ZARZĄDZENIE NR 28/2023

Dyrektora Narodowego Instytutu Onkologii im. Marii Skłodowskiej-Curie –
Państwowego Instytutu Badawczego
z dnia 25 maja 2023 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Systemu KRN w Narodowym Instytucie Onkologii im. Marii Skłodowskiej-Curie – Państwowym Instytucie Badawczym w Warszawie

Na podstawie § 7 Statutu Narodowego Instytutu Onkologii im. Marii Skłodowskiej-Curie – Państwowego Instytutu Badawczego, zarządza się, co następuje:

§ 1.

Wprowadza się do stosowania „Politykę Bezpieczeństwa Systemu KRN" w Narodowym Instytucie Onkologii im. Marii Skłodowskiej-Curie – Państwowym Instytucie Badawczym w Warszawie", stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem wydania.

DYREKTOR
Narodowego Instytutu Onkologii
im. Marii Skłodowskiej-Curie
- Państwowego Instytutu Badawczego
Prof. dr hab. n. med. Jan Walewski

Załącznik do Zarządzenia Nr 28/2023
Dyrektora Narodowego Instytutu Onkologii
im. Marii Skłodowskiej-Curie –
Państwowego Instytutu Badawczego
z dnia 25 maja 2023 roku

Polityka Bezpieczeństwa Systemu KRN

§ 1.

Wstęp

1. Niniejszy dokument stanowi Politykę Bezpieczeństwa Systemu KRN zaprojekowanego i wdrożonego w ramach projektu „Budowa nowoczesnej platformy gromadzenia i analizy danych z Krajowego Rejestru Nowotworów oraz onkologicznych rejestrów narządowych, zintegrowanej z bazami świadczeniodawców leczących choroby onkologiczne (e-KRN+)" realizowanego w ramach Programu Operacyjnego Polska Cyfrowa, oś priorytetowa II E-administracja i otwarty rząd, Działanie 2.2 Cyfryzacja procesów back-office w administracji rządowej.
2. Polityka Bezpieczeństwa Systemu KRN zawiera zasady i wymagania bezpieczeństwa przeznaczone do realizacji w ramach eksploatacji Systemu KRN, jak również główne obowiązki pracowników NIO-PIB związane z zapewnieniem poufności, dostępności i integralności danych w tym systemie.
3. Polityka Bezpieczeństwa Systemu KRN jest zgodna z przepisami prawa powszechnie obowiązującymi oraz zarządzeniami Dyrektora NIO-PIB.
4. Polityka Bezpieczeństwa Systemu KRN jest dokumentem nadrzędnym dla dedykowanych regulaminów, procedur i instrukcji zarządzania Systemem KRN oraz odwołuje się do procedur i regulaminów opracowanych przez Dział Systemów ICT i Cyberbezpieczeństwa NIO-PIB w ramach Zintegrowanego Systemu Zarządzania w NIO-PIB.

§ 2.

Słownik

Skróty i definicje terminów używanych w dalszej części dokumentu.

Termin/skrót	Definicja/znaczenie
NIO-PIB	Narodowy Instytut Onkologii im. Marii Skłodowskiej-Curie – Państwowy Instytut Badawczy (wcześniej Centrum Onkologii – Instytut im. Marii Skłodowskiej-Curie) – podmiot prowadzący Krajowy Rejestr Nowotworów
Administrator (Danych Osobowych)	Narodowy Instytut Onkologii im. Marii Skłodowskiej-Curie – Państwowy Instytut Badawczy, reprezentowany przez Dyrektora
Dyrektor	Dyrektor Narodowego Instytutu Onkologii im. Marii Skłodowskiej-Curie – Państwowego Instytutu Badawczego
Administrator Systemów Informatycznych ASI	zespół odpowiedzialny za administrację systemami informatycznymi Dział Systemów ICT i Cyberbezpieczeństwa w NIO-PIB
Administrator (administratorzy) Systemu KRN AS	pracownik lub pracownicy KRN dedykowani do administracji infrastrukturą ITS KRN

KRN	Krajowy Rejestr Nowotworów – jednostka organizacyjna NIO-PIB podlegająca bezpośrednio Dyrektorowi
WRN	Wojewódzki Rejestr Nowotworów
System KRN	system informatyczny zaprojekowany i wdrożony w ramach projektu „Budowa nowoczesnej platformy gromadzenia i analizy danych z Krajowego Rejestru Nowotworów oraz onkologicznych rejestrów narządowych, zintegrowanej z bazami świadczeniodawców leczących choroby onkologiczne (e-KRN+)"
ZPRO	Zintegrowana Platforma Rejestrów Onkologicznych – infrastruktura techniczno-systemowa zbudowana w ramach projektu „Budowa nowoczesnej platformy gromadzenia i analizy danych z Krajowego Rejestru Nowotworów oraz onkologicznych rejestrów narządowych, zintegrowanej z bazami świadczeniodawców leczących choroby onkologiczne (e-KRN+)"
WS	Wykonawca Systemu KRN
Administrator KRN AKRN	pracownik KRN odpowiedzialny za administrację aplikacjami KRN, m.in. nadający uprawnienia użytkownikom KRN
Dane osobowe	informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
DLP / system DLP	system przeciwdziałania wyciekom danych
Incydent bezpieczeństwa: - incydent związany z bezpieczeństwem informacji	pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Szczególnym przypadkiem incydentu jest naruszenie danych osobowych
- incydent związany z bezpieczeństwem danych osobowych	incydent związany z bezpieczeństwem informacji obejmujący naruszenie ochrony danych osobowych
- incydent w podmiocie publicznym	incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez NIO-PIB
- incydent krytyczny	incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV
Infrastruktura techniczno-systemowa	urządzenia, systemy operacyjne, bazodanowe, systemu bezpieczeństwa i narzędziowe KRN oraz serwery aplikacyjne i platformy uruchomieniowe działające na

	platformie ZPRO (czyli System KRN bez warstwy aplikacji)
IOD	Inspektor Ochrony Danych powołany przez Dyrektora
(Jednostkowe) dane medyczne	dane osoby fizycznej o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej oraz dotyczące jej stanu zdrowia, w tym profilaktyki zdrowotnej i realizacji programów zdrowotnych
Osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa	osoba wyznaczona przez NIO-PIB, do utrzymywania kontaktów z innymi podmiotami krajowego systemu cyberbezpieczeństwa, w tym w szczególności z właściwym CSIRT poziomu krajowego
PDZR	podsystem dostępu i zarządzania rejestrami obejmujący węzeł dostępowy
Opiekun Merytoryczny Systemu KRN (OM)	Kierownik KRN podejmujący bieżące decyzje w zakresie zarządzania systemem KRN w tym nadawania uprawnień użytkownikom, delegujący swoje uprawnienia innym pracownikom NIO-PIB (np. w zakresie nadawania uprawnień)
Zmiana standardowa	zmiana o niskim ryzyku i wpływie na działania Systemu (np. reset hasła użytkownika), które mogą być wykonywane cyklicznie, są dobrze opisane i zdefiniowane i nie wymagają szczegółowych analiz dotyczących wpływu na działanie Systemu KRN
Zmiana normalna	zmiana planowana realizowana zgodnie z uzgodnionym cyklem z którą może być związane ryzyko (np. instalacja poprawki lub nowej wersji aplikacji)
Zmiana awaryjna	zmiana, której wprowadzenia nie można było przewidzieć i zaplanować zgodnie z założeniami zmiany normalnej lub standardowej, a konsekwencją jej nie wprowadzenia w określonych ramach czasowych jest spadek parametrów Systemu

§ 3.

Zgodność podstawy prawne, normalizacyjne i regulacje wewnętrzne

1. Niniejsza Polityka jest zgodna z wewnętrznymi regulacjami NIO-PIB oraz następującymi aktami prawnymi:
   1) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t. j. Dz. U. z 2017 r. poz. 2247);
   2) ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2023 r. poz. 913);
   3) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – (Dz.U.UE.L.2016.119.1) (RODO);

4) rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (t. j. Dz. U. z 2022 r. poz. 1304);
5) rozporządzenie Ministra Zdrowia z dnia 14 czerwca 2018 r. w sprawie Krajowego Rejestru Nowotworów (Dz. U. z 2018 r. poz. 1197);
6) ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. z 2022 r. poz. 2509).

2. W Polityce wykorzystano wymagania i zalecenia następujących Polskich Norm:
1) PN-EN ISO/IEC 27001:2017-06 PN-EN ISO/IEC 27001:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania;
2) PN-EN ISO/IEC 27002:2017-06 PN-EN ISO/IEC 27002:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji.

§ 4.

Podstawowe zasady bezpieczeństwa

Podstawowymi zasadami bezpieczeństwa przyjętymi w NIO-PIB i obowiązującymi w KRN są:
1) zasada wiedzy uzasadnionej i minimalnych uprawień;
2) zasada wielopoziomowych zabezpieczeń;
3) zasada domyślnego braku dostępu;
4) zasada gromadzenia istotnych danych na serwerach i macierzach dyskowych;
5) zasada stosowania haseł odpornych na złamanie;
6) zasada co najmniej podstawowego zabezpieczenia stacji roboczych;
7) zasada monitoringu bezpieczeństwa infrastruktury informatycznej;
8) zasada ciągłego podnoszenia świadomości zagrożeń oraz sposobów zapobiegania im,
9) zasada zaawansowanych zabezpieczeń serwerów i macierzy dyskowych oraz regularnych kopii zapasowych;
10) zasada blokowania dostępu do Systemu po wygaśnięciu umów o zatrudnieniu/współpracy.

§ 5.

Role i odpowiedzialność za bezpieczeństwo

Zakresy obowiązków osób funkcyjnych w zakresie bezpieczeństwa Systemu KRN są następujące:
1) Dyrektor:
   a) powołuje zespół do opracowania oceny skutków naruszenia ochrony danych i zleca IOD jej konsultowanie oraz ostateczne zatwierdzenie,
   b) na wniosek OM, w przypadku wystąpienia incydentu krytycznego lub co dwa lata, powołuje zespół do przeprowadzenia aktualizacji oceny ryzyka oraz skutków naruszenia praw i wolności osób, których dane dotyczą,
   c) zleca audyty wewnętrzne,
   d) powołuje lub odwołuje IOD i zgłasza jego powołanie lub odwołanie do Prezesa Urzędu Ochrony Danych Osobowych (UODO),

e) nadzoruje realizację zadań wynikających z przepisów prawa powszechnie obowiązujących, o których mowa w § 3, oraz niniejszej polityki, powierzoną:
   i. IOD,
   ii. Dział Systemów ICT i Cyberbezpieczeństwa,
   iii. Dział Systemów Zarządzania.

2) IOD:
   a) prowadzi dokumentację zgodną z RODO, w tym rejestr czynności przetwarzania, w zakresie danych osobowych przetwarzanych w Systemie KRN,
   b) informuje, doradza i rekomenduje określone działania Administratorowi albo podmiotowi przetwarzającemu (jeżeli taki będzie powołany) w odniesieniu do Systemu KRN,
   c) przyjmuje informacje o naruszeniach danych osobowych w KRN, prowadzi postępowanie wyjaśniające, dokonuje zgłoszenia naruszenia do UODO i zaleca działania naprawcze oraz zapobiegawcze,
   d) realizuje inne zadania określone w Polityce Ochrony Danych Osobowych NIO-PIB (PODO).
3) ASI:
   a) przyjmuje informacje o incydentach bezpieczeństwa w KRN, zapewnia działania zapobiegawcze,
   b) realizuje inne zadania określone w PODO.
4) OM:
   a) określa indywidualne obowiązki i zakres odpowiedzialności przy przetwarzaniu danych osobowych i medycznych w systemie KRN przez podległych mu pracowników,
   b) realizuje inne zadania określone w PODO.
5) AS zarządzają infrastrukturą techniczno-systemową KRN w zakresie:
   a) konfigurowania systemów operacyjnych, bazodanowych i systemów bezpieczeństwa i narzędziowych,
   b) zakładania/modyfikowania kont imiennych innym użytkownikom na polecenie OM,
   c) dokonywania zatwierdzonych zmian w Systemie KRN,
   d) monitorowania wykonywania kopii zapasowych lub wykonywania ich na żądanie,
   e) monitorowania dostępności infrastruktury techniczno-systemowej i dostępności aplikacji,
   f) monitorowania logów,
   g) reagowania na awarie, w szczególności odtwarzanie Systemu z kopii zapasowych w przypadku awarii,
   h) opracowania i wdrażania polityk i procedur eksploatacji Systemu,
   i) opracowania i wdrożenia propozycji dodatkowych zabezpieczeń (technicznych i fizycznych),
   j) reagowania na incydenty i zgłaszania ich do OM lub IOD.
6) Dział Systemów Zarzadzania prowadzi nadzór nad dokumentacją objętą Zintegrowanym Systemem Zarządzania.

§ 6.

Bezpieczeństwo zasobów ludzkich

1. Administratorzy KRN muszą być osobami o kwalifikacjach, doświadczeniu oraz świadomości bezpieczeństwa informacji odpowiednim do zarządzania systemem informatycznym przetwarzającym znaczne ilości danych osobowych szczególnej kategorii. Ww. kwalifikacje potwierdzane są w procesie rekrutacji.
2. Osoby te muszą przejść instruktaże i szkolenia wymagane na danym stanowisku pracy, a jeżeli to konieczne powinny przejść dodatkowe szkolenia w zakresie danych osobowych oraz konfiguracji podsystemów bezpieczeństwa KRN.

§ 7.

Zarządzanie aktywami i ryzykiem

1. W systemie KRN są przetwarzane dane osobowe, w tym szczególnej kategorii, które powinny być chronione zgodnie z przepisami RODO. Na podstawie przepisów ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia ww. dane szczególnej kategorii będą nazywane jednostkowymi danymi medycznymi (lub danymi medycznymi).
2. Pełne dane osobowe są gromadzone tylko w Module Zarządzania Danymi Osobowymi (MZDO). Każdorazowe odwołanie do usług interfejsu MZDO wymaga uwierzytelnienia oraz będzie zapisywane w logach. W pozostałych modułach zamiast danych osobowych występują identyfikatory wiążące jednostkowe dane medyczne z konkretną osobą (pacjentem).
3. Szczegółowa identyfikacja aktywów w Systemie KRN odbywa się w czasie procesu szacowania ryzyka.

§ 8.

Kontrola dostępu

1. Użytkownikami Systemu są:
   1) lekarze, pracownicy szpitali, jak i prowadzący indywidualną praktykę - uprawnieni do dostępu do danych, które w przeszłości wprowadzili, co pozwoli na uzupełnienie informacji o pacjentach lub zweryfikowanie, czy dane obecnie wprowadzane są spójne z poprzednimi. Możliwy jest dostęp tylko zdalny, z własnych stacji roboczych (dotyczy to również lekarzy pracujących w NIO-PIB);
   2) pracownicy rejestrów nowotworów (KRN/WRN) - uprawnieni do dostępu do danych swojej jednostki mogą weryfikować dane wprowadzane przez lekarzy stosując te same formularze. W przypadku KRN są to wszystkie dane w Systemie. Pracownicy mają dostęp tylko poprzez tzw. terminalowe „stacje przesiadkowe";
   3) inne osoby (w ramach publicznego dostępu do danych statystycznych) - mają dostęp anonimowy do danych na publicznym Portalu Wiedzy. Są to dane statystyczne, opracowane na podstawie danych medycznych gromadzonych w KRN, pozbawione wszelkich cech umożliwiających identyfikację pacjentów lub ich jednostkowych danych medycznych;
   4) Administrator KRN (AKRN) - posiada dostęp do konta administracyjnego w Module Administracyjnym KRN i uprawnienia w zakresie:

a) zarzadzania grupami użytkowników oraz ich uprawnieniami w aplikacjach Systemu,
b) zakładania kont wewnętrznych i zewnętrznych w aplikacjach Systemu i przypisywaniu ich do grup uprawnień,
c) przesyłania użytkownikom e-mali z loginem i pierwszym hasłem, które powinno być samodzielnie zmienione przez użytkownika, zgodnie z polityką haseł obowiązującą w NIO-PIB,
d) definiowania reguł dla rejestrów narządowych.

§ 9.

Polityka haseł

Konfiguracja mechanizmów uwierzytelnienia w systemach operacyjnych, bazodanowych, systemach bezpieczeństwa i aplikacjach KRN powinna wymuszać na użytkownikach oraz AS stosowanie i zmienianie haseł zgodnie z polityką haseł obowiązującą w NIO-PIB – procedura PR60.5 Wytyczne w zakresie metod i środków uwierzytelnienia (polityka haseł).

§ 10.

Proces nadawania uprawnień

Proces nadawania uprawnień użytkownikom KRN powinien przebiegać w następujący sposób:
1) lekarz, chcący pracować w Systemie KRN, po uwierzytelnieniu w Węźle Krajowym zakłada samodzielnie własne konto w aplikacji webowej KRN. Konto to nie posiada jeszcze żadnych uprawnień w Systemie KRN;
2) AKRN dokonuje sprawdzenia, czy wnioskujący o dostęp lekarz figuruje w Centralnym Wykazie Pracowników Medycznych (CWPM) i nadaje mu uprawnienia;
3) alternatywnie lekarz przesyła do AKRN elektroniczny wniosek o nadanie uprawnień. Wniosek jest rozpatrywany przez AKRN, który po sprawdzeniu w CWPM zakłada lekarzowi konto i nadaje mu uprawnienia;
4) w przypadku tworzenia konta asystenta lekarza pracującego w Systemie KRN postępowanie jest analogiczne jak w pkt 1-3. Dodatkowo wymagana jest autoryzacja takiego konta przez lekarza;
5) pracownikom KRN/WRN zakładane są konta przez AKRN na podstawie list przesyłanych i uaktualnianych przez kierowników tych jednostek organizacyjnych. W przypadku zwolnienia pracownika lub zmiany jego zakresu obowiązków kierownik KRN/WRN niezwłocznie informuje AKRN;
6) nie rzadziej niż raz w roku kierownik KRN/WRN dokonuje przeglądu uprawnień pracowników do Systemu KRN;
7) konta nowym administratorom Systemu zakłada na polecenie Opiekuna Merytorycznego Systemu uprawniony AS lub, jeżeli jeszcze nie ma on konta, Wykonawca Systemu.

§ 11.

Zarządzanie przywilejami

Pracę administratorów Systemu KRN regulują następujące zasady:

1) W miarę możliwości powinien istnieć rozdział obowiązków na administratorów: systemowego, sieciowego i bezpieczeństwa, z zachowaniem systemu zastępstw obowiązującego w NIO-PIB;
2) W celu efektywnego zapewnienia zastępstw administratorzy powinni bezwzględnie dokumentować wszelkie zmiany w konfiguracji podlegających im urządzeń i systemów, a dokumentacja powykonawcza i ww. zmiany konfiguracyjne powinny być dostępne dla zmienników. Aktualne hasła do kont uprzywilejowanych ww. urządzeń i systemów będą deponowane u ich przełożonego lub innej wyznaczonej osoby w NIO-PIB;
3) Wszystkie systemy i urządzenia powinny być tak skonfigurowane, aby zdalne logowanie było możliwe zarówno na kontach imiennych, jak i na kontach uprzywilejowanych;
4) W przypadku odejścia z pracy/zmiany stanowiska konto imienne administratora (pracownika Wykonawcy na etapie wdrożenia) będzie natychmiast blokowane.

§ 12.

Zdalny dostęp użytkowników

1. Zdalny dostęp do Systemu jest możliwy wyłącznie po uwierzytelnieniu i autoryzacji:
   1) instytucji, z której ma mieć miejsce dostęp, na bazie certyfikatu wydanego przez zewnętrzne kwalifikowane CA, co pozwoli na zestawienie tunelu VPN;
   2) użytkownika w Węźle Krajowym z zastosowaniem wymagań Węzła Krajowego.
2. Dostęp zdalny wykonawcy Systemu w celu serwisu możliwy jest wyłącznie w tunelu VPN i zgodnie z zasadami niniejszego paragrafu.
3. Dostęp zdalny Administratora Systemu w celach administracyjnych możliwy jest wyłącznie w tunelu VPN i zgodnie z zasadami niniejszego paragrafu.
4. Pracownicy KRN i WRN są zobowiązani do przestrzegania zasad czystego biurka i ekranu, a w szczególności:
   1) odchodząc od komputera pracownik musi wylogować się z systemu lub uruchomić wygaszacz ekranu, w taki sposób aby wyłącznie wygaszacza wymagało ponownego uwierzytelnienia;
   2) wszystkie dokumenty papierowe (wydruki itp.) zawierające dane osobowe muszą być w czasie nieobecności pracownika (zwłaszcza po pracy) chronione w zamykanych szafach /szufladach / pojemnikach tak aby uniemożliwić dostęp osób niepowołanych.

§ 13.

Ochrona danych przed wyciekiem

1. Za ochronę danych osobowych (w tym medycznych) przetwarzanych na swoich stacjach roboczych na potrzeby raportowania w KRN, odpowiedzialni są lekarze, ich asystenci oraz ich pracodawcy zgodnie z przepisami ustawy o zawodzie lekarza i lekarza dentysty i rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.
2. Ochrona przed wyciekiem danych osobowych i medycznych w zakresie dostępu pracowników KRN i WRN jest zapewniona poprzez mechanizm terminalowych „stacji przesiadkowych". Dzięki temu mechanizmowi dane są wyświetlane na ekranach stacji

roboczych, ale nie mogą być wydrukowane czy zapisane na dysk stacji roboczej, z której ma miejsce dostęp do stacji przesiadkowej, a co za tym idzie i do Systemu. Stacje przesiadkowe nie będą miały dostępu do Internetu i będą miały zainstalowane oprogramowanie agenta DLP, który jako druga linia obrony chroni przed wyciekiem danych ze stacji roboczej.

3. Pracownicy KRN i WRN muszą być przeszkoleni w zakresie ochrony danych osobowych i medycznych.
4. W celu zapobiegania wyciekowi danych przy dostępie zdalnym pracowników Wykonawcy Systemu obowiązują następujące zasady:
   1) dostęp zdalny jest możliwy tylko do tych urządzeń, systemów operacyjnych, bazodanowych i narzędziowych w których nie są przetwarzane dane osobowe;
   2) dostęp do aplikacji i instancji bazy danych Modułu Zarządzania Danymi Osobowymi (MZDO), jak również maszyn wirtualnych na których jest zainstalowane ww. oprogramowanie i instancja bazy danych możliwy jest tylko pod nadzorem AS.

§ 14.

Zarządzanie infrastrukturą serwerową

1. W zarządzaniu infrastrukturą serwerową i sieciową Systemu AS powinien wykorzystywać procedury i dokumenty wymienione w załączniku nr 1 do niniejszej polityki.
2. Monitorowanie infrastruktury:
   1) System KRN musi być monitorowany w zakresie dostępności i poziomu usług przez odpowiednio skonfigurowane narzędzie, które zbiera dane nt. zajętości zasobów (CPU, RAM, HDD), dostępności interfejsów, działających procesów i dostępności aplikacji webowych;
   2) w przypadku awarii lub zagrożenia awarią generowane są alerty, które AS lub Wykonawca Systemu (w okresie gwarancji) obsługują zgodnie z procedurą monitorowania dostępności KRN;
   3) w przypadku zagrożenia poważną awarią AS niezwłocznie informuje ASI i OM oraz podejmuje działania zgodnie z ich wytycznymi.
3. Ochronę przed szkodliwym oprogramowaniem lub kodem szkodliwym Systemu KRN, zapewnia urządzenie zaporowe wyposażone w moduły zapobiegające atakom szkodliwego oprogramowania. Logi z ww. urządzenia muszą być przesyłane do systemu zarządzania logami.
4. Kopie zapasowe w ramach infrastruktury techniczno-systemowej Systemu KRN muszą funkcjonować na co najmniej 2 serwerach backup (jeden na Centrum Danych drugi na Zapasowym Centrum Danych) z zainstalowanym odpowiednim oprogramowaniem. Przy pomocy ww. narzędzia muszą być wykonywane kopie pełne i przyrostowe wszystkich maszyn wirtualnych Systemu KRN. Każda kopia zapasowa jest replikowana do drugiego serwera backup, który docelowo będzie zlokalizowany w innej serwerowni. Zgodnie z Polityką backup i retencji:
   1) pełną kopię każdej maszyny wirtualnej należy wykonywać raz w tygodniu;
   2) przyrostowe kopie każdej maszyny wirtualnej należy wykonywać w pozostałe dni tygodnia – 2 razy dziennie.

§ 15.

Monitorowanie bezpieczeństwa

1. Do zarządzania logami w Systemie KRN wykorzystywane jest odpowiednie oprogramowanie zbierające logi pochodzące z wielu różnych źródeł i umożliwiające ich przeszukiwanie w celu analizy.
2. Logi składowane w Systemie KRN obejmują:
   1) logi systemów operacyjnych, w tym dokumentujące działania AS i odpowiednio pracowników Wykonawcy realizujących działania serwisowe;
   2) logi komponentów składowych (np. serwerów aplikacyjnych);
   3) logi platformy wirtualizacyjnej;
   4) logi urządzeń sieciowych.
3. Każda operacja na danych osobowych jest rejestrowana przez aplikacje. Logi aplikacyjne powinny być składowane w bazie danych i powinny być przeglądane w aplikacji zarządzającej. Informacje o błędach aplikacji mogą być zapisywane w plikach.
4. Do zadań AS należy przeglądanie i analiza logów.
5. Zegary maszyn wirtualnych Systemu KRN muszą być zsynchronizowane, za pośrednictwem zapory, z zewnętrznym źródłem referencyjnym.

§ 16.

Monitorowanie wycieku danych

1. Monitorowanie wycieku danych z Systemu KRN realizowane jest przy pomocy Systemu DLP. Monitorowanie i blokowanie odbywa się na stacjach przesiadkowych (do których ma miejsce terminalowy dostęp ze stacji KRN/WRN) w zakresie:
   1) wysyłania danych protokołem http/https;
   2) wysyłania przez e-mail;
   3) drukowania;
   4) wysyłania w sieci LAN;
   5) kopiowania/wklejania.
2. System DLP monitoruje wszystkie pracujące jednocześnie stacje przesiadkowe.
3. Zakres danych podlegających kontroli przed wyciekiem jest zawarty w politykach ochrony danych zapisanych na serwerze Systemu DLP.

§ 17.

Nadzór nad oprogramowaniem produkcyjnym

1. Cały System KRN jest podzielony na dwa środowiska:
   1) produkcyjne;
   2) testowe.

   Ww. środowiska są od siebie logicznie odseparowane za pomocą mechanizmu VLAN.
2. Instalację nowych wersji aplikacji KRN przeprowadzają w ramach serwisu zgłoszeni wcześniej do NIO-PIB pracownicy Wykonawcy Systemu (w okresie gwarancji), którym konta imienne zakłada AS. Instalacja może się odbywać tylko w porze uzgodnionej z AS i powinna być najpierw zrealizowana w środowisku testowym (zgodnie z § 20 ust. 3).
3. Instalacja może odbywać się zdalnie z zastrzeżeniem sytuacji opisanych w § 12.

§ 18.

Zarządzanie podatnościami

1. Uaktualnienia i poprawki udostępniane przez producentów oprogramowania Systemu KRN instalowane są niezwłocznie, zgodnie z następującym schematem:
   1) automatyczne pobranie na wydzieloną maszynę wirtualną oraz ich dystrybucja na pozostałe maszyny;
   2) automatyczna instalacja uaktualnień i poprawek odbywająca się w oknie serwisowym, w porze nocnej, po wykonaniu kopii zapasowych.
2. Wszystkie maszyny wirtualne są nadzorowane przez system do monitorowania infrastruktury IT, który wykrywa ewentualne problemy po aktualizacji (niedziałające usługi, procesy, aplikacje webowe itp.). Nadzór nad systemem monitorującym sprawuje AS który w przypadku poważnej niekompatybilności przywraca ostatnią działającą konfigurację, odtwarzając maszynę wirtualną z kopii zapasowej. O każdym przypadku braku możliwości aktualizacji Systemu AS powiadamia OM, który będzie decydował o konieczności wdrożenia środków zaradczych.
3. OM potwierdza bezpieczeństwo Systemu KRN poprzez zlecanie podmiotowi zewnętrznemu przeprowadzenia okresowych testów podatności. Testy przeprowadzane będą co najmniej raz do roku. W przypadku wykrycia podatności OM zleca AS wdrożenie planu naprawczego (instalacja uaktualnień, hardening systemu), a w przypadku braku możliwości usunięcia podatności powiadamia o tym fakcie Dyrektora.

§ 19.

Zarządzanie siecią i ochrona kryptograficzna

1. Ochronę styku Systemu KRN z siecią publiczną i innymi systemami zapewnia wyspecjalizowany system zaporowy (dalej zapora). Komunikacja do i z Systemu powinna być ograniczona do niezbędnych protokołów i wymaganych numerów portów.
2. W warstwie sieciowej musi być zastosowany system obrony przed atakami typu sniffing i spoofing, jak również DoS/DDoS w warstwie aplikacyjnej. Zapora powinna przepuszczać połączenia zdalne użytkowników Systemu KRN zestawiane protokołem https bazującym na uznawanym za najbardziej bezpieczny (ze swojej rodziny) protokół TLS w wersji co najmniej „1.2." Ruch powinien być szyfrowany z uwierzytelnieniem serwera aplikacyjnego.
3. Połączenia z KRN do innych systemów muszą być oparte na protokole TLS 1.2 w wersji co najmniej z uwierzytelnieniem serwerów po obu stronach za pomocą certyfikatów SSL z kwalifikowanego centrum certyfikacji.
4. W ramach protokołu TLS dozwolone jest stosowanie silnych algorytmów:
   1) do szyfrowania - AES128, AES 196, AES256, CHACHA20-POLY1305;
   2) do wykonywania skrótu - SHA256 i wyższych;
   3) do realizacji podpisu i uwierzytelnienia - RSA i ECDSA;
   4) do tworzenia klucza sesyjnego - ECDHE.
5. Separacja danych i modułów realizowana jest za pomocą zapory, w której są skonfigurowane sieci VLAN. Sieci VLAN powinny być utworzone dla co najmniej:
   1) środowiska produkcyjnego;

2) środowiska testowego;
3) portalu wiedzy;
4) celów zarządzania infrastrukturą ITS i instalacji nowych wersji aplikacji;
5) strefy DMZ.

6. W celu podniesienia bezpieczeństwa dostępu z sieci publicznej utworzona jest strefa DMZ. Powinny tam być zlokalizowane:
   1) węzeł dostępowy odpowiedzialny za przyjmowanie ruchu od strony sieci publicznej i rozkładanie obciążenia między komponenty obsługujące użytkownika wewnętrznego oraz zautoryzowanego użytkownika zewnętrznego;
   2) serwery Portalu Wiedzy.
7. Dostęp ze strefy DMZ do sieci wewnętrznej musi być zablokowany, dozwolone powinno być jedynie wykonywanie zapytań od strony sieci wewnętrznej w kierunku portalu.
8. Zmiany w konfiguracji sieci VLAN mogą być wprowadzane tylko po wykonaniu szacowania ryzyka związanego z tą zmianą i jej zatwierdzeniu przez ASI i IOD.

§ 20.

Bezpieczeństwo rozwoju i wsparcia

1. System KRN powinien być zgodny z wytycznymi zawartymi w OWASP ASVS oraz wolny od podatności opisanych w dokumencie OWASP TOP (najnowsze wersje), w szczególności:
   1) SQL Injection;
   2) Broken Authentication and Session Management;
   3) Insecure Direct Object References;
   4) Security Misconfiguration;
   5) Sensitive Data Exposure;
   6) Missing Function Level Access Control;
   7) Cross-Site Request Forgery;
   8) Using Components with Known Vulnerabilities;
   9) Unvalidated Redirects and Forwards.
2. Zmiany w Systemie powinny być zarządzanie w taki sposób, aby zminimalizować ryzyko zmniejszenia poufności, integralności i dostępności.
   1) Realizacja zmiany normalnej wymaga:
      a) oszacowania ryzyka związanego ze zmianą,
      b) zaplanowania i zgody na rozpoczęcie zmiany,
      c) wprowadzenia i przetestowania zmiany na środowisku testowym,
      d) wprowadzenia zmiany na środowisku produkcyjnym,
      e) zatwierdzenia lub wycofania zmiany;
   2) Zmiany standardowe powinny być realizowane przez AS w trybie uproszczonym;
   3) Zmiany awaryjne powinny być realizowane przez AS niezwłocznie ale za wiedzą i zgodą a tam gdzie to właściwe ze wsparciem Wykonawcy systemu i/lub producentów infrastruktury techniczno-systemowej.
3. Bezpieczeństwo informacji w relacji z dostawcami usług, sprzętu i oprogramowania dla KRN należy zapewnić poprzez:

1) odpowiednie umowy zawierające obowiązek zachowania w poufności informacji uzyskanych od NIO-PIB w szczególności danych osobowych (umowy powierzenia);
2) nadzór nad pracą wykowywaną przez pracowników dostawców na terenie NIO-PIB;
3) ograniczeniu do niezbędnego minimum dostępu zdalnego lub zapewnieniu jego monitorowania.

4. Wykonawca Systemu KRN zapewnia bezpieczeństwo prac rozwojowych w zakresie kolejnych wersji aplikacji KRN w swoich środowiskach deweloperskim i testowym. WS zapewnia (w okresie gwarancji) zachowanie poufności (w tajemnicy) wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od NIO-PIB i od współpracujących z nim osób.
5. NIO-PIB może przeprowadzić kontrolę u WS albo powierzyć jej wykonanie audytorowi zewnętrznemu. Kontrola (audyt) możne dotyczyć środowiska deweloperskiego i testowego, w którym znajdują się kody źródłowe aplikacji KRN do których WS przekazał na rzecz NIO-PIB prawa autorskie i majątkowe.
6. Wymagania dotyczące zakupów sprzętu IT są zawarte w następujących procedurach:
   1) PR60.5 Zapewnienie działania i administracja serwerów;
   2) PR60.5 Zapewnienie działania i administracja sieci komputerowej i łączy;
   3) PR60.5 Zapewnienie działania sprzętu komputerowego.

   Dodatkowo przy zakupie sprzętu IT i oprogramowania należy zwracać uwagę, czy producent zapewnia wsparcie przez cały okres przez jaki NIO-PIB zamierza eksploatować dany sprzęt i oprogramowanie oraz czy poziom serwisu i warunki gwarancji/rękojmi są adekwatne do krytyczności systemu w którym dany sprzęt będzie używany.

§ 21.

Plan Zarządzania Incydentami Bezpieczeństwa

1. W przypadku wystąpienia zdarzenia, które może być incydentem bezpieczeństwa w Systemie KRN użytkownik lub osoba funkcyjna zgłasza ten fakt do swojego przełożonego lub bezpośrednio do IOD i osoby odpowiedzialnej w NIO-PIB za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
2. AS jest odpowiedzialny za reagowanie na incydenty bezpieczeństwa związane z infrastrukturą ITS oraz aplikacjami KRN.
3. IOD jest odpowiedzialny za reagowanie na naruszenia lub możliwości naruszenia praw lub wolności osób fizycznych, których dane osobowe są przetwarzane w Systemie KRN.
4. W przypadku naruszenia ochrony danych osobowych Dyrektor zgłasza ten fakt w ciągu 72 godzin do Urząd Ochrony Danych Osobowych (UODO).
5. W przypadku incydentu bezpieczeństwa w KRN - osoba odpowiedzialna w NIO-PIB za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa zgłasza ten incydent do CSIRT NASK w terminie do 24 godzin od wykrycia incydentu.
6. W każdej kwestii związanej z reagowaniem na incydenty bezpieczeństwa IOD lub AS powinni:
   1) współpracować ze sobą;
   2) żądać pomocy od innej jednostki/komórki organizacyjnej lub pracownika NIO-PIB,
   3) zwracać się o pomoc do uprawnionych podmiotów państwowych (np. CERT NASK); zewnętrznych ekspertów lub firm za zachowaniem zasady wiedzy uzasadnionej.

7. Szczegółowy wykaz procedur i dokumentów zawarto w załączniku nr 1 do niniejszej Polityki.
8. Proces zarządzania incydentami związanymi z bezpieczeństwem informacji składa się z następujących etapów, które ze względu na wymogi czasowe wynikające z obowiązującego prawa, mogą następować po sobie w różnej kolejności:
   1) po wykryciu incydentu musi nastąpić zgłoszenie zgodnie z ust. 1. Zgłoszenie powinno zawierać, w miarę możliwości, co najmniej następujące informacje:
      a) opis charakteru incydentu, w tym wskazanie kategorii i przybliżonej liczby: osób, których dane dotyczą oraz wpisów danych osobowych, których dotyczy naruszenie,
      b) opis możliwych konsekwencji incydentu,
      c) opis proponowanych działań naprawczych, w stosownych przypadkach, działań mających na celu zminimalizowanie ewentualnych negatywnych skutków;
   2) rejestracja incydentu - w zależności od typu incydentu rejestruje go w rejestrze incydentów AS lub IOD;
   3) zbieranie materiału dowodowego, który powinien obejmować w miarę możliwości:
      a) pełną informację o okolicznościach incydentu,
      b) szczegółową informację o zasobach dotkniętych incydentem,
      c) dane w postaci logów,
      d) logów z urządzeń sieciowych i urządzeń zabezpieczeń (systemy firewall, systemy antywirusowe, systemy DLP itd.) które mogły być związane z incydentem,
      e) zapisy pamięci trwałej i ulotnej systemów które mogły być przedmiotem incydentu,
      f) kategorie informacji (np. rodzaje danych osobowych), które mogą być zagrożone oraz ich zakres,
      g) ryzyko potencjalnego nadużycia lub szkody związanych z naruszeniem ochrony danych osobowych,
      h) łatwość identyfikacji osób, których dane dotyczą,
      i) dotkliwość skutków naruszenia dla poszczególnych osób (np. ryzyko kradzieży, oszustwa lub naruszenia dobrego imienia),
      j) szczególne cechy osób, których dotyczy naruszenie,
      k) liczbę osób, których dotyczy naruszenie;
   4) dysponując zebranym materiałem dowodowym, koordynujący jego obsługą powinien dokonać analizy incydentu, celem ustalenia:
      a) przyczyn incydentu,
      b) pełnego zakresu incydentu,
      c) osób lub podmiotów odpowiedzialnych za zaistniały incydent;
   5) zanim zostaną podjęte działania rozwiązujące incydent, w pierwszej kolejności powinny zostać podjęte działania mające na celu jego powstrzymanie i opanowanie oraz w miarę możliwości, odzyskanie wszelkich danych. Najważniejszym zadaniem w tej fazie jest ograniczenie potencjalnych konsekwencji i odzyskanie kontroli nad systemem. AS w porozumieniu z OM podejmuje działania w celu przywrócenia pełnej sprawności systemu poprzez:
      a) opracowanie metody rozwiązania incydentu,
      b) testowanie opracowanego rozwiązania,
      c) zastosowanie sprawdzonego rozwiązania,

d) zabezpieczenie przed dalszą utratą informacji, w szczególności danych osobowych, powinno mieć priorytet względem zabezpieczania materiału dowodowego bądź zapewniania ciągłości działania,
e) przywrócenie systemów do działania nie powinno zagrozić możliwości zebrania materiału dowodowego, w tym materiału dowodowego niezbędnego przy zgłoszeniu incydentu do organów ścigania, branżowych CSIRT/CERT lub organu nadzorczego,
f) wszelkie informacje dotyczące incydentu, jego analizy, sposobów rozwiązania oraz zgłoszenia i zawiadomienia osób których dane dotyczą, winny zostać odnotowane w Karcie Incydentu;

6) zgłoszenie organowi nadzorczemu lub innemu podmiotowi właściwemu (w wymaganych prawem przypadkach). OM biorąc pod uwagę zakres i wagę incydentu związanego z bezpieczeństwem danych osobowych inicjuje zgłoszenie incydentu organom ścigania, organowi nadzorczemu lub właściwym jednostkom CSIRT/CERT;
7) w sytuacji, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, należy bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o takim naruszeniu, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych.

§ 22.

Zarządzanie dostępnością i ciągłością działania

1. W celu zapewnienia dostępności i odporności Systemu KRN na awarie należy zastosować następujące środki techniczne i organizacyjne:
   1) implementację Systemu na maszynach wirtualnych pracujących na platformie wirtualizacyjnej;
   2) konfigurację serwerów aplikacyjnych najważniejszych podsystemów w klastrach;
   3) mechanizmy równoważenia obciążenia serwerów aplikacyjnych, przy zachowaniu wysokiej dostępności dla aplikacji wykorzystujących protokół http.
2. W ramach zapewnienia ciągłości działania AS zobowiązany jest:
   1) nie rzadziej niż raz na 3 miesiące, odtworzyć kopię produkcyjnych maszyn wirtualnych na zasoby środowiska testowego w celu upewnienia się, że proces wykonywania kopii i odtwarzania maszyn z kopii jest prawidłowy;
   2) nie rzadziej niż raz na 3 miesiące odtworzyć kopię wybranych baz danych na zasoby środowiska testowego w celu upewnienia się, że proces wykonywania kopii baz danych oraz ich odtwarzania jest prawidłowy;
   3) opracować procedury przełączania Systemu KRN z PCPD na urządzenia dedykowane do ZCPD.

§ 23.

Ochrona fizyczna systemu

1. Serwerownia w której są znajdują się urządzenia Systemu KRN musi być wyposażona w następujące techniczne środki ochrony fizycznej i systemy wspomagające:
   1) stalowe drzwi wejściowe;
   2) podłoga techniczna;
   3) system klimatyzacji;

4) czujniki temperatury;
5) system elektronicznej kontroli dostępu;
6) kamery systemu CCTV na korytarzu i przed wejściem;
7) system wykrywania włamania i napadu;
8) zintegrowany system ppoż;
9) podtrzymanie napięcia z urządzeń UPS;
10) zasilanie awaryjne z agregatu prądotwórczego.

2. Środki wymienione w ust. 1 pkt 3-10 podlegają regularnej konserwacji i testowaniu przez uprawnionych pracowników NIO-PIB i uprawnione firmy zewnętrzne.
3. Ochrona fizyczna stacji dostępowych do Systemu KRN jest w gestii jednostek organizacyjnych, w których te stacje są zlokalizowane.

W tabeli wymieniono procedery oraz dokumenty związane z Polityką Bezpieczeństwa Systemu KRN przeznaczone dla KRNAS.

Wykonawca	Nazwa dokumentu	Rodzaj dokumentu	Krótki opis
Gabos	Wykonywanie i odtwarzanie kopii zapasowych natywnych baz danych	Procedury eksploatacyjne	Procedura opisuje w jaki sposób wykonać oraz odtworzyć kopię zapasową bazy danych w sposób natywny
Gabos	Wykonywanie i odtwarzanie kopii zapasowych systemem Veeam	Procedury eksploatacyjne	Procedura opisuje w jaki sposób wykonać oraz odtworzyć kopię zapasową pełnej wirtualnej maszyny za pomocą dedykowanego systemu Veeam
Gabos	Aktualizacja pakietów systemu operacyjnego Windows	Procedury serwisowe	Procedura opisuje w jaki sposób bezpiecznie zaktualizować komponenty/pakiety natywne systemu operacyjnego dostępne z repozytorium systemu operacyjnego, dla przykładu - po wykryciu podatności pakietu. Procedura dotyczy systemu Windows
Gabos	Aktualizacja pakietów systemu operacyjnego Linux	Procedury serwisowe	Procedura opisuje w jaki sposób bezpiecznie zaktualizować komponenty/pakiety natywne systemu operacyjnego dostępne z repozytorium systemu operacyjnego, dla przykładu - po wykryciu podatności pakietu. Procedura dotyczy systemu Linux
Gabos	Aktualizacja oprogramowania HAProxy	Procedury serwisowe	Procedura opisuje sposób w jaki można dokonać aktualizacji pakietu HAProxy realizując budowę pakietu ze źródeł
Gabos	Aktualizacja komponentów aplikacji z zewnętrznego repozytorium	Procedury serwisowe	Instrukcja obrazuje w jaki sposób wykonać manualne pobranie nowej wersji kontenera aplikacji
Gabos	Zarządzanie klastrem bazodanowym oraz procedura awaryjna	Procedury serwisowe	Procedura opisująca zarządzanie bazą danych oraz postępowanie w przypadku awarii jednego z węzłów (przywrócenia pracy klastra)
Gabos	Podręczniki użytkowników systemu KRN	Dokumentacja użytkownika	Opis funkcjonalności aplikacji KRN podzielony na części: dla pracowników

Wykonawca	Nazwa dokumentu	Rodzaj dokumentu	Krótki opis
			Wojewódzkich biur Rejestracji oraz lekarzy/asystentów
Gabos	Instalacja węzła serwerowego i jego podstawowa konfiguracja	Dokumentacja administratora	Instrukcja opisuje w jaki sposób utworzyć nowy węzeł serwerowy oraz zapewnić jego "standardową" konfigurację realizowaną w ramach wdrożenia
Gabos	Instalacja HAProxy na węźle serwerowym	Dokumentacja administratora	Instrukcja opisuje instalację i konfigurację HAProxy ze źródeł
Gabos	Utworzenie klastra HAProxy z pływającym adresem IP	Dokumentacja administratora	Instrukcja opisuje w jaki sposób utworzyć klaster z pływającym adresem IP używając narzędzi pacemaker
Gabos	Instalacja silnika bazy danych	Dokumentacja administratora	Instrukcja opisuje w jaki sposób zainstalować jednowęzłowy serwer bazy danych używanych przez aplikację
Gabos	Instalacja i konfiguracja środowiska docker	Dokumentacja administratora	Instrukcja opisuje w jaki sposób zainstalować oraz skonfigurować środowisko docker na węźle serwerowym
Gabos	Instalacja i konfiguracja klastra bazy danych	Dokumentacja administratora	Instrukcja opisuje w jaki sposób zainstalować dwuwęzłowy klaster bazy danych używanych przez aplikację za pomocą pgpool-II i postgresql-13
Gabos	Dokumentacja środowiska i osadzenie komponentów	Dokumentacja administratora	Dokument opisuje schemat całego środowiska oraz opisuje administracyjnie za co odpowiadają dane komponenty i jak są osadzone i skonfigurowane