady do usunięcia.

Lp.	Narzędzie / konto	Adres lub nazwa konta	Administratorzy	Osoby z dostępem (rola)	2FA	Odnowienie / data przeglądu
1	*Poczta e-mail (przykład)*	*kontakt@[domena]*	*[A. Kowalska], [J. Nowak]*	*Zarząd (admin), koordynatorka (użytkownik)*	*Tak (aplikacja)*	*Przegląd: [data]*
2	*Domena i hosting (przykład)*	*[domena]*	*[A. Kowalska], [J. Nowak]*	*–*	*Tak*	*Odnowienie: [data]*
3						
4						
5						
6						
7						
8						
9						
10						

Gdzie przechowujemy kody zapasowe i dane do odzyskiwania kont: [miejsce]. Osoby z dostępem: [imiona i nazwiska].

Data ostatniego przeglądu: [data]. Podpis Administratora: [podpis].

Załącznik 2. Oświadczenie osoby korzystającej z kont Organizacji

Ja, [imię i nazwisko], pełniąc w [nazwa organizacji] rolę: [funkcja / wolontariusz / współpracownik], oświadczam, że:

1. zapoznałam/em się z Zasadami korzystania z kont, poczty i mediów społecznościowych Organizacji i zobowiązuję się ich przestrzegać;
2. będę korzystać z kont Organizacji wyłącznie w zakresie moich zadań i uprawnień;
3. nie udostępnię nikomu swoich danych logowania ani kodów weryfikacyjnych;
4. niezwłocznie zgłoszę Administratorowi każdy incydent, w tym utratę urządzenia lub podejrzenie przejęcia konta;
5. po zakończeniu współpracy zwrócę dostęp, urządzenia i materiały Organizacji oraz usunę jej dane z moich prywatnych urządzeń;
6. zachowam w tajemnicy informacje, do których uzyskałam/em dostęp w związku z działaniami Organizacji, w tym dane osobowe.

Zakres uprawnień przyznanych mi przez Organizację:

Narzędzie / konto	Rola (np. redaktor, użytkownik)	Od kiedy	Do kiedy

Miejscowość i data: [……] Podpis: [……]

Dane osobowe zawarte w oświadczeniu przetwarzamy w celu zarządzania dostępem do kont i zapewnienia ich bezpieczeństwa. Szczegóły: [odniesienie do klauzuli informacyjnej Organizacji].

Załącznik 3. Karta wyłączenia dostępu

Wypełnij, gdy osoba kończy współpracę lub zmienia rolę. Zaznacz wykonane czynności, wpisz datę i podpis.

Dane	
Imię i nazwisko osoby	[…]
Rola / funkcja	[…]
Data zakończenia współpracy	[…]
Administrator wykonujący czynności	[…]

Lp.	Czynność	Wykonano (data, podpis)
1	Wylogowano ze wszystkich sesji i urządzeń; usunięto zapamiętane logowania	
2	Poczta: zmieniono hasło lub zamknięto konto; ustawiono przekierowanie lub automatyczną odpowiedź na okres [ ]	
3	Chmura i wspólne foldery: odebrano dostęp; przeniesiono własność plików na Organizację	
4	Strona internetowa, panel domeny i hostingu: usunięto z ról i kont	
5	Media społecznościowe: usunięto z ról administratora, redaktora i moderatora	
6	Newsletter, ankiety, komunikatory, wideokonferencje, program księgowy: usunięto konto lub uprawnienia	
7	Zmieniono hasła wspólne, które osoba znała	
8	Zastąpiono numer telefonu, adres e-mail i urządzenia 2FA przypisane do kont danymi Organizacji	
9	Sprawdzono przekierowania poczty, podłączone aplikacje i integracje	
10	Zwrócono sprzęt, nośniki i klucze; potwierdzono usunięcie danych Organizacji z urządzeń prywatnych	
11	Przekazano materiały i informacje o bieżących sprawach	
12	Poinformowano osoby współpracujące o zmianie osoby kontaktowej	
13	Zaktualizowano Rejestr kont i dostępów (Załącznik 1)	

Podpis Administratora: […….] Podpis osoby kończącej współpracę: […….]

Załącznik 4. Zasady na jednej stronie

Ściągawka dla zespołu i wolontariuszy korzystających z kont [nazwa organizacji].

1. **Własne logowanie.** Każdy ma swój login. Nie dzielimy się hasłami.
2. **Długie, unikalne hasło.** Co najmniej 14 znaków, inne w każdym serwisie. Pomaga menedżer haseł.
3. **Włącz weryfikację dwuetapową** – wszędzie, gdzie jest dostępna.
4. **Kodów i haseł nikomu nie podajemy.** Także „pracownikowi banku", „serwisu" czy „prezesowi".
5. **Najpierw sprawdź, potem kliknij.** Pośpiech, groźba blokady i nieznany załącznik to sygnały ostrzegawcze.
6. **Aktualizuj telefon i komputer,** ustaw blokadę ekranu. Nie loguj się na cudzych urządzeniach.
7. **Sprawy Organizacji – na adresach Organizacji.** Nie przekierowujemy poczty na prywatne skrzynki.
8. **Publikując, pomyśl o ludziach.** Zdjęcia i dane uczestników tylko zgodnie z zasadami Organizacji. Dzieci – szczególnie ostrożnie.
9. **Zgłoś od razu, gdy coś jest nie tak.** Zgubiony telefon, dziwne logowanie, kliknięty link – zgłoś tego samego dnia. Nikt nie będzie oceniał, ważny jest czas.
10. **Kończysz współpracę?** Oddaj dostęp i sprzęt, usuń dane Organizacji z prywatnych urządzeń.

Gdy coś się stało – kontakt:
Administrator: [imię i nazwisko, telefon, e-mail]
Administrator zastępczy: [imię i nazwisko, telefon, e-mail]
Kontakt w sprawach danych osobowych: [osoba / adres]