



Fundacja ISTS
Instytut Strategii, Technologii
i Bezpieczeństwa

BEZPŁATNY PORADNIK ONLINE · WYDANIE 1 · PAŹDZIERNIK 2026

Cyber-higiena dla małych organizacji i instytucji lokalnych

Samoaudyt cyfrowy w 10 krokach dla sołectw, Kół Gospodyń Wiejskich, bibliotek i lokalnych organizacji

Sołectwa i sołtysi

Koła Gospodyń Wiejskich

Małe biblioteki

Lokalne NGO

Kluby sportowe i parafialne

Aktywni mieszkańcy

Inspirowane normami ISO/IEC 27001:2022 i ISO/IEC 42001:2023, przełożonymi na prostą praktykę dla wolontariuszy, bez żargonu i bez działu IT. Poradnik nie prowadzi do certyfikacji.

10

kroków samoaudytu z pytaniami
TAK/NIE

10

krótkich rozdziałów
praktycznych

5

wzorów gotowych do
skopiowania

Projekt „Audyt i edukacja cyfrowa dla powiatu”

Realizator: Fundacja ISTS – Instytut Strategii, Technologii i Bezpieczeństwa · powiat zduńskowski

Konkurs „Łódzkie Lokalnie NOWE FIO 2024-26” · operator: KIPR · umowa nr 25/31.08.2026



Poradnik online: aiists.netlify.app/poradnik



KIPR
Polskie NGO



**KOMITET
DO SPRAW
POŻYTKU
PUBLICZNEGO**



**NOWE
FIO**

Projekt sfinansowany ze środków Rządowego Programu Fundusz Inicjatyw Obywatelskich NOWEFIO na lata 2021–2030.

Wstęp i jak korzystać z poradnika

Sołectwo, koło gospodyń, biblioteka czy klub też ma swój „cyfrowy majątek”: skrzynkę e-mail, profil na Facebooku, konto w banku, zdjęcia z wydarzeń, listy członków i dokumenty z dotacji. Ten poradnik pomaga go uporządkować i chronić, bez kupowania drogich programów i bez informatyka na etacie.

Dla kogo jest ten poradnik

Dla osób, które działają społecznie i „przy okazji” zajmują się sprawami cyfrowymi organizacji: sołtysów i rad sołectkich, przewodniczących i członkiń KGW, bibliotekarzy w małych placówkach, zarządów stowarzyszeń, klubów sportowych i parafialnych, a także aktywnych mieszkańców. Zakładamy realną sytuację: jeden wspólny laptop w świetlicy, profil prowadzony z prywatnego telefonu i hasło, które „zna kilka osób”.

Czym różni się od poradników dla osób prywatnych

Poradniki dla seniorów i osób prywatnych uczą, jak chronić *siebie*: swoje konto w banku, telefon, dane. Ten poradnik dotyczy **organizacji**. Pytamy tu: kto ma dostęp do wspólnych kont, co się stanie, gdy skarbniczka zgubi telefon, jak przekazać profil po zmianie zarządu, kto zatwierdza przelewy, jak chronić dane uczestników i jak rozsądnie korzystać ze sztucznej inteligencji.

Jak korzystać – w pięciu ruchach

- 1 Zróbcie samoaudyt** (rozdział „Samoaudyt w 10 krokach”). Najlepiej we dwie lub trzy osoby, w 45–60 minut, z kartą z Załącznika A.
- 2 Wybierzcie trzy rzeczy do poprawy.** Nie wszystko naraz. Zaczynajcie od tego, co chroni pieniądze, dostęp do kont i dane ludzi.
- 3 Sięgnijcie do rozdziału** o tym samym numerze co krok samoaudytu. Krok 5 to rozdział 5 i tak dalej.
- 4 Skopiujcie wzory** z załączników: rejestr kont, politykę AI, procedurę przekazania kont, kartę incydentu.
- 5 Powtórzcie przegląd** co pół roku oraz zawsze po zmianie zarządu, sołtysa lub osoby prowadzącej konta.

OZNACZENIA W PORADNIKU

ISO Co mówi norma – jakiej dziedziny bezpieczeństwa dotyczy rozdział, opisane prostymi słowami. • **W 5 minut** – szybkie sprawdzenie. • **Uwaga** – częsty błąd lub pułapka. • ☐ TAK / NIE – pytanie do samoaudytu.

INSPIROWANE NORMAMI – ALE TO NIE JEST CERTYFIKACJA

Poradnik czerpie z idei dwóch międzynarodowych norm: **ISO/IEC 27001:2022** (system zarządzania bezpieczeństwem informacji, z załącznikiem A zawierającym zestaw zabezpieczeń) oraz **ISO/IEC 42001:2023** (system zarządzania sztuczną inteligencją). Opracował go audytor wewnętrzny obu norm.

Poradnik nie jest normą i jej nie zastępuje. Nie cytuje treści norm, nie prowadzi do certyfikacji i nie potwierdza zgodności z ISO/IEC 27001 ani ISO/IEC 42001. Odwołania podajemy wyłącznie na poziomie ogólnych obszarów (np. „kontrola dostępu”, „kopie zapasowe”), żeby pokazać źródło inspiracji. Pełne teksty norm są dostępne odpłatnie, m.in. w Polskim Komitecie Normalizacyjnym.

UWAGA

Poradnik zawiera praktyczne wskazówki, a nie porady prawne. W sprawach ochrony danych osobowych (RODO) i rozliczeń dotacji rozstrzygają przepisy, umowa dotacji i wytyczne grantodawcy. W razie wątpliwości zapytajcie operatora dotacji, prawnika lub sprawdźcie materiały Urzędu Ochrony Danych Osobowych (uodo.gov.pl). Wszystkie przykłady w poradniku są wymyślone.

SPIS TREŚCI

Co znajdziesz w poradniku

START

- Wstęp i jak korzystać
- ★ Samoaudyty w 10 krokach

ROZDZIAŁY

- 1 Inwentarz: co mamy
- 2 Kto ma dostęp
- 3 Hasła i logowanie
- 4 Urządzenia i telefony
- 5 Kopie zapasowe 3-2-1
- 6 Dane osobowe w praktyce
- 7 Oszustwa celujące w organizacje

- 8 AI w organizacji
- 9 Nowe technologie i VR na wydarzeniach
- 10 Plan na incydent
- + Co dalej: przegląd co pół roku

WZORY DO SKOPIOWANIA

- A Karta samoaudyty
- B Rejestr kont, dostępów i urządzeń
- C Polityka AI na jedną stronę
- D Przekazanie kont przy zmianie zarządu
- E Karta incydentu
- i Przydatne adresy i o projekcie

Samoaudyt w 10 krokach

Samoaudyt to uczciwe spojrzenie na to, jak organizacja dba o swoje konta, sprzęt, dane i pieniądze. Nie jest egzaminem. Każde „NIE” to po prostu zadanie do zrobienia.

Jak go przeprowadzić

- **Kto:** dwie lub trzy osoby, np. osoba z zarządu (sołtys, przewodnicząca, prezes), osoba prowadząca profil i skarbnik.
- **Ile czasu:** 45–60 minut. Każdy krok da się sprawdzić w około 5 minut.
- **Czego potrzebujecie:** wydruku karty z Załącznika A, telefonów i laptopa, z których korzystacie w sprawach organizacji.
- **Zasada:** zaznaczajcie TAK tylko wtedy, gdy to prawda *dziś*, a nie „prawie” albo „planujemy”.

Krok 1 Wiemy, co mamy

Dlaczego

Nie da się chronić czegoś, o czym nikt nie pamięta: starej skrzynki założonej przez byłą członkinię, zapomnianego profilu, domeny opłaconej z prywatnej karty.

Sprawdź w 5 min

Każda osoba osobno wypisuje na kartce wszystkie konta, profile, urządzenia i zbiory danych organizacji. Porównajcie listy. Różnice pokazują luki.

Co zrobić

Założcie rejestr kont i urządzeń (Załącznik B) i przypiszcie każdej pozycji osobę odpowiedzialną.

1.1 Mamy aktualną, spisaną listę kont, profili, urządzeń i ważnych plików organizacji.

☐ TAK ☐ NIE

1.2 Każda pozycja na liście ma osobę odpowiedzialną i zastępcę.

☐ TAK ☐ NIE

Więcej: rozdział 1

Krok 2 Wiemy, kto ma dostęp

Dlaczego

Dwa najczęstsze problemy to konto „na jedną osobę” (gdy odejdzie, tracimy dostęp) i hasło „znane wszystkim” (nie wiadomo, kto co zrobił, i nie da się odebrać dostępu).

Sprawdź w 5 min

Otwórzcie ustawienia strony na Facebooku i zobaczcie, kto ma do niej dostęp. Zapiszcie, kto zna hasło do poczty i kto ma dostęp do bankowości.

Co zrobić

Co najmniej dwie uprawnione osoby do kluczowych kont, żadnych „zapomnianych” administratorów. Przy zmianie zarządu stosujcie Załącznik D.

2.1 Poczta, profil/strona i bank organizacji mają co najmniej dwie uprawnione osoby, a nikt zbędny nie ma dostępu.

☐ TAK ☐ NIE

2.2 Gdy ktoś odchodzi lub zmienia się zarząd, odbieramy dostęp i zmieniamy hasła w ciągu kilku dni.

☐ TAK ☐ NIE

Więcej: rozdział 2, Załącznik D

Krok 6 Dbamy o dane osobowe ludzi

Dlaczego

Listy obecności, zdjęcia, numery telefonów w grupach na komunikatorach to dane ludzi, którzy nam zaufali. Im mniej ich zbieramy, tym mniej może wyciec.

Sprawdź w 5 min

Weźcie ostatnią listę obecności i formularz zapisu. Czy każda rubryka jest naprawdę potrzebna? Gdzie te listy teraz leżą?

Co zrobić

Minimalizacja danych, zgody na publikację wizerunku, porządek w grupach na komunikatorach.

6.1 Zbieramy tylko dane, które są potrzebne (np. bez numeru PESEL, jeśli nie wymaga go umowa dotacji), i przechowujemy je pod kontrolą.

☐ TAK ☐ NIE

6.2 Pytamy o zgodę na publikację zdjęć (dzieci – rodziców) i szanujemy odmowę.

☐ TAK ☐ NIE

Więcej: rozdział 6

Krok 7 Przelewów nie da się „wyłudzić” jednym mailem

Dlaczego

Oszuści podszywają się pod dostawców („zmieniliśmy numer konta”), pod prezesa czy sőtysa („pilnie przelej”) i pod grantodawców. Jedna rozmowa telefoniczna na znany numer zwykle wystarcza, żeby ich zatrzymać.

Sprawdź w 5 min

Zapytajcie skarbnika: co zrobi, gdy dostanie maila o zmianie numeru konta dostawcy? Kto jeszcze widzi przelew przed wystaniem?

Co zrobić

Zasada weryfikacji drugim kanałem i zasada dwóch osób.

7.1 Każdą zmianę numeru rachunku i każdą „pilną” prośbę o przelew sprawdzamy telefonicznie na wcześniej znany numer.

☐ TAK ☐ NIE

7.2 Przelewy zatwierdzają dwie osoby albo druga osoba sprawdza dane przelewu przed wystaniem.

☐ TAK ☐ NIE

Więcej: rozdział 7

Krok 8 Korzystamy z AI świadomie

Dlaczego

Czaty AI pomagają pisać posty i wnioski, ale mogą podać nieprawdę tonem eksperta, a to, co do nich wkleimy, opuszcza organizację.

Sprawdź w 5 min

Zapytajcie się nawzajem: kto z nas używa AI do spraw organizacji? Do czego? Co tam wkleja?

Co zrobić

Przyjmijcie politykę AI na jedną stronę (Załącznik C).

8.1 Mamy spisane proste zasady korzystania z AI: czego nie wklejamy i kto sprawdza wynik.

☐ TAK ☐ NIE

8.2 Każdą treść przygotowaną z pomocą AI człowiek czyta, sprawdza i poprawia przed publikacją.

☐ TAK ☐ NIE

Więcej: rozdział 8, Załącznik C

Krok 9 Nowe technologie na wydarzeniach są bezpieczne dla uczestników

Dlaczego

Gogle VR, kamery i inne nowe urządzenia przyciągają ludzi, ale mają kamery, mikrofony i konta producenta, a z goglami styka się twarz wielu osób po kolei.

Sprawdź w 5 min

Przejrzyjcie plan najbliższego wydarzenia: kto zakłada gogle, na czym koncie działa sprzęt, co trafia na ekran, czy będą dzieci?

Co zrobić

Lista kontrolna z rozdziału 9: prywatność, higiena, dobrowolność, dzieci.

9.1 Uczestnicy wiedzą, co jest pokazywane lub nagrywane, a przy dzieciach mamy zgodę rodzica lub opiekuna.

☐ TAK ☐ NIE

9.2 Udział jest dobrowolny, a sprzęt czyścimy między osobami zgodnie z instrukcją producenta.

☐ TAK ☐ NIE

Więcej: rozdział 9

Krok 10 Wiemy, co robić, gdy coś pójdzie źle

Dlaczego

Przy przejętym koncie albo złym przelewie liczą się minuty. Kto wie, do kogo dzwonić, ten szybciej ogranicza szkody.

Sprawdź w 5 min

Zadajcie pytanie: „Nasz profil właśnie publikuje reklamy oszustów. Kto co robi?”. Jeśli zapada cisza, potrzebny jest plan.

Co zrobić

Plan na incydent na jedną stronę i karta incydentu (Załącznik E).

10.1 Wszyscy wiedzą, kto koordynuje reakcję na incydent i do kogo dzwonić.

☐ TAK ☐ NIE

10.2 Mamy pod ręką kontakty: bank, CERT Polska (incydent.cert.pl, SMS 8080), osoby z dostępem do kont.

☐ TAK ☐ NIE

Więcej: rozdział 10, Załącznik E

Wynik i plan działań

Policzcie odpowiedzi TAK (maksymalnie 20).

17–20 TAK

Dobra podstawa. Utrzymujcie ją i róbcie przegląd co pół roku.

11–16 TAK

Solidny początek. Wybierzcie trzy odpowiedzi NIE i ustalcie terminy.

0–10 TAK

Zacznijcie od kroków 2, 7, 5 i 10: dostęp, przelewy, kopie, plan na incydent.

Punktacja jest orientacyjna i służy wyłącznie do planowania. Nie jest oceną zgodności z żadną normą ani przepisami.

Nasze trzy zadania na najbliższe tygodnie

Co poprawiamy	Kto	Do kiedy	Zrobione
np. dodać drugą osobę z pełnym dostępem do strony na Facebooku i włączyć 2FA	Anna (zarząd)	do końca miesiąca	☐
			☐
			☐
			☐

Systemy zarządzania z rodziny ISO opierają się na regularnym sprawdzaniu samych siebie: **audycie wewnętrznym, przeglądzie przez kierownictwo i ciągłym doskonaleniu** (zaplanuj – wykonaj – sprawdź – popraw). Samoaudyty to bardzo uproszczona wersja tej idei: patrzymy, co działa, zapisujemy, co poprawić, i wracamy do tego po pewnym czasie.

ROZDZIAŁ 1

Inwentarz: co mamy

Organizacja ma zwykle więcej cyfrowego majątku, niż się wydaje. Spis zajmuje jedno spotkanie, a potem oszczędza nerwów przy każdej zmianie zarządu.

Co wpisać do inwentarza

Grupa	Przykłady
Konta	skrzynka e-mail organizacji, bankowość internetowa, dysk w chmurze (np. Google Drive, OneDrive), Canva, konta na platformach grantowych i urzędowych, konto producenta sprzętu (np. gogli VR)
Strony i profile	strona i grupa na Facebooku, Instagram, kanał YouTube, strona internetowa i domena, wizytówka w Mapach Google
Urządzenia	laptop w świetlicy, telefon organizacji, tablet, pendrive'y i dyski zewnętrzne, aparat, gogle VR, router Wi-Fi
Dane i dokumenty	lista członków, listy obecności, zgody na wizerunek, zdjęcia i nagrania, protokoły, umowy i dokumenty dotacji, faktury, korespondencja
Płatności i terminy	kto płaci za domenę, hosting, abonament; na czyje dane jest zarejestrowana usługa; kiedy wygasa

Jak to zrobić w praktyce

- 1 Umówcie się na 30 minut z osobami, które prowadzą konta. Weźcie telefony i laptop.
- 2 Wypełnijcie rejestr z Załącznika B. **Nie wpisujecie do niego haseł**, tylko informację, gdzie są przechowywane (np. „menedżer haseł, sejf”).
- 3 Dla każdej pozycji wskaźcie **osobę odpowiedzialną i zastępcę**.
- 4 Oznaczcie, co jest najważniejsze: wszystko, co dotyczy **pieniędzy, danych osobowych i wizerunku** organizacji.
- 5 Przechowujcie rejestr w bezpiecznym miejscu i aktualizujcie go przy każdej zmianie.

UWAGA – TYPOWE PUŁAPKI

- Konto organizacji założone na **prywatny e-mail lub telefon** osoby, która już nie działa w organizacji. Odzyskanie dostępu bywa wtedy bardzo trudne.
- Domena opłacana z prywatnej karty. Gdy karta wygaśnie, strona znika, a adres może kupić ktoś obcy.
- Stary, porzucony profil, który ktoś może przejąć i wykorzystać do podszywania się pod organizację.

W 5 MINUT

Wpiszcie w wyszukiwarkę i na Facebooku nazwę organizacji. Czy wszystkie znalezione profile i strony są Wasze i czy macie do nich dostęp? Jeśli nie – dopiszcie je do rejestru i zdecydujcie: odzyskać, zamknąć czy zgłosić jako podszywanie się.

ISO CO MÓWI NORMA

Bezpieczeństwo informacji zaczyna się od **inwentaryzacji aktywów**: organizacja wie, jakie ma informacje, konta i sprzęt, a każdy zasób ma **właściciela**, czyli osobę, która za niego odpowiada. Ustala też zasady **dopuszczalnego korzystania** z tych zasobów. W małej organizacji wystarczy do tego jedna tabela.

ROZDZIAŁ 2

Kto ma dostęp

Dwie proste zasady: **każdy ma tyle dostępu, ile potrzebuje do swojego zadania, i do każdego kluczowego konta mają dostęp co najmniej dwie osoby.**

Role zamiast wspólnego hasła

Rola	Kto zwykle	Zakres dostępu
Administrator	2 osoby z zarządu	pełny dostęp, dodawanie i usuwanie osób, ustawienia bezpieczeństwa
Redaktor / moderator	osoba prowadząca profil	publikowanie, odpowiadanie na wiadomości; bez zmiany administratorów
Finanse	skarbnik + osoba zatwierdzająca	bankowość według pełnomocnictw w banku
Wolontariusz	osoba pomagająca przy wydarzeniu	tylko to, co potrzebne, i tylko na czas zadania

Strona na Facebooku: zamiast dzielić się hasłem, nadajcie dostęp do strony konkretnym osobom w jej ustawieniach. Każda osoba loguje się swoim kontem z włączonym 2FA. Nie zakładajcie „wspólnego konta prywatnego” na fikcyjną osobę – regulamin Facebooka tego zabrania, a takie konta są łatwo blokowane. Pełny dostęp powinny mieć co najmniej dwie zaufane osoby.

Sołectwo: profil i skrzynka powinny należeć do sołectwa, a nie do prywatnego konta obecnego sołtysa. Po wyborach nowa osoba przejmuje konta sołectwa, a prywatne konto poprzednika zostaje prywatne.

Wspólna skrzynka e-mail

- Używajcie adresu organizacji (np. *kontakt@...* albo *kgw.nazwa@...*), a nie prywatnego adresu członka.
- Hasło przechowujcie w menedżerze haseł z funkcją bezpiecznego udostępniania. Zapiszcie w rejestrze, kto je zna.
- Jeśli usługa na to pozwala, korzystajcie z **delegowania dostępu** lub skrzynki współdzielonej. Wtedy każdy loguje się swoim kontem i nie trzeba podawać hasła.
- Telefon i e-mail do odzyskiwania konta powinny należeć do organizacji albo do dwóch osób z zarządu, nie do kogoś przypadkowego.

Menedżer haseł – sejf na wszystkie hasła

Menedżer haseł to program, który przechowuje hasła w zaszyfrowanej postaci, podpowiada je przy logowaniu i tworzy nowe, trudne do odgadnięcia. Pamiętajcie tylko jedno, mocne hasło główne. Są wersje bezpłatne i wersje dla organizacji z udostępnianiem haseł w zespole. Przykłady to m.in. Bitwarden (w chmurze) lub KeePassXC (plik na komputerze). Podajemy je jako przykłady, nie jako rekomendację handlową.

UWAGA

Hasła głównego do menedżera zwykle **nie da się odzyskać**. Zapiszcie je wraz z kodami odzyskiwania na kartce, włóżcie do zaklejonej, podpisanej koperty i przechowujcie w zamkniętym miejscu (np. sejf, szafa zarządu). Kopertę otwiera się tylko w sytuacji awaryjnej, a po jej otwarciu zmienia hasło.

Odejście członka i zmiana zarządu

Najwięcej problemów z dostępem pojawia się przy zmianach osób. Zasada: **przekazujemy konta przed odejściem, a nie po**. Pełna lista kroków jest w Załączniku D. Najważniejsze:

- spiszcie protokół przekazania (lista kont i urządzeń, bez haseł);
- dodajcie nowe osoby jako administratorów, zanim usuniecie dotychczasowe;
- zmieńcie hasła i dane do odzyskiwania (telefon, e-mail zapasowy), wylogujcie wszystkie sesje;
- odbierzcie sprzęt organizacji, klucze i nośniki;
- zaktualizujcie w banku listę osób uprawnionych – zwykle wymaga to dokumentów (np. uchwały, odpisu z rejestru), więc zacznijcie wcześniej.

Rozstanie w zgodzie czy w sporze – procedura jest ta sama. Dzięki temu nikt nie czuje się podejrzan.

ISO CO MÓWI NORMA

To obszar **kontroli dostępu i zarządzania tożsamością**. Dostęp nadaje się świadomie, według potrzeb zadania (zasada najmniejszych uprawnień), regularnie się go przegląda i odbiera, gdy ktoś zmienia rolę lub odchodzi. Do tego dochodzi **zwrot aktywów**: sprzęt i informacje wracają do organizacji, a ważne obowiązki nie spoczywają na jednej osobie.

ROZDZIAŁ 3

Hasła i logowanie

Jak tworzyć dobre hasło, wie już wiele osób. Tu chodzi o coś innego: o wspólne zasady dla całej organizacji, żeby hasła nie krążyły po czatach i karteczkach.

Zasady haseł naszej organizacji – w sześciu zdaniach

1. Każde konto organizacji ma **inne hasło**.
2. Hasło ma **co najmniej 12 znaków**. Najlepiej sprawdza się hasło-zdanie z kilku przypadkowych słów, łatwe do zapamiętania i trudne do odgadnięcia.
3. Hasła przechowujemy w **menedżerze haseł**, a hasła awaryjne w zaklejonej kopercie. Nigdy w Messengerze, WhatsAppie, SMS-ie, e-mailu ani na karteczce.
4. Na wszystkich ważnych kontach mamy włączone **logowanie dwuetapowe (2FA)**.
5. Na wspólnym komputerze **nie zapisujemy haseł w przeglądarce** i wylogowujemy się po pracy.
6. Hasło zmieniamy od razu, gdy: ktoś z dostępem odchodzi, podejrzewamy wyciek, hasło zostało komuś podane „na chwilę”.

Logowanie dwuetapowe w organizacji

Logowanie dwuetapowe oznacza, że oprócz hasła potrzebny jest drugi składnik: kod z aplikacji, potwierdzenie w telefonie, klucz sprzętowy albo kod SMS. Od najmocniejszego:

- **klucz sprzętowy lub klucz dostępu (passkey)** – najbardziej odporne na fałszywe strony logowania;
- **aplikacja uwierzytelniająca** w telefonie (np. Google Authenticator, Microsoft Authenticator);
- **kod SMS** – słabszy, ale wciąż dużo lepszy niż samo hasło.

UWAGA – PROBLEM TYPOWY DLA ORGANIZACJI

Kod przychodzi na **prywatny telefon jednej osoby**. Gdy ta osoba zmieni numer, zgubi telefon albo odejdzie, organizacja traci dostęp. Dlatego: dodajcie drugą metodę lub drugą osobę, a **kody zapasowe** (jednorazowe kody odzyskiwania, które daje większość serwisów) wydrukujcie i schowajcie do koperty awaryjnej lub zapiszcie w menedżerze haseł.

Sprawdźcie, czy adres organizacji nie wyciekł

Na stronie **haveibeenpwned.com** można wpisać adres e-mail i sprawdzić, czy pojawił się w znanych wyciekach danych. Jeśli tak, zmieńcie hasło do tego serwisu i wszędzie tam, gdzie było takie samo.

ZŁOTA ZASADA

Kodu z SMS-a ani kodu z aplikacji nie podajemy nikomu – także „pracownikowi Facebooka”, „bankowi” czy „koleżance z koła, która prosi o pomoc w głosowaniu”. Prawdziwa firma nigdy o niego nie poprosi.

ISO CO MÓWI NORMA

To obszar **bezpiecznego uwierzytelniania i ochrony informacji uwierzytelniających**, czyli haseł, kodów i kluczy. Organizacja przydziela je i przechowuje w kontrolowany sposób, a osoby korzystające z kont wiedzą, jak o nie dbać. Spisane zasady haseł to najprostsza forma takiej polityki.

ROZDZIAŁ 4

Urządzenia i telefony

W małej organizacji sprawy prowadzi się na wspólnym laptopie w świetlicy albo na prywatnych telefonach. To normalne. Wystarczy kilka ustawień, żeby było bezpiecznie.

Wspólny komputer (świetlica, biblioteka, biuro)

- ☐ **Osobne konta użytkowników:** jedno dla organizacji (z hasłem), osobne dla gości lub uczestników zajęć. Goście nie widzą plików organizacji.
- ☐ **Hasło lub PIN** i automatyczna blokada ekranu po kilku minutach. Odchodząc od komputera, naciśnij **Windows + L**.
- ☐ **Automatyczne aktualizacje** systemu i przeglądarki włączone. Komputer raz na jakiś czas trzeba też uruchomić ponownie, żeby aktualizacje się zainstalowały.
- ☐ **Ochrona antywirusowa** włączona (w Windows wbudowany jest program Microsoft Defender). Programy instalujemy tylko z oficjalnych źródeł.
- ☐ **Przeglądarka nie zapamiętuje haseł** na koncie wspólnym. Komputer publiczny w bibliotece: tryb prywatny i wylogowanie po każdej osobie.
- ☐ **Szyfrowanie dysku**, jeśli system je oferuje. Wtedy skradziony laptop nie zdradza danych.

Prywatny telefon do spraw organizacji

To najczęstsza sytuacja i nie trzeba jej zakazywać. Ustalcie jednak minimum, które spełnia każdy telefon z dostępem do kont organizacji:

- ☐ **Blokada ekranu** (PIN co najmniej 6 cyfr, wzór lub biometria) i krótki czas do zablokowania.
- ☐ **Aktualny system** i aplikacje tylko z oficjalnego sklepu (Google Play, App Store).
- ☐ **Włączona funkcja lokalizowania i zdalnego czyszczenia:** „Znajdź moje urządzenie” (Android) lub „Lokalizator” (iPhone).
- ☐ **Zdjęcia uczestników** (zwłaszcza dzieci) po wydarzeniu przenosimy do folderu organizacji i usuwamy z telefonu. Pamiętajmy, że mogą się automatycznie kopiować do prywatnej chmury.
- ☐ **Po odejściu z funkcji** wylogowujemy się z kont organizacji na telefonie i usuwamy jej pliki.

Uprawnienia aplikacji – przegląd raz na kwartał

W ustawieniach telefonu (zwykle: *Ustawienia* → *Prywatność* lub *Aplikacje* → *Uprawnienia*) sprawdźcie, które aplikacje mają dostęp do **aparatu, mikrofonu, lokalizacji, kontaktów i zdjęć**. Edytor zdjęć nie potrzebuje kontaktów, a latarka – lokalizacji. Odbierzcie zbędne uprawnienia i usuńcie aplikacje, których nikt nie używa.

Pendrive'y, Wi-Fi i stary sprzęt

- **Znalezionego pendrive'a nie podłączamy.** Plików z danymi osobowymi nie nosimy na niezaszyfrowanych nośnikach.
- **Router w świetlicy:** zmieńcie domyślne hasło do panelu administracyjnego i hasło do Wi-Fi. Jeśli router na to pozwala, utwórzcie osobną sieć dla gości.
- **Sprzedaż, przekazanie lub wyrzucenie sprzętu:** wylogujcie konta, usuńcie urządzenie z konta Google/Apple/Microsoft, przywróćcie ustawienia fabryczne. Dysk z danymi, którego nie da się wyczyścić, trzeba fizycznie zniszczyć.

ISO CO MÓWI NORMA

Ten rozdział łączy kilka obszarów: **urządzenia końcowe użytkowników, zarządzanie podatnościami technicznymi** (czyli aktualizacje), **ochronę przed złośliwym oprogramowaniem**, zasadę **czystego biurka i czystego ekranu** oraz **bezpieczne usuwanie lub ponowne użycie sprzętu**. Zasady dotyczą także urządzeń prywatnych, jeśli korzysta się na nich z informacji organizacji.

Kopie zapasowe 3-2-1 i test odtworzenia

Dokumentację dotacji trzeba często przechowywać przez kilka lat. Zdjęcia z jubileuszu koła są nie do odtworzenia. Kopia zapasowa to najtańsze ubezpieczenie organizacji.

Zasada 3-2-1

3

kopie danych: oryginał i dwie kopie

2

różne nośniki lub miejsca, np.
chmura i dysk zewnętrzny

1

kopia poza siedzibą, np. w chmurze
lub u drugiej osoby

PRZYKŁAD DLA KOŁA GOSPODYŃ LUB STOWARZYSZENIA

Oryginał: folder organizacji na dysku w chmurze. **Kopia 1:** dysk zewnętrzny w szafie zarządu, kopiowanie raz w miesiącu. **Kopia 2:** drugi dysk zewnętrzny u skarbnika, wymieniany co kwartał. Dyski są podpisane, zaszyfrowane lub trzymane pod kluczem, bo zawierają dane osobowe.

Co kopiować w pierwszej kolejności

1. dokumenty dotacji i finansowe (umowy, faktury, sprawozdania, listy obecności);
2. dokumenty organizacji (statut, uchwały, protokoły, rejestr członków);
3. zgody i oświadczenia uczestników;
4. zdjęcia i nagrania z wydarzeń – także te, które leżą na prywatnych telefonach;
5. rejestr kont i dostępów (Załącznik B) oraz plan na incydent.

UWAGA – SYNCHRONIZACJA TO NIE KOPIA

Jeśli folder synchronizuje się z chmurą, to usunięcie lub zaszyfrowanie pliku na komputerze zwykle przenosi się też do chmury. Pomaga kosz i historia wersji w usłudze chmurowej – sprawdźcie, przez ile dni są przechowywane. Dysk zewnętrzny **odłączajcie po zrobieniu kopii**: podłączony na stałe może zostać zaszyfrowany razem z komputerem przez złośliwe oprogramowanie.

Test odtworzenia – raz na pół roku

1. Wybierzcie losowo kilka plików (np. jeden dokument, jedno zdjęcie, jeden arkusz).
2. Odtwórzcie je z kopii na **innym** komputerze lub do innego folderu.
3. Otwórzcie pliki i sprawdźcie, czy są kompletne i aktualne.
4. Zapiszcie datę testu i wynik w rejestrze. Jeśli się nie udało – poprawcie sposób robienia kopii.

Kopia, której nikt nigdy nie sprawdził, to tylko nadzieja. Pamiętajcie też o profilach społecznościowych: Facebook pozwala pobrać kopię informacji ze strony. Raz w roku warto ją zapisać razem z innymi kopiami.

To obszar **kopii zapasowych informacji**: kopie wykonuje się regularnie według ustalonych zasad i **sprawdza się, czy da się z nich odtworzyć dane**. Łączy się z obszarem **ciągłości działania**: organizacja wie z góry, jak wróci do pracy po awarii, kradzieży czy ataku, zamiast improwizować w stresie.

ROZDZIAŁ 6

Dane osobowe w praktyce

Organizacje lokalne przetwarzają dane sąsiadów, dzieci i seniorów. Najlepsza ochrona jest prosta: zbierać mniej, wiedzieć, gdzie dane leżą, i nie udostępniać ich szerzej, niż trzeba.

Wskazówki praktyczne, nie porada prawna. Obowiązki wynikają z RODO, przepisów krajowych i umów dotacji. Materiały dla organizacji publikuje Urząd Ochrony Danych Osobowych (uodo.gov.pl).

Minimalizacja: zbieraj tylko to, czego potrzebujesz

- Lista obecności zawiera tylko rubryki wymagane przez grantodawcę lub cel spotkania. Jeśli nie trzeba numeru PESEL, adresu czy telefonu – nie zbieramy ich „na wszelki wypadek”.
- Na liście lub formularzu umieszczamy krótką informację: kto zbiera dane, w jakim celu, jak długo je przechowuje i do kogo można się zgłosić.
- Dane o zdrowiu (np. dieta, alergie, niepełnosprawność przy wycieczce) zbieramy tylko wtedy, gdy są niezbędne, trzymamy osobno i usuwamy po wydarzeniu.

Listy obecności i dokumenty papierowe

- Po wydarzeniu lista nie zostaje na stole. Trafia do teczki i do zamkniętej szafy.
- Nie fotografujemy list z danymi telefonem „dla siebie” i nie publikujemy ich zdjęć.
- Skany trzymamy w folderze z dostępem tylko dla osób, które go potrzebują – nie w folderze udostępnionym „każdemu, kto ma link”.
- Przechowujemy je tak długo, jak wymaga umowa dotacji lub przepisy, a potem niszczymy (niszczarka, nie kosz na papier).

Zdjęcia i zgody

- Na początku wydarzenia mówimy, że robimy zdjęcia i gdzie je opublikujemy.
- Na publikację zdjęć, na których ktoś jest wyraźnie widoczny, prosimy o zgodę. W przypadku **dzieci zgodę wyraża rodzic lub opiekun**.
- Dajemy łatwy sposób odmowy, np. kolorową naklejkę „bez zdjęć” albo miejsce na sali poza kadrem. Odmowa nie ma żadnych konsekwencji.
- Nie podpisujemy zdjęć dzieci imieniem i nazwiskiem ani nazwą szkoły czy klasy.
- Na prośbę osoby szybko usuwamy zdjęcie z profilu.

Grupy na Messengerze i WhatsAppie

Grupy są świetne do szybkiej informacji, ale nie nadają się na archiwum dokumentów. Zasady:

- Grupa ma dwie osoby administrujące. Osoby, które odeszły z organizacji, usuwamy z grupy.
- Pamiętamy, że **wszyscy członkowie grupy widzą numery telefonów** lub profile pozostałych. Mówimy o tym nowym osobom.
- W grupie **nie wysyłamy** skanów dowodów, list z danymi, informacji o zdrowiu ani haset.

- Do ogłoszeń dla wielu osób lepszy jest kanał, w którym piszą tylko administratorzy (np. ustawienie „tylko administratorzy mogą wysyłać wiadomości”).
- E-mail do wielu osób spoza zarządu wysyłamy w polu **UDW** (ukryta kopia), żeby nie ujawniać adresów wszystkim odbiorcom.

Proste oznaczanie informacji

Poziom	Przykłady	Jak postępujemy
PUBLICZNE	plakat, ogłoszenie, relacja z wydarzenia (za zgodą osób)	można publikować
WEWNĘTRZNE	protokoły zebrań, plany, korespondencja zarządu	tylko członkowie, bez publikacji
POUFNE	listy z danymi osobowymi, zgody, dane o zdrowiu, dane bankowe, hasła	tylko osoby, które muszą, w zamkniętym folderze lub szafie

UWAGA – GDY DANE TRAFIĄ W NIEPOWOŁANE RĘCE

Lista wysłana do niewłaściwej osoby, zgubiony pendrive, przejęta skrzynka – to naruszenie ochrony danych. Postępujcie według rozdziału 10. Administrator danych może mieć obowiązek zgłoszenia naruszenia do Prezesa UODO w ciągu 72 godzin od jego stwierdzenia. Sprawdźcie to od razu na uodo.gov.pl lub zapytajcie prawnika.

ISO CO MÓWI NORMA

Ten rozdział nawiązuje do obszarów **prywatności i ochrony danych osobowych, klasyfikacji i oznaczania informacji** (co jest publiczne, wewnętrzne, poufne) oraz **bezpiecznego przekazywania informacji**. Normy nie zastępują przepisów o ochronie danych – oczekują, że organizacja je zna, stosuje i ma na to praktyczne sposoby.

ROZDZIAŁ 7

Oszustwa celujące w organizację

Organizacje mają rachunek bankowy, profil z wieloma obserwującymi i dobre imię w okolicy. Oszuści o tym wiedzą. Ich metody bazują na pośpiechu, autorytecie i zaufaniu.

Fałszywa faktura lub „zmiana numeru konta”

Jak to wygląda: e-mail „od dostawcy” (catering, drukarnia, sklep z koszulkami): „Zmieniliśmy bank, prosimy o przelew na nowy rachunek”. Bywa wysłany z łudząco podobnego adresu albo z przejętej, prawdziwej skrzynki dostawcy.

Co robimy: zmianę numeru potwierdzamy telefonicznie na numer z umowy lub wcześniejszej korespondencji, nigdy z tego maila. Rachunek firmy będącej czynnym podatnikiem VAT można sprawdzić w wykazie podatników VAT („biała lista”) na podatki.gov.pl.

„Prezes prosi o pilny przelew”

Jak to wygląda: SMS, wiadomość na komunikatorze lub e-mail „od prezesa, sołtysa, proboszcza”: „Jestem na spotkaniu, nie mogę rozmawiać. Pilnie przelej... Nikomu nie mów”. Może to być nawet podrobiony głos w telefonie.

Co robimy: rozłączamy się i oddzwaniamy na numer zapisany w telefonie. Żadna prawdziwa prośba nie ucierpi przez pięć minut sprawdzania.

AI w organizacji

Czaty AI, tłumacze i generatory grafik pomagają napisać post, plakat czy szkic wniosku. Warto z nich korzystać – z głową. Ten rozdział inspirowany jest normą o zarządzaniu sztuczną inteligencją, ISO/IEC 42001.

Korzyści i ryzyka w skrócie

Co AI daje	Na co uważać
szybszy szkic posta, zaproszenia, podziękowań; streszczenie długiego regulaminu; tłumaczenie; pomysły na wydarzenie; prosta grafika	pewnie brzmiące nieprawdy (tzw. halucynacje); wyciek danych wklejonych do czatu; prawa autorskie i wizerunek; podrobione nagrania (deepfake); bezkrytyczne zaufanie

Prosta polityka AI na jedną stronę

Gotowy wzór jest w **Załączniku C**. Wystarczy go przyjąć na zebraniu, uzupełnić i wywiesić. Zawiera m.in.: kto odpowiada za AI w organizacji, z jakich narzędzi korzystamy, czego nie wklejamy, kto sprawdza treści i jak je oznaczamy.

Czego nie wklejamy do narzędzi AI

- ☐ danych osobowych: list uczestników, numerów PESEL, adresów, telefonów, zdjęć osób;
- ☐ danych o zdrowiu, sytuacji rodzinnej i materialnej, informacji o dzieciach;
- ☐ haseł, kodów, danych logowania i danych bankowych;
- ☐ dokumentów wewnętrznych i poufnych (spory w zarządzie, niepublikowane umowy, skany dokumentów);
- ☐ nagrań głosu i wizerunku innych osób bez ich zgody.

Zamiast tego **anonimizujemy**: „uczestniczka, 70 lat” zamiast imienia i nazwiska; opis sytuacji zamiast skanu. W ustawieniach wielu usług można wyłączyć wykorzystywanie rozmów do trenowania modeli – sprawdźcie to w swoim narzędziu.

AI pisze szkic, człowiek odpowiada

- **Weryfikacja:** każdą datę, kwotę, nazwę, przepis, cytat i link sprawdzamy w źródle (regulaminie konkursu, na stronie urzędu). AI potrafi wymyślić nieistniejący paragraf lub termin.
- **Oznaczenie:** realistyczne obrazy, nagrania i głos wygenerowane przez AI podpisujemy, np. „Grafika wygenerowana z pomocą AI”. Przepisy UE o sztucznej inteligencji (AI Act) przewidują obowiązki przejrzystości m.in. dla treści typu deepfake. Uczciwe oznaczanie buduje zaufanie mieszkańców.
- **Wizerunek:** nie generujemy realistycznych obrazów ani głosu prawdziwych osób (np. wójta, sołtysa, członkiń koła) bez ich zgody.
- **Człowiek decyduje:** AI nie decyduje o ludziach – o przyjęciu do organizacji, przyznaniu nagrody, ocenie prac dzieci w konkursie czy wyborze wolontariuszy. Może pomóc uporządkować informacje, ale decyzję i odpowiedzialność ponosi człowiek.

UWAGA – DEEPPAKE GŁOSU I OBRAZU

Wystarczy krótkie nagranie, by podrobić czyjś głos. „Sołtys” w telefonie prosi o przelew, „wójt” na nagraniu zachęca do „inwestycji”. Zasada pozostaje ta sama: **sprawdzamy drugim kanałem**, a w zarządzie mamy słowo-hasło (rozdział 7). Fałszywe nagrania z wizerunkiem osób z organizacji zgłaszamy platformie i opisujemy w karcie incydentu.

Ocena ryzyka użycia AI w 4 pytaniach

Zanim zaczniecie używać AI do nowego zadania, odpowiedzcie:

1. **Jakie dane trafią do narzędzia?** Jeśli osobowe lub poufne – stop albo anonimizacja.
2. **Kogo może dotknąć błąd?** Ludzi, pieniądze, dobre imię organizacji?
3. **Kto i jak sprawdzi wynik**, zanim zostanie użyty?
4. **Czy odbiorcy powinni wiedzieć**, że użyliśmy AI?

Przykład użycia	Ocena	Warunek
szkic posta o zebraniu wiejskim	niskie ryzyko	przeczytać i poprawić przed publikacją
streszczenie regulaminu konkursu grantowego	średnie	terminy i warunki sprawdzić w oryginale
grafika z realistyczną osobą na plakat	średnie	bez wizerunku prawdziwych osób, z oznaczeniem AI
porządkowanie listy uczestników z danymi	wysokie	nie wklejać danych osobowych
ocena i ranking zgłoszeń w konkursie	wysokie	decyduje komisja; AI najwyżej jako pomoc techniczna

ISO CO MÓWI NORMA

ISO/IEC 42001 opisuje **system zarządzania sztuczną inteligencją**. Jego idee to m.in.: **polityka AI**, przypisane **role i odpowiedzialność**, **ocena ryzyka AI** i **ocena wpływu** zastosowań AI na ludzi i społeczność, **odpowiedzialne korzystanie** z AI, dbałość o **dane**, **informowanie** zainteresowanych oraz rozsądny wybór **dostawców**. W małej organizacji: jedna strona zasad, jedna osoba odpowiedzialna i cztery pytania przed nowym użyciem.

ROZDZIAŁ 9

Nowe technologie i VR na wydarzeniach

Gogle wirtualnej rzeczywistości, kamery czy interaktywne pokazy przyciągają mieszkańców w każdym wieku. Zanim sprzęt trafi w ręce uczestników, zadbajcie o prywatność, higienę i bezpieczeństwo.

Prywatność

- ☐ Sprzęt działa na **koncie organizacji** z 2FA, a nie na prywatnym koncie wolontariusza. Do konta nie podpinamy karty płatniczej albo blokujemy zakupy PIN-em.
- ☐ Pamiętamy, że gogle VR mają **kamery i mikrofony** do śledzenia otoczenia. Nie używamy ich tam, gdzie leżą dokumenty z danymi.
- ☐ Jeśli obraz z gogli jest **wyświetlany na ekranie** lub nagrywany, mówimy o tym uczestnikowi przed założeniem gogli.
- ☐ Po wydarzeniu **usuwamy zrzuty ekranu i nagrania** uczestników, chyba że mamy zgodę na ich wykorzystanie.
- ☐ Instalujemy tylko aplikacje ze sklepu producenta, sprawdzone wcześniej przez osobę prowadzącą.

Higiena i dbałość o sprzęt

- Jednorazowe nakładki higieniczne lub wymienne wyściółki; przecieranie części stykających się z twarzą między osobami środkami zgodnymi z instrukcją producenta.
- Soczewki czyścimy suchą ściereczką z mikrofibry, bez płynów.
- Gogli nie zostawiamy na stołcu – światło skupione przez soczewki może uszkodzić wyświetlacz.

Bezpieczeństwo, dobrowolność i dzieci

- **Wolna przestrzeń** wokół osoby w goglach i **asystent obok**. Osobom z zawrotami głowy proponujemy pozycję siedzącą i krótkie sesje.
- Przekazujemy **ostrzeżenia zdrowotne producenta** (np. dotyczące padaczki i choroby lokomocyjnej) i każdemu pozwalamy przerwać w dowolnym momencie.
- **Udział jest dobrowolny**. Zawsze jest alternatywa, np. oglądanie pokazu na ekranie. Bez namawiania i presji grupy.
- **Dzieci**: przestrzegamy minimalnego wieku podanego przez producenta, mamy zgodę rodzica lub opiekuna, skracamy czas sesji, opiekun jest obok. Nie zakładamy dzieciom kont.

NOWE URZĄDZENIE W ORGANIZACJI – LISTA PRZED PIERWSZYM UŻYCIEM

- ☐ wpisane do inwentarza (Załącznik B) z osobą odpowiedzialną;
- ☐ zmienione domyślne hasła i PIN-y, zainstalowane aktualizacje;
- ☐ konto organizacji z 2FA, przejrane ustawienia prywatności i udostępniania;
- ☐ krótka ocena ryzyka: jakie dane zbiera urządzenie, kogo dotyczy, co może pójść źle.

ISO CO MÓWI NORMA

Ten rozdział łączy obszary **bezpieczeństwa fizycznego sprzętu, prywatności i zarządzania zmianą** (nowe urządzenie to zmiana, którą warto przemyśleć przed wdrożeniem). Z normy o AI pochodzi idea **oceny wpływu** technologii na ludzi – także na dzieci i osoby wrażliwe – zanim zaczniesz się z niej korzystać.

ROZDZIAŁ 10

Plan na incydent

Incydent to każde zdarzenie, które zagraża kontom, pieniądзом, danym lub dobremu imieniu organizacji: przejęty profil, przelew do oszusta, zgubiony telefon z dostępem do kont, zaszyfrowane pliki, wyciek listy uczestników, fałszywy profil podszywający się pod organizację.

Kto dzwoni do kogo – uzupełnijcie i wywieście

Koordynator incydentu: _____ tel. _____

Zastępca: _____ tel. _____

Finanse / bank: _____ tel. _____

Administrator profilu: _____ tel. _____

Infolinia banku (numer z karty lub oficjalnej strony banku): _____

Wsparcie techniczne (zaufana osoba): _____

CERT Polska: zgłoszenie incydentu na **incydent.cert.pl** · podejrzany SMS przekaz bezpłatnie na numer **8080** · **Policja**: w nagłej sytuacji 112, zawiadomienie o oszustwie – najbliższa jednostka

Zasada: **kto zauważy problem, od razu dzwoni do koordynatora**, a nie próbuje sam „naprawić po cichu”.

Cztery kroki

1 Zatrzymaj

Nie klikaj dalej, nie płać, nie odpowiadaj oszustowi. Komputer, na którym dzieje się coś dziwnego (np. pliki zmieniają nazwy, pojawia się żądanie okupu), **odłącz od internetu**. Okupu nie płacimy.

2 Zabezpiecz

Przy przelewie: **natychmiast dzwoń do banku**. Zmień hasła z innego, sprawnego urządzenia, wyloguj wszystkie sesje, sprawdź w poczcie reguły przekazywania i dane do odzyskiwania konta. Profil na Facebooku odzyskuj przez facebook.com/hacked.

3 Zgłoś

CERT Polska (incydent.cert.pl), policja przy oszustwie finansowym, platforma (fałszywy profil, przejęta strona). Przy wycieku danych osobowych – sprawdź obowiązek zgłoszenia do UODO (72 godziny). Jeśli dotyczy to środków lub sprzętu z dotacji – poinformuj operatora. Ostrzeż odbiorców: „Nasz profil został przejęty, nie klikajcie linków”.

4 Zapisz i wyciągnij wnioski

Wypełnij kartę incydentu (Załącznik E). Zachowaj dowody: zrzuty ekranu, e-maile, numery, godziny – nie kasuj ich. Po wszystkim omówcie na zebraniu, co zmienić, **bez szukania winnych**.

PRZEĆWICZCIE TO W 15 MINUT

Na najbliższym zebraniu przeczytajcie na głos scenariusz: „Skarbnik dostał e-mail od drukarni o zmianie numeru konta i już zlecił przelew”. Kto co robi? Do kogo dzwoni? Gdzie jest numer do banku? Zapiszcie, czego zabrakło.

UWAGA – KULTURA ZGŁASZANIA

Osoba, która kliknęła w zły link, powinna móc to powiedzieć od razu i bez wstydu. Każda minuta zwłoki działa na korzyść oszusta. Dziękujcie za zgłoszenia.

ISO CO MÓWI NORMA

To obszar **zarządzania incydentami bezpieczeństwa informacji**: przygotowanie (role, kontakty, procedury), ocena zdarzeń, reakcja, **wyciąganie wniosków** i **zabezpieczanie dowodów**. Ważne jest też **zgłaszanie zdarzeń** – każdy w organizacji wie, jak i komu zgłosić niepokojącą sytuację.

CO DALEJ

Przegląd co pół roku

Bezpieczeństwo to nawyk, nie jednorazowa akcja. Wystarczy krótki przegląd dwa razy w roku i po każdej zmianie zarządu. Ten cykl to znana z norm zasada **ciągłego doskonalenia**.

1 Zaplanuj

Wpiszcie przegląd do kalendarza organizacji, np. przy zebraniu wiosennym i jesiennym.

2 Wykonaj

Zróbcie zadania z planu działań z samoaudytu i zaktualizujcie rejestr kont.

3 Sprawdź

Powtórzcie samoaudyt, test odtworzenia kopii i przegląd osób z dostępem.

4 Popraw

Wybierzcie trzy kolejne zadania. Zapiszcie wnioski z incydentów, jeśli jakieś były.

Karta samoaudytu

Organizacja: _____ Data: _____
 Osoby wypełniające: _____ Następny przegląd: _____

Nr	Pytanie	TAK	NIE
1.1	Mamy aktualną listę kont, profili, urządzeń i ważnych plików.	☐	☐
1.2	Każda pozycja ma osobę odpowiedzialną i zastępcę.	☐	☐
2.1	Pocztą, profil i bank mają co najmniej dwie uprawnione osoby; nikt zbędny nie ma dostępu.	☐	☐
2.2	Przy odejściu osoby lub zmianie zarządu odbieramy dostęp i zmieniamy hasła w ciągu kilku dni.	☐	☐
3.1	Pocztą, profil i bank mają włączone logowanie dwuetapowe.	☐	☐
3.2	Hasła są w menedżerze haseł lub zapieczętowanej kopercie, nie na kartce ani w czacie.	☐	☐
4.1	Urządzenia z dostępem do kont (także prywatne telefony) mają blokadę ekranu i aktualny system.	☐	☐
4.2	Wspólny komputer nie zapamiętuje haseł, goście mają osobne konto.	☐	☐
5.1	Najważniejsze pliki są w co najmniej dwóch miejscach, jedno poza siedzibą.	☐	☐
5.2	W ostatnich 6 miesiącach udało się odtworzyć plik z kopii.	☐	☐
6.1	Zbieramy tylko potrzebne dane i przechowujemy je pod kontrolą.	☐	☐
6.2	Pytamy o zgodę na publikację zdjęć (dzieci – rodziców) i szanujemy odmowę.	☐	☐
7.1	Zmianę numeru rachunku i „pilne” przelewy sprawdzamy telefonicznie na znany numer.	☐	☐
7.2	Przelewy zatwierdzają dwie osoby lub druga osoba sprawdza je przed wysłaniem.	☐	☐
8.1	Mamy spisane zasady korzystania z AI (czego nie wklejamy, kto sprawdza).	☐	☐
8.2	Treści z pomocą AI człowiek sprawdza i poprawia przed publikacją.	☐	☐
9.1	Przy VR i nowym sprzęcie uczestnicy wiedzą, co jest pokazywane lub nagrywane; przy dzieciach jest zgoda rodzica.	☐	☐
9.2	Udział jest dobrowolny, sprzęt czyścimy między osobami.	☐	☐
10.1	Wszyscy wiedzą, kto koordynuje reakcję na incydent.	☐	☐
10.2	Mamy pod ręką kontakty: bank, CERT Polska (incydent.cert.pl, SMS 8080), osoby z dostępem.	☐	☐

Liczba odpowiedzi TAK: _____ / 20 (17–20 dobra podstawa · 11–16 solidny początek · 0–10 zacznij od kroków 2, 7, 5, 10)

Trzy zadania: 1.

2.

3.

Wynik służy do planowania i nie jest oceną zgodności z normami ISO ani z przepisami.

Rejestr kont, dostępów i urządzeń

UWAGA

Nie wpisujcie tu haseł. Rejestr mówi, co mamy i kto ma dostęp, a nie jak się zalogować. Przechowujcie go w miejscu z ograniczonym dostępem.

B1. Konta, strony i profile

Konto / usługa	Do czego	Login (adres)	Gdzie jest hasło	2FA – na czym urządzeniu	Administratorzy (min. 2)	Kto jeszcze ma dostęp	Przegląd
Strona na Facebooku	ogłoszenia	konto osobiste adminów	nie dotyczy	każdy admin swoje	A. Nowak, B. Kowalska	C. Wiśniewska (redaktor)	03.2027
Poczta organizacji	korespondencja	kontakt@...	menedżer haseł	telefon organizacji + kody w kopercie	A. Nowak, B. Kowalska	–	03.2027

B2. Urządzenia i nośniki

Urządzenie	Gdzie jest	Osoba odpowiedzialna	Blokada / szyfrowanie	Aktualizacje	Uwagi (np. z dotacji, nr ewidencyjny)
Laptop świetlicy	szafa zarządu	B. Kowalska	hasło, szyfrowanie dysku	automatyczne	konto „Gość” dla uczestników

B3. Kopie zapasowe i testy odtworzenia

Data	Co skopiowano	Gdzie (nośnik / miejsce)	Test odtworzenia: udany?	Kto

Polityka AI na jedną stronę

Zasady korzystania ze sztucznej inteligencji w _____

przyjęte dnia _____ · obowiązują wszystkie osoby działające w imieniu organizacji

- Po co korzystamy z AI.** AI pomaga nam w przygotowaniu szkiców tekstów, tłumaczeniach, streszczeniach i prostych grafikach. Nie zastępuje ludzi w kontaktach z mieszkańcami.
- Osoba odpowiedzialna za AI:** _____. Odpowiada na pytania, prowadzi listę narzędzi i aktualizuje te zasady.
- Narzędzia, z których korzystamy:** _____. Nowe narzędzie dodajemy po ocenie w 4 pytaniach (pkt 8).
- Czego nie wklejamy:** danych osobowych, danych o zdrowiu i dzieciach, hasła i danych bankowych, dokumentów poufnych, cudzego głosu i wizerunku bez zgody. Gdy trzeba – anonimizujemy.
- Sprawdzamy:** każdą treść z AI czyta i poprawia człowiek. Fakty, daty, kwoty, przepisy i linki sprawdzamy w źródle. Za opublikowaną treść odpowiada osoba, która ją opublikowała.
- Oznaczamy:** realistyczne obrazy, nagrania i głos wygenerowane przez AI podpisujemy „wygenerowano z pomocą AI”. Nie tworzymy realistycznych wizerunków prawdziwych osób bez ich zgody.
- Człowiek decyduje:** AI nie podejmuje decyzji o ludziach (przyjęcia, nagrody, oceny, wybór wolontariuszy).
- Ocena przed nowym użyciem – 4 pytania:** Jakie dane trafią do narzędzia? Kogo może dotknąć błąd? Kto i jak sprawdzi wynik? Czy odbiorcy powinni wiedzieć o użyciu AI?
- Deepfake i podszywanie się:** nietypowe prośby (o pieniądze, dane, dostęp) sprawdzamy drugim kanałem, nawet jeśli głos lub obraz wydaje się znajomy. Podejrzenia zgłaszamy koordynatorowi incydentu.
- Przegląd zasad:** co najmniej raz w roku oraz gdy zaczynamy używać AI do nowego rodzaju zadań.

podpis osoby odpowiedzialnej za AI

podpis za zarząd / sőtysa

Wzór można dowolnie skracać i dopasowywać do organizacji.

Przekazanie kont przy zmianie zarządu lub sołtysa

Przed zmianą (najlepiej 2–4 tygodnie wcześniej)

- ☐ Zaktualizować rejestr kont, dostępów i urządzeń (Załącznik B).
- ☐ Sprawdzić, na czyje dane (e-mail, telefon) zarejestrowane są konta, domena i usługi; przenieść je na dane organizacji.
- ☐ Przygotować dokumenty do banku dotyczące zmiany osób uprawnionych (zgodnie z wymaganiami banku).
- ☐ Uporządkować pliki: wszystko, co organizacyjne, przenieść z prywatnych dysków i telefonów do folderu organizacji.

W dniu przekazania

- ☐ Dodać nowe osoby jako administratorów (profil, poczta, dysk, menedżer haseł) **zanim** usunie się dotychczasowe.
- ☐ Przekazać sprzęt, nośniki, klucze, kopertę awaryjną – zgodnie z rejestrem.
- ☐ Zmienić hasła do kont wspólnych i dane do odzyskiwania (telefon, e-mail zapasowy), wygenerować nowe kody zapasowe.
- ☐ Wylogować wszystkie sesje i usunąć zaufane urządzenia osób odchodzących.
- ☐ Podpisać protokół przekazania (poniżej).

Do 30 dni po zmianie

- ☐ Usunąć dostęp osób odchodzących (o ile nie pozostają w nowej roli) i usunąć je z grup administracyjnych.
- ☐ Potwierdzić w banku nową listę osób uprawnionych; sprawdzić ustawienia podwójnej autoryzacji.
- ☐ Sprawdzić, czy na prywatnych urządzeniach osób odchodzących nie zostały pliki organizacji.
- ☐ Zrobić krótki samoaudyt (Załącznik A) w nowym składzie.

Protokół przekazania kont i urządzeń

W dniu _____ w _____

osoba przekazująca: _____ osoba przejmująca: _____

przekazano dostęp do kont i urządzeń wymienionych w rejestrze z dnia _____ (bez wpisywania haseł do protokołu). Hasła do kont wspólnych zostały zmienione: ☐ tak ☐ nie (dlaczego?) _____

Uwagi / braki:

podpis osoby przekazującej

podpis osoby przejmującej

Karta incydentu

Data i godzina zauważenia: _____ Kto zauważył: _____

Co się stało (fakty, bez ocen):

Rodzaj: ☐ przejęte konto/profil ☐ przelew/oszustwo ☐ zgubione/skradzione urządzenie ☐ złośliwe oprogramowanie ☐ wyciek lub błędne wystanie danych ☐ podszywanie się / deepfake ☐ inne: _____

Czego dotyczy (konta, urządzenia, dane, kwota):

Czy dotyczy danych osobowych? ☐ tak ☐ nie ☐ nie wiem → jeśli tak: sprawdzono obowiązek zgłoszenia do UODO (72 h) dnia _____

Podjęte działania

Godzina	Działanie (np. telefon do banku, zmiana hasła, zgłoszenie do CERT)	Kto

Zgłoszenia: ☐ bank ☐ CERT Polska (nr zgłoszenia: _____) ☐ policja ☐ platforma ☐ UODO ☐ operator dotacji ☐ poinformowano osoby, których dotyczy

Dowody zachowane (zrzuty ekranu, e-maile, gdzie zapisane):

Wnioski: co zmieniamy, żeby się nie powtórzyło:

Zamknięto dnia: _____ Podpis koordynatora: _____

Przydatne adresy i o projekcie

Gdzie szukać pomocy i wiedzy

- **CERT Polska** – zgłaszanie incydentów: incydent.cert.pl; podejrzane SMS-y: bezpłatnie przekaż na numer **8080**; ostrzeżenia i porady: cert.pl.
- **Urząd Ochrony Danych Osobowych** – poradniki i informacje o zgłaszaniu naruszeń: uodo.gov.pl.
- **Wykaz podatników VAT („biała lista”)** – sprawdzanie rachunku kontrahenta: podatki.gov.pl.
- **Pomoc przy przejętym koncie na Facebooku**: facebook.com/hacked.
- **Sprawdzanie wycieków adresu e-mail**: haveibeenpwned.com.
- **Normy**: ISO/IEC 27001:2022 i ISO/IEC 42001:2023 – opisy na iso.org; zakup norm m.in. w Polskim Komitecie Normalizacyjnym (pkn.pl).

O poradniku

Poradnik „Cyber-higiena dla małych organizacji i instytucji lokalnych” powstał w projekcie „**Audyt i edukacja cyfrowa dla powiatu**”, realizowanym przez **Fundację ISTS – Instytut Strategii, Technologii i Bezpieczeństwa** dla mieszkańców i organizacji powiatu zduńskowolskiego, w ramach konkursu „**Łódzkie Lokalnie NOWE FIO 2024-26**” (operator: KIPR, umowa nr 25/31.08.2026).

Opracowanie: Fundacja ISTS. Autor: audytor wewnętrzny ISO/IEC 27001 i ISO/IEC 42001.

Wydanie 1, październik 2026. Poradnik jest bezpłatny i dostępny online: aiists.netlify.app/poradnik. Będzie aktualizowany przy kolejnych edycjach.

Licencja: Creative Commons Uznanie autorstwa 4.0 (CC BY 4.0) – można kopiować, drukować i dostosowywać z podaniem źródła.



PORADNIK ONLINE

<https://aiists.netlify.app/poradnik/>

Zeskanuj kod telefonem, aby otworzyć najnowszą wersję poradnika. Wersję PDF pobierzesz z tej samej strony.

ZASTRZEŻENIE

Poradnik jest inspirowany normami ISO/IEC 27001:2022 i ISO/IEC 42001:2023, ale nie jest ich częścią ani streszczeniem, nie cytuje ich treści, nie prowadzi do certyfikacji i nie potwierdza zgodności z nimi. Nie stanowi porady prawnej. Informacje sprawdzono według stanu na październik 2026 r.