Środki techniczne i organizacyjne stosowane w PHU ELKA Radosław Miczyński

1. Wprowadzenie.

Niniejszy dokument stanowi kompleksowy opis środków technicznych, organizacyjnych i fizycznych wdrożonych w PHU ELKA w celu zapewnienia ochrony danych osobowych, bezpieczeństwa informacji oraz zgodności z RODO, ustawą o świadczeniu usług drogą elektroniczną, ustawą o krajowym systemie cyberbezpieczeństwa, a także normami ISO 27001 i ISO 9001.

Dokument jest częścią Systemu Zarządzania Bezpieczeństwem Informacji i jest powiązany z:

- Księgą Systemu Zarządzania Jakością ISO 9001
- Księgą Zarządzania Bezpieczeństwem Informacji ISO 27001
- Polityką Bezpieczeństwa Informacji,
- Polityką Zabezpieczeń IT,
- Polityką Zarządzania Ryzykiem,
- Matrycą Aktywów Informacyjnych,
- Matrycą Zagrożeń i Zabezpieczeń,
- Procedurą zarządzania incydentami,
- Procedurą ciągłości działania (BCP),
- Instrukcjami dotyczącymi haseł, kopii zapasowych, zarządzania dostępami, urządzeniami mobilnymi,

PHU ELKA wdrożyła i utrzymuje zintegrowany system zarządzania bezpieczeństwem informacji zgodny z ISO 27001 oraz system zarządzania jakością wg ISO 9001.

Wprowadzane środki są adekwatne do:

- charakteru i zakresu przetwarzania danych,
- ryzyka naruszenia praw osób fizycznych,
- technologii stosowanej w organizacji,
- wyników analiz ryzyka (ryzyko SZBI + ryzyko RODO).

Środki są regularnie przeglądane, testowane, aktualizowane i rozwijane w oparciu o cykl PDCA.

Dokument stanowi realizację obowiązków z art. 24, 25 i 32 RODO, a także A.5–A.18 normy ISO 27001.

2. Klasyfikacja informacji

W organizacji stosuje się klasyfikację informacji:

- publiczne
- ograniczone
- poufne

Dla każdej klasy informacji określone są:

- poziomy zabezpieczeń,
- wymagania dostępu,
- sposób przechowywania i niszczenia.

3. Środki organizacyjne

Struktura odpowiedzialności i nadzoru

W PHU ELKA wyznaczono formalnie:

- Administratora Systemów Informatycznych (ASI),
- Inspektora Ochrony Danych (IOD),
- właścicieli aktywów informacji,
- właścicieli procesów odpowiedzialnych za zgodność z SZJ i SZBI.

Każdy pracownik posiada:

- zakres obowiązków,
- upoważnienie do przetwarzania danych,
- oświadczenie o zachowaniu poufności,
- dostęp nadawany zgodnie z zasadą minimalnych uprawnień (least privilege).

Stosowane jest rozdzielenie ról i odpowiedzialności (SoD).

ul. Kosowa 3A
66-008 Wilkanowo

tel. 68 324 77 80
tel. 68 414 60 00

kontakt@grupa-elka.pl
www.grupa-elka.pl

Dokumentacja i polityki

W organizacji obowiązują:

- Księga Systemu Zarządzania Jakością ISO 9001
- Księga Zarządzania Bezpieczeństwem Informacji ISO 27001
- Polityka Bezpieczeństwa Informacji
- Polityka Zabezpieczeń IT
- Polityka Haseł
- Polityka Dostępu
- Polityka Zarządzania Ryzykiem
- Polityka Backupów
- Polityka Retencji i Niszczenia Danych
- Instrukcja Zarządzania Incydentami
- Instrukcja Funkcjonowania Systemów IT
- Procedury szkoleniowe i audytowe

Zasady dostępu i upoważnienia

Dostępy nadawane są zgodnie z zasadami: niezbędnej wiedzy, minimalnych uprawnień oparte o model bezpieczeństwa „Zero Trust".

Dostępy są przeglądane cyklicznie:

- po zmianie stanowiska,
- po zakończeniu współpracy,
- co najmniej raz na 12 miesięcy.

Upoważnienia pracowników są rejestrowane, ewidencjonowane i archiwizowane.

Klauzule poufności

Wszyscy pracownicy i współpracownicy podpisują:

- klauzulę poufności,
- klauzulę zachowania tajemnicy przedsiębiorstwa,
- upoważnienie RODO.

3. Środki techniczne

Kontrola dostępu – systemy i aplikacje

Logowanie do serwisów SaaS wymaga unikalnych identyfikatorów użytkowników.

Wymuszane są polityki haseł zgodne z normami:

- złożoność,
- cykliczna zmiana,

Dostępy do serwisów SaaS, baz danych, paneli administracyjnych są logowane i audytowane.

Zarządzanie uprawnieniami oparte jest na rolach.

Stosowane są automatyczne blokady kont, time-out i limity prób logowania.

Kontrola dostępu fizycznego

Dostęp do pomieszczeń jest zabezpieczony:

- kartami dostępowymi,
- atestowanymi zamkami,
- dozorem firmy ochroniarskiej 24/7,
- systemem monitoringu CCTV.

Dostęp do serwerowni jest ograniczony tylko do upoważnionego personelu technicznego.

Szyfrowanie i poufność transmisji

Wszelkie połączenia z systemami produkcyjnymi są szyfrowane (TLS 1.2/1.3).

Zdalny dostęp odbywa się wyłącznie poprzez VPN z kryptograficznym zabezpieczeniem tunelu.

Dostęp administracyjny jest dodatkowo zabezpieczony (SSH, VPN, kontrola IP, logowanie zdarzeń).

Stosowane jest szyfrowanie danych na dyskach, jeśli wymaga tego poziom ryzyka.

Bezpieczeństwo sieci

Stosowane są:

- zapory sieciowe (firewall),
- reguły ograniczające porty i protokoły,
- segmentacja sieci,

ul. Kosowa 3A
66-008 Wilkanowo

tel. 68 324 77 80
tel. 68 414 60 00

kontakt@grupa-elka.pl
www.grupa-elka.pl

- IDS/IPS wykrywające anomalie i sygnatury zagrożeń.

Połączenia wewnętrzne i zewnętrzne są monitorowane pod kątem nieautoryzowanych aktywności.

Ochrona usług i serwerów

Serwery są chronione przez:

- firewall systemowy,
- monitorowanie aktywności,
- aktualizacje i łatki bezpieczeństwa,
- mechanizmy RAID zabezpieczające przed awarią dysków,
- kontrolę integralności.

Wszystkie systemy produkcyjne są utrzymywane na serwerach spełniających co najmniej równoważne standardy bezpieczeństwa.

Kopie zapasowe (backupy) i ciągłość działania

Backupy wykonywane są zgodnie z Polityką Kopii Zapasowych:

- backupy dzienne,
- testy odtwarzania,
- szyfrowanie lub izolacja backupów,
- przechowywanie in-site i/lub off-site.

Opracowano i wdrożono Plan Ciągłości Działania (BCP).

Odzyskiwanie po awarii (DRP) testowane jest cyklicznie.

4. Środki fizyczne

Obiekty firmy PHU ELKA są chronione przez firmę ochroniarską 24/7.

Teren i budynki są objęte monitoringiem wizyjnym.

Serwerownie i pomieszczenia techniczne są zabezpieczone przed dostępem osób nieuprawnionych.

Dokumenty papierowe z klauzulą poufności przechowywane są w:

- metalowych szafach,
- pomieszczeniach z kontrolą dostępu.

5. Środki proceduralne i operacyjne

Zarządzanie incydentami

Obowiązuje formalna Procedura Zarządzania Incydentami (ISO + RODO).

Każdy incydent jest:

- rejestrowany,
- klasyfikowany,
- analizowany,
- raportowany (w tym zgłaszany do IOD).

Pracownicy zostali przeszkoleni i mają obowiązek niezwłocznego zgłaszania wszelkich incydentów bezpieczeństwa.

Szkolenia

Pracownicy przechodzą:

- szkolenie wstępne z RODO,
- szkolenie okresowe,
- szkolenia z bezpieczeństwa informacji, phishingu, cyberzagrożeń,
- szkolenia stanowiskowe wynikające z Polityk SZBI.

Szkolenia są dokumentowane i podlegają audytowi.

Audyty i przeglądy

Firma PHU ELKA prowadzi:

- audyty wewnętrzne ISO 27001 i ISO 9001,
- audyty systemów IT,
- przeglądy dostawców,
- testy bezpieczeństwa (techniczne i organizacyjne).

Wyniki audytów są analizowane i stanowią podstawę działań doskonalących.

6. Środki stosowane u podmiotów zewnętrznych

ul. Kosowa 3A
66-008 Wilkanowo
tel. 68 324 77 80
tel. 68 414 60 00
kontakt@grupa-elka.pl
www.grupa-elka.pl

Dostawcy usług IT (hosting, chmura, SaaS, serwis) muszą zapewniać poziom bezpieczeństwa równoważny lub wyższy.
Wszelkie przetwarzanie danych przez podmioty trzecie odbywa się na podstawie:
- umowy powierzenia,
- oceny ryzyka dostawcy,
- przeglądu środków bezpieczeństwa kontrahenta,
- regularnych audytów/monitorowania.

7. Środki dotyczące urządzeń i danych mobilnych
Zabronione jest przetwarzanie danych osobowych na urządzeniach prywatnych bez zgody ASI.
Nośniki danych muszą być szyfrowane lub zabezpieczone mechanicznie.

8. Środki dotyczące retencji i niszczenia danych
Dane przechowywane są zgodnie z:
- Polityką Retencji,
- przepisami rachunkowości i podatkowymi,
- umowami z klientami.

Dane są niszczone:
- bezpiecznymi metodami,
- poprzez demagnetyzację, niszczenie fizyczne, kasowanie kryptograficzne,
- zgodnie z protokołem niszczenia.

9. Ocena skutków i privacy-by-design
Wszelkie nowe systemy, wdrożenia i aplikacje podlegają zasadom: Data Protection Impact Assessment + Security by Design + Privacy by Design + Privacy by Default.
Każda nowa usługa SaaS jest analizowana pod kątem:
- ryzyka RODO,
- ryzyka SZBI,
- matrycy zagrożeń,
- zgodności z ISO 27001 A.5–A.18.

10. Postanowienia końcowe
PHU ELKA zastrzega prawo do aktualizowania niniejszego dokumentu zgodnie z:
- aktualizacjami prawa,
- zmianami technologii,
- wynikami audytów i incydentów.

Niniejszy dokument stanowi część zintegrowanego systemu zarządzania i jest elementem umów powierzenia danych.
Niniejszy dokument posiada oznaczenie wersji oraz datę obowiązywania i podlega zatwierdzeniu przez:
- Właściciela PHU ELKA,
- Inspektora Ochrony Danych Osobowych PHU ELKA
- Administratora Systemów Informatycznych PHU ELKA

Data publikacji: 01.04.2026
Zatwierdził: Paweł Walczak
Zatwierdził: Sebastian Nowak
Zatwierdził: Radosław Miczyński

ul. Kosowa 3A
66-008 Wilkanowo
tel. 68 324 77 80
tel. 68 414 60 00
kontakt@grupa-elka.pl
www.grupa-elka.pl