INSTRUKCJA ZARZĄDZANIA DOSTĘPAMI I SYSTEMAMI INFORMATYCZNYMI

§ 1. Cel i zakres instrukcji

1. Instrukcja określa zasady bezpiecznego korzystania z systemów informatycznych oraz nadawania, zmiany, przeglądu i odbierania dostępów do danych osobowych w placówce.
2. Instrukcja obejmuje w szczególności system EDM, system rejestracji, pocztę elektroniczną, systemy księgowe i kadrowe, komputery, laptopy, urządzenia mobilne, sieć lokalną, usługi chmurowe, nośniki danych, kopie zapasowe oraz inne systemy wykorzystywane w placówce.
3. Zasady stosuje się do pracowników, osób wykonujących zawody medyczne, zleceniobiorców, współpracowników, administratorów IT, serwisantów i innych osób posiadających dostęp do systemów lub danych.

§ 2. Zasady nadawania dostępu

1. Dostęp nadaje się wyłącznie osobie, która posiada odpowiednią podstawę do wykonywania czynności na danych i której dostęp jest niezbędny do realizacji obowiązków.
2. Zakres dostępu odpowiada stanowisku, roli i zasadzie minimalnych uprawnień. Lekarz, pielęgniarka, rejestracja, administracja, księgowość i personel IT otrzymują zakresy adekwatne do swoich zadań.
3. Każdy użytkownik otrzymuje indywidualny identyfikator. Konta współdzielone są niedopuszczalne, chyba że wyjątkowo wymagają tego rozwiązania techniczne, a ryzyko zostało ocenione i zastosowano mechanizmy rozliczalności.
4. Nadanie dostępu jest dokumentowane w ewidencji upoważnień/uprawnień. Należy odnotować użytkownika, system, rolę lub zakres, datę nadania oraz osobę zatwierdzającą.
5. Uprawnienia administracyjne nadaje się wyłącznie osobom, które rzeczywiście ich potrzebują.

§ 3. Zmiana, przegląd i odebranie uprawnień

1. Uprawnienia zmienia się niezwłocznie po zmianie stanowiska, obowiązków lub zakresu współpracy.
2. Po ustaniu zatrudnienia lub współpracy dostęp do systemów, poczty, VPN, usług chmurowych i innych zasobów należy odebrać bez zbędnej zwłoki, nie później niż w dniu ustania potrzeby dostępu.

3. Placówka przeprowadza okresowy przegląd aktywnych kont i uprawnień, rekomendowane co najmniej raz na 6–12 miesięcy oraz po istotnych zmianach organizacyjnych.
4. Konta nieużywane, zbędne lub pozostawione po byłych współpracownikach są blokowane lub usuwane zgodnie z zasadami retencji i wymaganiami systemu.

§ 4. Hasła i uwierzytelnianie

1. Hasła muszą być unikalne, odpowiednio długie i trudne do odgadnięcia. Zabrania się ujawniania haseł innym osobom oraz przesyłania ich w sposób niezabezpieczony.
2. Tam, gdzie jest to technicznie możliwe i adekwatne do ryzyka, stosuje się uwierzytelnianie wieloskładnikowe, w szczególności dla dostępu zdalnego, kont administracyjnych, poczty i usług chmurowych.
3. Hasło należy niezwłocznie zmienić w razie podejrzenia ujawnienia lub przejęcia konta.
4. Nie zapisuje się haseł w widocznych miejscach. Dopuszcza się zatwierdzony przez Administratora menedżer haseł.

§ 5. Stanowiska komputerowe i urządzenia

1. Komputery i urządzenia służbowe zabezpiecza się przed dostępem osób nieuprawnionych. Ekran blokuje się przy każdorazowym odejściu od stanowiska.
2. Ustawia się automatyczną blokadę ekranu po okresie bezczynności adekwatnym do warunków pracy.
3. Instalowanie oprogramowania bez zgody osoby odpowiedzialnej za IT jest zabronione.
4. Urządzenia mobilne zawierające dane placówki powinny być zabezpieczone kodem/hasłem, a tam gdzie jest to zasadne – szyfrowaniem i możliwością zdalnego zablokowania lub usunięcia danych.
5. Dokumentacji medycznej i danych pacjentów nie przechowuje się lokalnie na prywatnych urządzeniach, chyba że Administrator dopuścił takie rozwiązanie po ocenie ryzyka i wdrożeniu zabezpieczeń.

§ 6. Poczta elektroniczna i komunikacja

1. Przed wysłaniem wiadomości zawierającej dane osobowe należy zweryfikować adresata, zakres załączników i konieczność przekazania danych.
2. Dane dotyczące zdrowia i dokumentacja medyczna są przesyłane wyłącznie z wykorzystaniem sposobów zapewniających bezpieczeństwo adekwatne do ryzyka.

3. Zabrania się automatycznego przekierowywania poczty służbowej na prywatne skrzynki.
4. Podejrzanych linków i załączników nie należy otwierać; próby phishingu zgłasza się osobie odpowiedzialnej za IT lub Administratorowi.

§ 7. EDM i systemy medyczne

1. Dostęp do EDM jest oparty na rolach i zakresie obowiązków. Użytkownik korzysta wyłącznie z danych niezbędnych do realizacji powierzonych zadań.
2. System powinien rejestrować, w zakresie dostępnych funkcjonalności, logowania i istotne operacje użytkowników. Logi zabezpiecza się przed nieuprawnioną zmianą i przechowuje przez okres ustalony na podstawie ryzyka oraz wymagań prawnych.
3. Niedopuszczalne jest przeglądanie dokumentacji pacjenta z ciekawości lub bez związku z wykonywanymi obowiązkami.
4. Eksportowanie danych z EDM na lokalny komputer lub nośnik ogranicza się do przypadków uzasadnionych i odpowiednio zabezpieczonych.

§ 8. Dostęp zdalny

1. Dostęp zdalny do systemów zawierających dane pacjentów dopuszcza się wyłącznie za zgodą Administratora i z wykorzystaniem zatwierdzonych, bezpiecznych rozwiązań.
2. Dostęp zdalny powinien wykorzystywać szyfrowane połączenie oraz – tam, gdzie jest to możliwe – uwierzytelnianie wieloskładnikowe.
3. Nie korzysta się z niezaufanych, publicznych komputerów do dostępu do systemów placówki.
4. Serwisowy dostęp zdalny podmiotu zewnętrznego powinien być ograniczony czasowo i zakresowo, rejestrowany, a gdy to możliwe aktywowany wyłącznie na czas wykonywania prac.

§ 9. Serwis IT i podmioty zewnętrzne

1. Dostawcy IT mają dostęp do danych tylko w zakresie niezbędnym do wykonania usługi i na podstawie właściwej umowy, w tym umowy powierzenia, gdy występuje przetwarzanie w imieniu Administratora.
2. Przed rozpoczęciem współpracy ocenia się gwarancje bezpieczeństwa dostawcy.
3. Serwisant nie powinien kopiować danych na własne urządzenia, chyba że jest to niezbędne, uzgodnione i odpowiednio zabezpieczone.
4. Po zakończeniu prac tymczasowe konta i dostępy serwisowe są wyłączane, jeśli nie są już potrzebne.

§ 10. Aktualizacje i ochrona przed złośliwym oprogramowaniem

1. Systemy operacyjne, aplikacje, przeglądarki, urządzenia sieciowe i oprogramowanie medyczne są aktualizowane w sposób kontrolowany, z uwzględnieniem krytyczności poprawek i zgodności z systemami medycznymi.
2. Stosuje się odpowiednią ochronę przed złośliwym oprogramowaniem oraz zaporę sieciową.
3. Oprogramowanie niewspierane przez producenta podlega ocenie ryzyka i powinno zostać zaktualizowane, odizolowane lub zastąpione.
4. Placówka okresowo ocenia podatności i skuteczność zabezpieczeń.

§ 11. Kopie zapasowe i odtwarzanie

1. Dla systemów i danych wymagających zapewnienia dostępności wykonuje się regularne kopie zapasowe według ustalonego harmonogramu.
2. Co najmniej jedna kopia powinna być logicznie lub fizycznie odseparowana od środowiska produkcyjnego w sposób ograniczający skutki awarii lub ransomware.
3. Dostęp do kopii zapasowych jest ograniczony. Kopie zawierające dane osobowe podlegają takim samym zasadom ochrony jak dane źródłowe.
4. Możliwość odtworzenia danych z kopii zapasowych jest okresowo testowana, a wyniki testów dokumentowane.

§ 12. Nośniki i wydruki

1. Korzystanie z przenośnych nośników danych ogranicza się do niezbędnego minimum. Preferuje się nośniki zatwierdzone i szyfrowane.
2. Nośniki zawierające dane osobowe ewidencjonuje się lub kontroluje adekwatnie do ryzyka.
3. Przed ponownym użyciem, przekazaniem lub utylizacją nośnika dane usuwa się w sposób uniemożliwiający ich odtworzenie.
4. Wydruki zawierające dane pacjentów należy niezwłocznie odbierać z drukarki i przechowywać poza dostępem osób nieuprawnionych.

§ 13. Bezpieczeństwo sieci i pomieszczeń

1. Sieć wykorzystywana do przetwarzania danych jest zabezpieczona przed nieuprawnionym dostępem. Dostęp gościnny, jeżeli jest oferowany, powinien być odseparowany od sieci systemów medycznych.
2. Urządzenia sieciowe mają zmienione domyślne dane uwierzytelniające i są konfigurowane przez osoby uprawnione.
3. Pomieszczenia i szafy, w których znajdują się serwery, urządzenia sieciowe lub dokumentacja, są zabezpieczone przed dostępem osób nieuprawnionych.

4. Osoby zewnętrzne przebywające w obszarach przetwarzania danych podlegają zasadom nadzoru adekwatnym do ryzyka.

§ 14. Incydenty bezpieczeństwa

1. Użytkownik niezwłocznie zgłasza: utratę sprzętu, podejrzenie przejęcia konta, ujawnienie hasła, wysłanie danych do niewłaściwego odbiorcy, infekcję, ransomware, utratę dokumentacji, nieuprawniony dostęp lub inne nietypowe zdarzenie.
2. Po zgłoszeniu zabezpiecza się dowody i ogranicza skutki incydentu zgodnie z procedurą naruszeń ochrony danych.
3. Użytkownik nie usuwa samodzielnie logów ani śladów incydentu, jeśli mogłoby to utrudnić analizę.

§ 15. Kontrola, testy i szkolenia

1. Placówka regularnie testuje, mierzy i ocenia skuteczność stosowanych środków technicznych i organizacyjnych odpowiednio do ryzyka.
2. Wyniki przeglądów, testów kopii zapasowych, przeglądów uprawnień oraz istotnych działań naprawczych są dokumentowane.
3. Personel przechodzi szkolenia z ochrony danych i bezpieczeństwa informacji przed uzyskaniem dostępu oraz okresowo w trakcie współpracy.
4. Instrukcja jest przeglądana po istotnych zmianach systemów, po incydencie, zmianie ryzyka lub przepisów oraz okresowo.

§ 16. Postanowienia końcowe

1. Naruszenie zasad Instrukcji może skutkować odebraniem dostępu i konsekwencjami wynikającymi z przepisów, umowy lub regulacji wewnętrznych.
2. W sprawach nieuregulowanych stosuje się Politykę ochrony danych osobowych placówki, procedurę naruszeń, zasady retencji oraz inne dokumenty bezpieczeństwa.
3. Instrukcja wchodzi w życie z dniem 31 sierpnia 2026 r.

_____

Za Administratora – Prezes Zarządu

ZAŁĄCZNIK 1 – KARTA NADANIA / ZMIANY / ODEBRANIA DOSTĘPU

Imię i nazwisko użytkownika	
Stanowisko / rola	
System / zasób	
Zakres / rola w systemie	
Rodzaj operacji	
Data nadania / zmiany / odebrania	
Dostęp zdalny (tak/nie)	
MFA (tak/nie/nie dotyczy)	
Zatwierdził	
Uwagi	