ZARZĄDZENIE NR 3

PRZEWODNICZĄCEGO NACZELNEJ KOMISJI BIOETYCZNEJ

z dnia 18.07.2023 r.

w sprawie ustalenia Polityki Bezpieczeństwa Teleinformatycznego w Naczelnej Komisji Bioetycznej

Na podstawie art. 15 ust. 9 ustawy z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi (Dz. U. 2023 poz. 605) zarządza się, co następuje:

§ 1 1. Ustala się Politykę Bezpieczeństwa Teleinformatycznego w Naczelnej Komisji Bioetycznej stanowiącej załącznik do niniejszego Zarządzenia.

§ 2 1. Zarządzenie wchodzi w życie z dniem podpisania.

PRZEWODNICZĄCY NACZELNEJ KOMISJI BIOETYCZNEJ

Załącznik do Zarządzenia nr 3
Przewodniczącego Naczelnej Komisji
Bioetycznej
z dnia 18.07.2023 r.

Polityka bezpieczeństwa teleinformatycznego w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Obowiązuje od:	**18.07.2023 r.**
Wersja:	**1.0**

Spis treści

Rozdział 1

Postanowienia ogólne

§ 1.

1. Polityka bezpieczeństwa teleinformatycznego w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych (dalej: Polityka) określa zasady funkcjonowania systemu zarządzania bezpieczeństwem teleinformatycznym w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych (dalej: NKB), w tym ochrony Aktywów wykorzystywanych w ramach Systemu teleinformatycznego.
2. Za nadzór nad stosowaniem Polityki odpowiada Inspektor Ochrony Danych.
3. Ilekroć w Polityce jest mowa o Członkach NKB, jej postanowienia stosuje się odpowiednio do innych Użytkowników.

§ 2.

1. Definicje użyte w Polityce oznaczają:
   1) ABM – Agencja Badan Medycznych;
   2) Administrator Systemu – pracownik lub komórka organizacyjna ABM, Członek NKB, któremu powierzono nadzór nad Systemem teleinformatycznym;
   3) Aktywa – wszystko co ma wartość dla NKB. Aktywa dzielą się na informacje, dane oraz tzw. Aktywa wspierające (w szczególności sprzęt, budynki i pomieszczenia, oprogramowanie, zasoby ludzkie);
   4) Członek NKB – Przewodniczący NKB lub inny członek NKB;
   5) Dostępność – właściwość informacji polegająca na byciu dostępnym i użytecznym na żądanie uprawnionego podmiotu;
   6) Dziennik pracy systemu – rejestr wykonywanych czynności oraz zdarzeń zachodzących w Systemie teleinformatycznym;
   7) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi;
   8) Incydent bezpieczeństwa – pojedyncze zdarzenie lub seria niepożądanych, niespodziewanych zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych, zagrażają bezpieczeństwu lub stanowią naruszenie obowiązujących zasad bezpieczeństwa;
   9) Integralność – właściwość informacji polegająca na jej dokładności i kompletności;
   10) IOD - Inspektor Ochrony Danych;
   11) Konto – część Systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), która jest przypisana do identyfikatora Użytkownika;
   12) Kopia archiwalna – duplikat danych, przechowywanych z uwagi na przepisy prawa lub potrzeby dokumentowania działalności NKB. Kopia archiwalna nie służy do odtworzenia Systemu teleinformatycznego lub jego elementów;
   13) Kopia zapasowa – duplikat danych, przechowywany na wymiennym nośniku komputerowym, służący do odtworzenia Systemu teleinformatycznego lub jego elementów;
   14) Kopie – Kopie zapasowe i Kopie archiwalne;
   15) Nośnik danych – urządzenie wymienne i przenośne umożliwiające zapis, modyfikację lub odczyt danych, takie jak: pendrive, dysk przenośny, dysk wewnętrzny, karta pamięci, taśma magnetyczna, nośnik optyczny itp.;
   16) Podatność – słabość Aktywa lub grupy Aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń;
   17) Podmiot zewnętrzny – osoba prawna, osoba fizyczna lub inny podmiot dostarczający na rzecz NKB produkty lub świadczący na rzecz NKB usługi na podstawie umowy lub innego stosunku prawnego (w tym w ramach zawartych umów przez ABM), która w związku z realizacją tych zadań przetwarza informacje, niebędący Członkiem NKB, personelem zapewniającym obsługę NKB, członkiem komisji bioetycznej wpisanej na listę komisji dokonującej oceny wniosku o przeprowadzenie badania klinicznego, ekspertem, o który mowa w art. 30 ust. 4 i 5 Ustawy, przedstawicielem podmiotów, o którym mowa w art. 30 ust. 3 Ustawy;

18) Portal Unii Europejskiej (CTIS) - określony w art. 80 rozporządzenia 536/2014, jeden punkt na poziomie Unii Europejskiej, za pośrednictwem, którego przekazywane są dane i informacje dotyczące badań klinicznych zgodnie z rozporządzeniem 536/2014;
19) Poufność – właściwość informacji polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieuprawnionym osobom;
20) Przewodniczący NKB – Przewodniczący NKB, Zastępca Przewodniczącego NKB lub osoba przez niego upoważniona;
21) System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. System teleinformatyczny obejmuje między innymi sprzęt komputerowy, urządzenia przenośne, oprogramowanie systemowe, systemy (podsystemy), sieć, aplikacje;
22) Urządzenie przenośne – informatyczne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie lub wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią, takie jak laptop, smartfon, tablet lub nośnik danych;
23) Ustawa – ustawa z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi;
24) Użytkownik – Członek NKB lub inna osoba realizująca zadania na rzecz NKB na podstawie umowy lub innego stosunku prawnego, która w związku z realizacją tych zadań przetwarza informacje;
25) Właściciel aktywa – Przewodniczący NKB lub inna osoba głównie odpowiedzialna za zarządzanie danym Aktywem;
26) Zagrożenie – potencjalna przyczyna niepożądanego incydentu bezpieczeństwa, którego skutkiem może być szkoda dla Systemu teleinformatycznego.

§ 3.

1. NKB zapewnia bezpieczeństwo Systemu teleinformatycznego, w szczególności poprzez:
   1) zarządzanie bezpieczeństwem Aktywów składających się na System teleinformatyczny, poprzez ochronę tych Aktywów przez utratą, uszkodzeniem, nieuprawnioną modyfikacją lub naruszeniem w inny sposób;
   2) zapewnienie odpowiedniej konfiguracji Aktywów, o których mowa w pkt 1, w tym tworzenie Kopii zapasowych, monitorowanie Aktywów oraz ich ochronę przed złośliwym oprogramowaniem;
   3) zarządzanie dostępem do Aktywów, o których mowa w pkt 1;
   4) określenie zasad:
      a) zarządzania Systemem teleinformatycznym przez Administratora Systemu i inne upoważnione osoby;
      b) korzystania z Systemu teleinformatycznego przez Użytkowników.
2. Wymagania dotyczące bezpieczeństwa, określone w przepisach prawa powszechnie obowiązującego oraz regulacjach wewnętrznych NKB powinny być uwzględniane w każdym procesie realizowanym z wykorzystaniem Systemu teleinformatycznego, w tym w ramach tworzenia nowego i rozbudowy istniejącego oprogramowania.

§ 4.

1. Zasady określone w Polityce, dotyczące zarządzania Systemem teleinformatycznym, obowiązują Administratora Systemu oraz inne osoby, którym powierzono wykonywanie czynności dotyczących zarządzania tym systemem.
2. O ile Polityka nie stanowi inaczej, pozostałe zasady dotyczą wszystkich Użytkowników.

Rozdział 2

Podstawowe zasady eksploatacji Systemu teleinformatycznego

§ 5.

1. Administrator Systemu prowadzi i na bieżąco aktualizuje ewidencję Aktywów stanowiących elementy Systemu teleinformatycznego.
2. Ewidencja, o której mowa w ust. 1, może być prowadzona w formie elektronicznej, pod warunkiem zachowania historii zmian.
3. Ewidencja zawiera co najmniej:
   1) nazwę i opis Aktywa;
   2) informacje o Właścicielu aktywa.
4. Ewidencja podlega okresowemu przeglądowi przez Administratora Systemu, nie rzadziej niż raz na pół roku.
5. Niezależnie od postanowień ust. 4, Właściciele aktywów informują na bieżąco Administratora Systemu o zmianach dotyczących powierzonych im Aktywów.

§ 6.

1. W celu zapewnienia prawidłowej i bezpiecznej eksploatacji kluczowego oprogramowania użytkowego wprowadza się, realizuje i dokumentuje procedury eksploatacyjne, które muszą być zgodne z cyklem życia tego oprogramowania. W przypadku nowych elementów Systemu teleinformatycznego procedury eksploatacyjne obejmują prace projektowe, testowanie, obsługę i ich rozwój.
2. Procedury eksploatacyjne elementów Systemu teleinformatycznego zawierają co najmniej instrukcje ich bezpiecznej eksploatacji oraz dokładny opis zastosowanych w ich konstrukcji mechanizmów zabezpieczających, zarządzanych i nadzorowanych przez wyznaczoną grupę Użytkowników.
3. Procedury eksploatacyjne chronione są przed nieuprawnionym dostępem.
4. Procedury eksploatacyjne są opracowywane przez Administratora Systemu. Przewodniczący NKB może powierzyć nadzór nad procedurami eksploatacyjnymi wybranych elementów Systemu teleinformatycznego (na przykład systemu administrowania podpisem elektronicznym) wyznaczonemu członkowi NKB.
5. Za prawidłową organizację pracy, zapewnienie bezpieczeństwa oraz eksploatację Systemu teleinformatycznego, w tym komputerów i innych urządzeń stanowiących elementy Systemu teleinformatycznego, odpowiedzialni są Członkowie NKB.
6. Za bezpieczeństwo i dostęp do komputera i innych urządzeń stanowiących elementy Systemu teleinformatycznego oraz za ich prawidłową eksploatację odpowiedzialny jest Użytkownik danego komputera lub innego urządzenia.
7. Uprawnienia powinny być rozdzielone w taki sposób, aby żaden Użytkownik nie mógł uzyskać dostępu, modyfikować lub korzystać z Aktywów bez autoryzacji drugiego Użytkownika mającego dostęp do tych Aktywów lub wykrycia takiego przypadku dostępu lub modyfikacji.

§ 7.

1. Wnioski mające na celu podniesienie poziomu bezpieczeństwa Systemu teleinformatycznego należy zgłaszać do IOD.
2. IOD analizuje wniosek, w razie potrzeby konsultując się z Administratorem Systemu oraz właściwymi Członkiem NKB a następnie przekazuje swoje rekomendacje Członkowi NKB lub innej upoważnionej osobie.
3. Wnioski dotyczące bieżącego funkcjonowania Systemu teleinformatycznego należy zgłaszać do Administratora Systemu. Zmiany w Systemie teleinformatycznym wynikające z wniosków wymagają uzgodnienia z IOD.

Rozdział 3

Zarządzanie dostępem do Systemu teleinformatycznego

§ 8.

1. Użytkownik jest jednoznacznie identyfikowany poprzez indywidualną nazwę Użytkownika (identyfikator).

2. Stosowane identyfikatory Użytkownika nie wskazują na poziom uprawnień danego Użytkownika.
3. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego Użytkownika (chyba, że z przyczyn technicznych nie ma możliwości stosowania osobistych identyfikatorów).
4. Raz użyty identyfikator nie może być przydzielony innemu Użytkownikowi.
5. Uprawnienia dostępu są nadawane wyłącznie w zakresie niezbędnym do prawidłowego wykonywania obowiązków powierzonych Użytkownikowi.
6. Bezzasadne nadanie uprawnień dostępu stanowi Incydent bezpieczeństwa.
7. Uprawnienia Użytkownika w Systemie teleinformatycznym określa Przewodniczący NKB w porozumieniu i za zgodą Właścicieli aktywów, do których podległy Użytkownik otrzymuje dostęp, a uprawnienia do portalu Unii Europejskiej (CTIS) określa tylko Przewodniczący NKB, nie upoważniając do tej czynności innej osoby.
8. Dostęp jest przyznawany, modyfikowany i odbierany przez Administratora Systemu na podstawie wniosku Przewodniczącego NKB , którego wzór stanowi Załącznik nr 1 do Polityki.
9. Administrator Systemu prowadzi rejestr Użytkowników wraz z informacją o uprawnieniach do poszczególnych elementów Systemu teleinformatycznego, w tym aplikacji.

§ 9.

1. Administrator Systemu raz w miesiącu dokonuje przeglądu stanu aktywności Kont Użytkowników.
2. Konta nieużywane przez okres co najmniej 30 dni są blokowane z wyłączeniem Kont pocztowych Członków NKB, którzy są długotrwale nieobecni z przyczyn usprawiedliwionych dłużej niż 30 dni.

§ 10.

1. Prawa uprzywilejowanego dostępu tj. większe uprawnienia niż wynika to z realizowanych typowych zadań Użytkownika, podlegają ścisłej ewidencji prowadzonej przez Administratora Systemu.
2. Prawa uprzywilejowanego dostępu nie mogą być nadane przed zakończeniem procesu autoryzacji Użytkownika, na podstawie wniosku, o którym mowa w § 8 ust. 8 stosowanego odpowiednio.
3. Uprzywilejowane Konto nie może służyć do realizacji typowych zadań Użytkownika. W przypadku potrzeby jednoczesnego wykonywania zadań Użytkownika o zwykłym dostępie i takich wymagających dostępu uprzywilejowanego, prawa uprzywilejowanego dostępu przydziela się innemu identyfikatorowi Użytkownika, niż temu wykorzystywanemu do typowych zadań.
4. Prawa uprzywilejowanego dostępu podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
5. Prawa uprzywilejowanego dostępu nadawane są osobie zastępującej danego Użytkownika na czas jego nieobecności. Osobie zastępującej Użytkownika przekazywane są Hasła dostępu oraz informacje o czynnościach wykonywanych na danym stanowisku.
6. Nadawane prawa uprzywilejowanego dostępu podlegają regularnym przeglądom i nadzorowi przez Administratora Systemu.

§ 11.

1. Uprawnienia Administratora Systemu są nadawane ograniczonej liczbie Użytkowników.
2. Mechanizm dziedziczenia uprawnienia Administratora Systemu na podstawie uprawnień Administratora Systemu nadanych w systemie operacyjnym lub na platformie bazodanowej jest zablokowany.

§ 12.

1. Wyznaczony przez Przewodniczącego NKB Członek NKB jest odpowiedzialny za aktualność uprawnień przyznanych nadzorowanym Użytkownikom do pracy w Systemie teleinformatycznym.
2. W tym celu wyznaczony przez Przewodniczącego NKB Członek NKB monitoruje uprawnienia podległych Użytkowników:
   1) na bieżąco, nie rzadziej niż raz na tydzień;
   2) każdorazowo, w przypadku zmian w stosunku prawnym łączącym NKB i Użytkownika lub Podmiotu zewnętrznego, w szczególności ustaniu stosunku prawnego.

3. W przypadku ustania stosunku prawnego łączącego NKB i Użytkownika lub gdy z innych względów niezbędne jest odebranie lub modyfikacja uprawnień dostępu Użytkownika, Członek NKB niezwłocznie informuje o tym Administratora Systemu.

§ 13.

1. W przypadku uzyskania informacji o zmianie lub ustaniu stosunku prawnego łączącego NKB i Użytkownika:
   1) Administrator Systemu modyfikuje prawa dostępu Użytkownika, stosownie do okoliczności;
   2) w przypadku odbioru praw dostępu, gdy uprawnienia dostępu zostały przyznane większej grupie Użytkowników (na przykład na podstawie identyfikatora grupy), należy usunąć Użytkownika z każdej grupowej listy dostępu oraz poinformować pozostałych Użytkowników w grupie, aby nie dzielili się informacjami z Użytkownikiem, któremu odebrano prawa dostępu;
   3) jeżeli Użytkownik posiada Hasła dostępu do Kont, które pozostają aktywne, należy dokonać zmiany Haseł.
2. Modyfikacja praw dostępu powinna być odzwierciedlona w dokumentacji dotyczącej praw dostępu.

§ 14.

1. Dostęp Podmiotu zewnętrznego do Systemu teleinformatycznego wymaga przeprowadzenia udokumentowanej oceny ryzyka.
2. Ocenę ryzyka przeprowadza Właściciel aktywa na podstawie informacji dostarczonych przez Administratora Systemu, uwzględniając w szczególności:
   1) podstawę udzielenia dostępu dla danego Podmiotu zewnętrznego;
   2) zakres i sposób dostępu do Systemu teleinformatycznego, w tym zakres przydzielanych uprawnień;
   3) proponowane przez Administratora Systemu rozwiązania techniczne i organizacyjne służące ograniczeniu ryzyka dla bezpieczeństwa Systemu teleinformatycznego.
3. Zgodę na udzielenie dostępu Podmiotowi zewnętrznemu wydaje Właściciel aktywa, po zaakceptowaniu i wdrożeniu rozwiązań, o których mowa w ust. 3 pkt 3.
4. W przypadku zmiany okoliczności mogącej mieć wpływ na poziom ryzyka należy przeprowadzić ponowną ocenę ryzyka, w zakresie uzasadnionym zaistniałą zmianą.
5. Doraźne działania serwisowe Podmiotów zewnętrznych (nie mające charakteru stałego utrzymania Systemu teleinformatycznego) są dokumentowane przez Administratora Systemu w Dzienniku pracy systemu. Zapis w Dzienniku pracy systemu zawiera co najmniej:
   1) dokładny czas rozpoczęcia i zakończenia działania serwisowego;
   2) identyfikację osoby realizującej działania serwisowe po stronie Podmiotu zewnętrznego oraz nadzorującej te działania po stronie NKB;
   3) dokładny opis przeprowadzonych działań wraz ze wskazaniem statusu tych działań (na przykład: „wymagające kontynuacji", „zakończone").
6. Doraźne działania serwisowe w Systemie teleinformatycznym osób nie będących uprawnionymi Członkami NKB dokonywane są w obecności Administratora Systemu.
7. Osobie reprezentującej Podmiot zewnętrzny, wykonującej działania serwisowe, nie mogą zostać nadane uprawnienia Administratora Systemu. Jeśli wyjątkowa sytuacja uzasadnia taką potrzebę, to nadanie takich uprawnień wymaga zgody Właściciela aktywów. Niezwłocznie po zakończeniu pracy uprawnienia Administratora Systemu oraz jakiekolwiek inne uprawnienia nadane osobie reprezentującej Podmiot zewnętrzny muszą zostać odebrane.
8. W przypadku dokonywania zmian konfiguracji (naprawy, rekonfiguracje) przez Podmiot zewnętrzny NKB zapewnia odpowiednie uprawnienia do użycia oprogramowania narzędziowego służącego do zarządzania konfiguracją.

Rozdział 4

Zarządzanie Hasłami dostępu do Systemu teleinformatycznego oraz innymi poufnymi informacjami uwierzytelniającymi

§ 15.

1. W celu uwierzytelnienia Użytkowników NKB wykorzystuje Hasła lub klucze kryptograficzne chronione Hasłem.
2. Niedopuszczalne jest występowanie w Systemie teleinformatycznym Kont niezabezpieczonych Hasłem.
3. Administrator Systemu, za pomocą ustawień systemowych, wymusza natychmiastową zmianę Hasła początkowego, przydzielonego Użytkownikowi, na nowe przez niego wybrane (o ile istnieją możliwości techniczne takiego wymuszenia).
4. Zabronione jest przekazywanie Haseł za pośrednictwem osób trzecich lub za pośrednictwem otwartych wiadomości poczty elektronicznej. Nie dotyczy to Haseł tymczasowych do systemów wyposażonych w mechanizm wymuszający zmianę Hasła przy pierwszej próbie uwierzytelnienia się w danym systemie.
5. Hasła tymczasowe, dostarczane w przypadku utraty Hasła, są wydawane dopiero po pozytywnej weryfikacji tożsamości Użytkownika.
6. Użytkownik potwierdza odbiór Haseł w sposób określony przez Administratora Systemu.

§ 16.

1. Systemy operacyjne, aplikacje oraz o ile to stosowne, inne elementy Systemu teleinformatycznego spełniają wymagania dotyczące możliwości ustawienia następujących parametrów Haseł:
   1) siły Hasła (długość i złożoność Haseł);
   2) maksymalnego okresu ważności;
   3) ograniczenia możliwości ponownego wykorzystania Hasła (pamięć ostatnio używanych Haseł).
2. Przy konfigurowaniu mechanizmów logowania uwzględnia się następujące zasady:
   1) Użytkownik zobowiązany jest do podania swojego identyfikatora oraz Hasła;
   2) w polu logowania nie jest prezentowana ostatnio użyta nazwa Użytkownika (o ile system to umożliwia);
   3) wpisywane Hasło nie jest widoczne na ekranie logowania;
   4) w trakcie procedury logowania nie są wyświetlane komunikaty pomocnicze, które mogłyby pomóc w dostępie osobie nieuprawnionej;
   5) w przypadku wystąpienia błędu nie jest wskazywane, która z informacji jest niepoprawna;
   6) do chwili pomyślnego zalogowania się nie są wyświetlane identyfikatory systemu lub aplikacji;
   7) system logowania chroni przed próbami zalogowania się przez podanie wszystkich możliwych kombinacji;
   8) wykonywane są zapisy prób logowania (zarówno udanych, jak i nieudanych);
   9) w przypadku wykrycia próby lub udanego przełamania zabezpieczeń logowania generowany jest alert;
   10) nieaktywne sesje są zamykane po określonym czasie nieaktywności;
   11) liczba nieudanych prób logowania do systemu jest ograniczona;
   12) po maksymalnie pięciu następujących po sobie nieudanych próbach logowania Konto jest blokowane;
   13) o ile to zasadne – możliwości zalogowania się do systemu są ograniczone do określonych przedziałów czasowych („okna logowania");
   14) szyfrowanie przesyłanych Haseł.
3. Ustawienia zasad zarządzania Hasłami w systemach operacyjnych obejmują:
   1) wymuszanie użycia indywidualnych Haseł;
   2) wybór i zmianę Haseł przez Użytkowników;
   3) potwierdzanie zmiany Haseł dla uniknięcia błędów podczas ich wprowadzania;
   4) wymuszenie wyboru Haseł o odpowiedniej jakości, tj.: składających się co najmniej z 12

znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne;
5) wymuszenie zmiany Haseł tymczasowych przy pierwszym rejestrowaniu się w systemie;
6) zapamiętywanie Haseł przez system w celu zapobiegania ponownemu ich użyciu (liczba Haseł pamiętanych przez system powinna wynosić co najmniej 12).

4. Postanowienia paragrafu stosuje się odpowiednio do innych poufnych informacji uwierzytelniających.

§ 17.

Tworzenie automatów (skryptów) programowych odblokowujących dostęp, na przykład po upływie określonego czasu, jest zabronione.

§ 18.

Szczegółowe zasady tworzenia Haseł określa Regulamin użytkownika systemu teleinformatycznego, stanowiący Załącznik nr 2 do Polityki.

§ 19.

1. Specjalne warunki przechowywania duplikatów Haseł dotyczą:
   1) elementów aktywnych sieci teleinformatycznej;
   2) Haseł administracyjnych do systemów, aplikacji i baz danych;
   3) konfiguracji komputerów, w tym Hasła do BIOS.
2. Hasła administracyjne przechowuje się w postaci zaszyfrowanej.

§ 20.

1. Ewidencja Haseł i innych poufnych informacji uwierzytelniających jest prowadzona przez Administratora Systemu i jest przechowywana w miejscu zabezpieczonym przed dostępem nieupoważnionych osób.
2. Za aktualność przechowywanych Haseł odpowiedzialny jest Administrator Systemu.

Rozdział 5
Bezpieczeństwo sieci

§ 21.

NKB zapewnia bezpieczeństwo sieci w szczególności za pomocą:
1) zapory typu firewall oraz systemów wykrywania i przeciwdziałania włamaniom na poziomie sieci i hostów;
2) oprogramowania antywirusowego stosowanego podczas wymiany danych pomiędzy siecią NKB a sieciami należącymi do innych organizacji lub sieciami publicznymi;
3) rozdzielania sieci – sieć grupowana jest w zależności od wykonywanych zadań w logicznie rozdzielonych segmentach sieciowych (VLAN);
4) uwierzytelniania Użytkowników i urządzeń (o ile jest to możliwe techniczne);
5) wyłączania (blokowania) usług sieciowych, które nie są wykorzystywane lub ich korzystanie nie jest uzasadnione potrzebami NKB albo są uznawane za niebezpieczne, niezależnie do tego czy są udostępniane wewnątrz sieci NKB, czy także na zewnątrz;
6) konfigurowania aplikacji, usług lub systemów operacyjnych w sposób zapewniający bezpieczeństwo informacji;
7) aktualizowania aplikacji, systemów operacyjnych oraz usług sieciowych do najnowszej oraz bezpiecznej i stabilnej wersji;
8) stosowania fizycznych zabezpieczeń dostępu.

§ 22.

1. Podsieci logiczne VLAN wewnątrz sieci NKB tworzy się dla elementów Systemu teleinformatycznego o różnych wymaganiach bezpieczeństwa. Każda z takich podsieci stanowi odrębną strefę bezpieczeństwa, do której dostęp musi być kontrolowany z wykorzystaniem zapory typu firewall, zapewniającej ścisłą kontrolę oraz selektywny dostęp do wybranych usług i systemów

w danej strefie.

2. Ruch między podsieciami powinien być kontrolowany za pomocą reguł filtrujących wprowadzonych w urządzeniach sieciowych oraz serwerach.
3. Należy stosować mechanizmy kontroli trasowania (routingu) w sieciach oparte na zdefiniowaniu możliwych tras pakietów w sieci.
4. Sygnatury systemów wykrywania i przeciwdziałania włamaniom podlegają regularnej aktualizacji.
5. Komunikacja systemów zewnętrznych z Systemem teleinformatycznym NKB powinna być realizowana poprzez routery dostępowe przyłączone w jednej ze stref zapory typu firewall – strefy dostępowej dedykowanej dla komunikacji z systemami zewnętrznymi.
6. Do realizacji połączeń z systemami zewnętrznymi wymagane jest wykorzystanie łączy dedykowanych. W szczególnie uzasadnionych przypadkach oraz do celów testowych zezwala się na dostęp do systemów aplikacyjnych ABM za pośrednictwem łączy wirtualnych realizowanych poprzez sieć publiczną z wykorzystaniem technologii VPN (połączenia terminowane w zaporze typu firewall lub koncentratorze VPN zlokalizowanym w strefie dostępowej).

§ 23.

1. NKB wykorzystuje mechanizm identyfikacji urządzeń do uwierzytelniania połączeń z określonych lokalizacji lub urządzeń.
2. Identyfikacja urządzeń realizowana jest w oparciu o przydzielanie stałego adresu IP, na podstawie unikalnego adresu MAC, dla każdego urządzenia podłączanego do sieci NKB.
3. W szczególnie uzasadnionych przypadkach możliwe jest odstępstwo od stosowania mechanizmu określonego w ust. 1 i 2. O zastosowaniu odstępstwa decyduje Administrator Systemu w porozumieniu z IOD.

§ 24.

1. Wszelkie zmiany topologii sieci lub konfiguracji urządzeń sieciowych są przeprowadzane zgodnie z metodologią zarządzania zmianą.
2. Urządzenia sieciowe są chronione Hasłem dostępu przechowywanym w postaci zaszyfrowanej.
3. Zarządzanie siecią odbywa się z wydzielonych stacji roboczych zlokalizowanych w sieci lokalnej lub przez konsole podłączone bezpośrednio do urządzeń sieciowych.

§ 25.

1. Ustawienia parametrów konfiguracyjnych oraz przeprowadzenie diagnostyki urządzeń Systemu teleinformatycznego wykonuje się z lokalnej konsoli administracyjnej, wykorzystując do tego celu dedykowane Konta administracyjne (lokalny dostęp administracyjny).
2. W szczególnych przypadkach działania administracyjne mogą być wykonywane w trybie zdalnego dostępu. Zdalny dostęp administracyjny jest realizowany wyłącznie z wybranych hostów, zlokalizowanych w segmencie sieci wewnętrznej, dedykowanym dla systemów administracyjnych.
3. Do nawiązywania zdalnych połączeń administracyjnych muszą być stosowane:
   1) protokoły komunikacyjne zapewniające bezpieczne uwierzytelnianie Użytkowników, poufność i integralność przesyłanych danych, w szczególności IPsec;
   2) łącze dedykowane z wydzielonej stacji klienckiej do Systemu teleinformatycznego;
   3) połączenie szyfrowane do Systemu teleinformatycznego z zakończeniem na serwerze SSH-relay;
   4) oddzielna autoryzacja Użytkownika zestawiającego tunel SSH, obejmująca adres IP stacji klienckiej oraz Konto Użytkownika na serwerze SSH.

§ 26.

1. Sieć NKB może być podłączona do sieci ogólnodostępnych (np. sieć publiczna Internet) tylko na poziomie tzw. rozległej sieci komputerowej (WAN) i jedynie przy użyciu specjalnych systemów zabezpieczających (zapora typu firewall, systemy IDS/IPS).
2. Wszystkie połączenia pomiędzy sieciami publicznymi a siecią NKB są realizowane przy użyciu specjalnych systemów zabezpieczających (zapora typu firewall, systemy wykrywania włamań).

3. Architektura zapory typu firewall oddzielającej sieć publiczną od sieci NKB powinna być skonfigurowana na zasadzie przepuszczania tylko ściśle zdefiniowanego ruchu przychodzącego i wychodzącego.
4. Serwery zewnętrznych usług sieciowych zlokalizowane są w wydzielonych strefach ograniczonego zaufania (DMZ).

§ 27.

Informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje podlegają ochronie, w szczególności przed przerwaniem transmisji, błędom w trasowaniu, nieuprawnionym zmianom, ujawnieniu lub powieleniu.

Rozdział 6
Bezpieczeństwo systemów operacyjnych

§ 28.

W NKB stosuje się następujące mechanizmy bezpieczeństwa systemów operacyjnych:
1) uwierzytelnianie Użytkowników, zgodnie z przyjętymi zasadami kontroli dostępu;
2) rejestrowanie nieudanych prób dostępu do systemu;
3) rejestrowanie korzystania z przywilejów systemowych;
4) generowanie alarmów w przypadku naruszenia reguł bezpieczeństwa systemu;
5) ograniczanie czasu nieaktywności sesji Użytkowników.

§ 29.

1. W celu wymuszenia ochrony urządzeń Systemu teleinformatycznego stosuje się następujące mechanizmy uruchamiane w przypadku stwierdzenia braku aktywności Użytkownika:
   1) blokowanie lub wyłączanie stacji roboczej (sesji połączeniowej),
   2) powtarzanie identyfikacji i uwierzytelnianie Użytkownika.
2. System operacyjny po ustalonym okresie bezczynności Użytkownika, jednak nie dłużej niż 10 minut, przechodzi w stan nieaktywny, w którym blokowany jest dostęp do konsoli; powrót do stanu aktywności wymaga podania Hasła.

Rozdział 7
Bezpieczeństwo wymiany danych

§ 30.

1. Serwisy intranetowe i ekstranetowe są lokalizowane na serwerach, do których dostęp wymaga identyfikacji i uwierzytelnienia.
2. Udostępnienie informacji w serwisach intranetowych lub ekstranetowych wymaga zatwierdzenia przez Właściciela aktywa.
3. Dostęp do serwisów ekstranetowych posiadają Członkowie NKB. W uzasadnionych przypadkach dostęp do serwisów ekstranetowych mogą posiadać inni Użytkownicy.

§ 31.

1. Uprawnionymi do korzystania z poczty elektronicznej NKB na czas obowiązywania umowy lub innego stosunku prawnego są Członkowie NKB.
2. Uprawnienia do korzystania z poczty elektronicznej mogą być przyznane także członkom komisji bioetycznej wpisanej na listę dokonująca oceny wniosku o przeprowadzenie badania klinicznego, ekspertom, o którym mowa w art. 30 ust. 4 i 5 Ustawy lub przedstawicielom podmiotów, o których mowa w art. 30 ust. 3 Ustawy na czas trwania umowy lub innego stosunku prawnego.
3. Użytkownicy otrzymują uprawnienia po podpisaniu umowy lub nawiązaniu innego stosunku prawnego, na podstawie wniosku, o którym mowa w § 8 ust. 8 stosowanego odpowiednio.
4. W systemie poczty elektronicznej mogą funkcjonować Konta organizacyjne i funkcyjne, utworzone na wniosek Przewodniczącego NKB na potrzeby obsługi m.in., zespołów, wydarzeń i projektów na czas funkcjonowania takiego Konta określony przez Przewodniczącego NKB.

§ 32.

1. System poczty elektronicznej zapewnia w szczególności:
   1) ochronę przed szkodliwym oprogramowaniem rozpowszechnianym za pomocą poczty elektronicznej;
   2) ochronę antywirusową załączników przesyłanych w poczcie elektronicznej;
   3) ochronę antyspamową;
   4) możliwość użycia dostępnych technik kryptograficznych do ochrony poufności i integralności wiadomości poczty elektronicznej;
   5) rejestrowanie poczty elektronicznej.
2. Zasoby poczty elektronicznej (wszystkie skrzynki pocztowe) podlegają sporządzaniu Kopii zapasowej. Kopia zapasowa sporządzana jest każdego dnia. Okres przechowywania Kopii zapasowych wynosi co najmniej 3 dni.
3. System poczty elektronicznej nakłada ograniczenia rozmiaru pojedynczej skrzynki pocztowej oraz wielkości przesyłanej wiadomości.

§ 33.

1. Ruch HTTP między klientem poczty elektronicznej w Internecie a serwerem poczty elektronicznej zabezpieczony jest za pomocą protokołu szyfrującego SSL.
2. Uwierzytelnienie dostępu Użytkownika do poczty elektronicznej realizowane jest za pomocą certyfikatu (podstawowa metoda uwierzytelniania) lub identyfikatora i Hasła (zapasowa metoda uwierzytelniania).
3. Uwierzytelnienie dostępu Podmiotów zewnętrznych do wybranych elementów Systemu teleinformatycznego odbywa się za pomocą protokołu szyfrującego SSL.
4. Administrator Systemu jest odpowiedzialny za zapewnienie bezpieczeństwa pary kluczy kryptograficznych (klucz prywatny i klucz publiczny) służących do zabezpieczenia transmisji za pomocą protokołu SSL w trakcie ich generowania oraz wydania i zainstalowania certyfikatu klucza publicznego. W szczególności, generowanie pary kluczy powinno odbywać się na wydzielonej stacji roboczej w sposób uniemożliwiający przechwycenie lub modyfikację klucza prywatnego.
5. Administrator Systemu jest odpowiedzialny za ochronę kluczy w trakcie ich użytkowania, w szczególności za ochronę klucza prywatnego przed ujawnieniem lub nieautoryzowanym użyciem. W przypadku naruszenia ochrony klucza prywatnego lub jego uzasadnionego podejrzenia należy niezwłocznie przeprowadzić proces unieważniania certyfikatu.
6. Administrator systemu jest odpowiedzialny za przechowywanie kluczy kryptograficznych w okresie ich ważności. Klucze przechowywane są na zabezpieczonym Nośniku danych niepodłączonym do sieci teleinformatycznej w pomieszczeniu objętym systemem kontroli dostępu.
7. Odnowienie certyfikatu klucza publicznego musi nastąpić przed końcem okresu jego ważności.
8. Po zakończeniu użytkowania certyfikatu klucza publicznego, w przypadku stosowania go wyłącznie do zabezpieczenia komunikacji w protokole SSL, należy parę kluczy trwale zniszczyć.

§ 34.

Szczegółowe zasady korzystania z poczty elektronicznej określa Regulamin użytkownika systemu teleinformatycznego.

Rozdział 8

Ochrona antywirusowa

§ 35.

1. Stacje robocze i serwery w NKB są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory typu firewall, zapewniających integralność zasobów przechowywanych i przetwarzanych w Systemie teleinformatycznym.
2. Oprogramowanie antywirusowe jest zainstalowane w taki sposób, aby funkcjonowało przez cały czas jako oddzielny proces.
3. W Systemie teleinformatycznym NKB wdrożono scentralizowany system antywirusowy.

4. Za skuteczność oprogramowania antywirusowego w NKB odpowiada Administrator Systemu.

§ 36.

1. Aktualizacja baz wirusów odbywa się automatycznie, przynajmniej raz dziennie.
2. Po każdej naprawie lub konserwacji urządzenia, przed ponownym podłączeniem do Systemu teleinformatycznego zawartość stałych nośników komputerowych sprawdzana jest za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy antywirusowe.
3. W przypadku, gdy stacje robocze oraz serwery nie są objęte ochroną w czasie rzeczywistym Administrator Systemu, co najmniej raz w tygodniu, dokonuje rutynowej kontroli pod kątem obecności złośliwego oprogramowania, przy czym kontrola może być realizowana:
   1) automatycznie, zgodnie z harmonogramem zdefiniowanym w scentralizowanym systemie zarządzającym lub osobno dla każdego systemu;
   2) ręcznie, centralnie lub osobno dla każdego systemu.

§ 37.

1. W przypadku wykrycia szkodliwego oprogramowania, które wywiera lub może wywrzeć istotny wpływ na bezpieczeństwo informacji w NKB, Administrator Systemu niezwłocznie informuje o tym IOD.
2. Administrator Systemu sporządza w każdym miesiącu raport dotyczący wykrytego szkodliwego oprogramowania i przekazuje go IOD.

§ 38.

Administrator Systemu, we współpracy z IOD, wysyła Użytkownikom regularne informacje na temat zagrożeń związanych z działaniem niepożądanego oprogramowania, zasad korzystania z oprogramowania antywirusowego, itp.

Rozdział 9

Zarządzanie Kopiami zapasowymi i archiwalnymi

§ 39.

1. Kopie zapasowe systemów, aplikacji, baz danych i dokumentów użytkowanych w NKB służą zapewnieniu możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych lub konfiguracji systemów i aplikacji.
2. Kopie zapasowe sporządza się w szczególności:
   1) przed dokonaniem zmiany konfiguracyjnej (na przykład aktualizacji oprogramowania, ustawień systemowych);
   2) po przeprowadzeniu udanej zmiany konfiguracyjnej.

§ 40.

Kopie archiwalne sporządza się w celu utrwalenia istotnych dokumentów, systemów, baz danych i aplikacji, które nie są aktualnie wykorzystywane, a których obowiązek przechowywania wynika z przepisów prawa powszechnie obowiązującego, regulacji wewnętrznych lub których przechowywanie jest uzasadnione potrzebami NKB.

§ 41.

1. Kopie są wykonywane dla systemów, baz danych i aplikacji oraz dokumentów użytkowanych w NKB.
2. Kopie przechowywane są przez okres określony w przepisach prawa powszechnie obowiązującego lub regulacjach wewnętrznych NKB.
3. Za tworzenie Kopii odpowiedzialny jest Administrator Systemu, któremu Właściciel aktywa zlecił wykonanie Kopii.
4. Dla wskazanych dokumentów, systemów, baz danych i aplikacji podlegających tworzeniu Kopii Właściciel aktywa, w porozumieniu z Administratorem Systemu, określa:
   1) strategię tworzenia Kopii uwzględniającą w szczególności: częstotliwość tworzenia Kopii,

rodzaj Kopii (przyrostowa, pełna, różnicowa), liczbę Kopii, miejsce, okres i sposób przechowywania Kopii, rotację nośników;

2) warunki techniczne realizacji procesu zarządzania Kopiami, w tym określenie urządzenia lub oprogramowania do wykonywania Kopii, rodzaj nośnika, sposób wykonywania Kopii (automatyczny, ręczny), okno eksploatacyjne wykonywania Kopii (jeśli ma zastosowanie), sposób weryfikacji poprawności wykonanej Kopii.

5. Użytkownicy mogą zlecać Administratorowi Systemu wykonanie Kopii przetwarzanych przez nich danych (np. Kopii folderów osobistych).
6. Nośniki informacji przeznaczone do wykonywania Kopii powinny być wymienione nie później niż w momencie osiągnięcia 80% zużycia określonego w odniesieniu do czasu przechowywania danych lub ilości dokonanych zapisów zagwarantowanych przez producenta nośnika.
7. Po utworzeniu Kopii automatycznie (jeżeli jest to technicznie możliwe) jest generowany raport o przebiegu wykonania Kopii. Raport podlega weryfikacji przez Administratora Systemu.
8. Miejsce przechowywania Kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska, na takim poziomie na jakim jest zabezpieczony system lub inny element Systemu teleinformatycznego, z którego Kopia zapasowa została wykonana. Kopie zapasowe powinny być ponadto przechowywane poza pomieszczeniami, w których zostały utworzone, w pomieszczeniach na tyle oddalonych, aby zdarzenie lokalne (na przykład pożar, zalanie) nie zniszczyło jednocześnie nośników w obu pomieszczeniach.
9. Regularnie, nie rzadziej niż raz na pół roku, Administrator Systemu w porozumieniu z Właścicielem aktywów przeprowadza testowe sprawdzenie odtworzenia systemów, aplikacji, baz danych lub dokumentów z Kopii. Testowe odtworzenie podlega udokumentowaniu w Dzienniku pracy systemu.

§ 42.

1. W przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z przepisów prawa powszechnie obowiązującego, regulacji wewnętrznych lub innych wymagań w zakresie bezpieczeństwa informacji, dane z nośników są przenoszone na inny nośnik.
2. Kopię na inny nośnik wykonuje Administrator Systemu. Nośnik, z którego przeniesiono zapis, jest niszczony zgodnie z zasadami obowiązującymi w NKB, a całość operacji przeniesienia jest dokumentowana.
3. Kopie archiwalne są niszczone zgodnie z zasadami określonymi w regulacjach wewnętrznych NKB.

§ 43.

1. Usługi transportowania lub przechowywania Kopii zapasowych lub archiwalnych mogą być powierzone Podmiotowi zewnętrznemu na podstawie umowy.
2. Umowa, o której mowa w ust. 1, powinna zawierać co najmniej:
   1) wymagania bezpieczeństwa dotyczące transportu i przechowywania Kopii;
   2) tryb przekazywania i odbioru Kopii:
      a) zwykły (rotacja Kopii zapasowych),
      b) awaryjny (w celu użycia Kopii zapasowej lub archiwalnej);
   3) zasady komunikacji z Podmiotem zewnętrznym, w tym potwierdzania dostarczenia Kopii w trybie awaryjnym;
   4) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie Kopii.

Rozdział 10
Zasady monitorowania systemów i ich użycia

§ 44.

1. Monitorowanie systemów i ich użycia ma na celu w szczególności wykrycie nieuprawnionych działań.
2. Rejestrowane i monitorowane są wszystkie zdarzenia polegające na użyciu środków przetwarzania informacji oraz programów narzędziowych, diagnostycznych, w sposób zapewniający weryfikację i rozliczalność Użytkowników. W szczególności rejestrowaniu podlegają:
   1) identyfikatory Użytkowników;
   2) data, czas i szczegóły istotnych zdarzeń, na przykład zarejestrowania w systemie i wyrejestrowania z niego;
   3) identyfikatory stacji roboczych lub terminali (nazwa komputera w systemie);
   4) dostęp do systemu z uprawnieniami administracyjnymi;
   5) dostęp do konfiguracji systemu, w tym konfiguracji zabezpieczeń;
   6) dostęp do przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;
   7) pomyślne i nieudane próby logowania do systemu;
   8) zmiany zapisów w rejestrach;
   9) zmiany konfiguracji systemu;
   10) informacje o korzystaniu z przywilejów
   11) informacje o korzystaniu z narzędzi systemowych i aplikacji;
   12) używane pliki wraz ze sposobem użycia;
   13) adresy sieciowe i protokoły;
   14) aktywacje i dezaktywacje systemów ochrony (na przykład oprogramowania antywirusowego);
   15) zapisy transakcji dokonywanych przez Użytkowników w aplikacjach;
   16) błędy systemu i procedury obsługi tych błędów;
   17) zawieszenie i ponowne uruchomienia systemu;
   18) uruchamianie programów narzędziowych;
   19) zmiany w plikach konfiguracyjnych i krytycznych zmiennych systemowych;
   20) wersje systemu i stan uaktualnień w porównaniu z zalecanymi przez producenta (jeśli ma zastosowanie).
3. Rejestry są utrzymywane i przechowywane dla wszystkich istotnych systemów i aplikacji.
4. Informacje w rejestrach są przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach prawa powszechnie obowiązującego, a w przypadku braku takich przepisów – przez dwa lata.
5. Systemy rejestrów są objęte standardową procedurą tworzenia Kopii archiwalnych.
6. Serwery kontrolujące dostęp do Internetu tworzą zdalne pliki rejestrów lub mają wdrożony system przesyłania rejestrów zdarzeń na inne, wewnętrzne serwery.
7. Administrator Systemu regularnie monitoruje zapisy dokonywane automatycznie przez systemy w rejestrach zdarzeń pod kątem właściwego wykorzystania Systemu teleinformatycznego i zarządzania nim.
8. Rejestry są zabezpieczone przed nieuprawnionymi zmianami.

§ 45.

1. Administrator Systemu prowadzi Dziennik pracy systemu. Dziennik pracy systemu zawiera zapisy dotyczące w szczególności:
   1) informacji o nadaniu, modyfikacji lub cofnięciu przywilejów w Systemie teleinformatycznym;
   2) przejęcia obowiązków Administratora Systemu;
   3) błędów systemowych i podjętych działań naprawczych;
   4) zdarzeń związanych z bezpieczeństwem informacji;
   5) błędów zgłaszanych przez Użytkowników oraz innych administratorów, a także przez strony trzecie świadczące usługi na rzecz Systemu teleinformatycznego oraz podjętych działaniach naprawczych;
   6) informacji o sesjach połączeń zdalnych wykonywanych przez Podmioty zewnętrzne (jeżeli ma zastosowanie) zawierających:
      a) cel połączenia;

b) opis działań;
c) specyfikację danych i systemów, do których firma serwisowa będzie miała dostęp;
d) nazwisko osoby nawiązującej połączenie ze strony firmy zewnętrznej oraz nazwę firmy;
e) datę i godzinę połączenia;
7) informacji o instalacjach oprogramowania lub zmianach wersji;
8) informacji o użyciach programów narzędziowych;
9) informacji o zmianach konfiguracji sprzętu i systemu operacyjnego.

2. Każdy zapis w Dzienniku pracy systemu zawiera informacje dodatkowe o czynnościach lub zdarzeniu, takie jak:
1) czas rozpoczęcia i zakończenia pracy w Systemie teleinformatycznym;
2) nazwisko osoby wykonującej wpis do Dziennika pracy systemu;
3) identyfikator Konta, z którego wykonano czynności (jeśli ma zastosowanie).

3. Administrator Systemu odnotowuje w Dzienniku pracy systemu wszelkie dodatkowe informacje, które pozwolą zlokalizować przyczynę błędu:
1) w przypadku awarii sprzętu lub usługi, w szczególności:
a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w Dzienniku pracy systemu);
b) objawy towarzyszące (np. komunikaty systemowe, logi połączeń);
c) krytyczność awarii, zgodnie z klasyfikacją uzgodnioną z dostawcą sprzętu lub usługi;
2) w przypadku awarii oprogramowania, w szczególności:
a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w Dzienniku pracy systemu);
b) zrzuty ekranów;
c) konfiguracje oprogramowania i baz danych (np. otwarte pliki, zapisy w rejestrach);
d) krytyczność błędu, zgodnie z klasyfikacją przewidzianą dla danego oprogramowania, w szczególności uzgodnioną z dostawcą oprogramowania.

4. Dla każdego serwera, urządzenia sieciowego, aplikacji mogą być prowadzone oddzielne Dzienniki pracy systemu.
5. Dzienniki pracy systemu lub ich części prowadzone są w formie elektronicznej lub papierowej.
6. Dziennik pracy systemu są zabezpieczone przed nieuprawnionymi zmianami.
7. Rejestracja błędów może być prowadzona poza Dziennikami pracy systemu, w dedykowanym rejestrze.

§ 46.

Administrator Systemu sporządza w każdym miesiącu raport dotyczący wykrytych nieprawidłowości w funkcjonowaniu Systemu teleinformatycznego i przekazuje go IOD.

§ 47.

1. Odpowiednia dokładność i możliwość korelacji rejestrów, o których mowa w § 44, jest zapewniona przez właściwe ustawienie zegarów urządzeń teleinformatycznych.
2. Do synchronizacji czasu wykorzystuje się protokół NTP.
3. Źródłem synchronizacji jest zewnętrzny wzorzec czasu.
4. Stacje robocze synchronizują czas z kontrolerów domen.

Rozdział 11

Monitorowanie pojemności i wydajności Systemów teleinformatycznych

§ 48.

1. Administrator Systemu jest odpowiedzialny za prognozowanie wymagań dotyczących pojemności oraz wydajności kluczowych elementów Systemu teleinformatycznego w celu ograniczenia ryzyka przeciążenia Systemu teleinformatycznego.
2. Wymagania dotyczące pojemności nowych elementów Systemu teleinformatycznego, wynikające z potrzeb NKB, są definiowane i zatwierdzane przed dokonaniem zakupu.
3. Administrator Systemu monitoruje na bieżąco eksploatację Systemu teleinformatycznego w aspekcie krytycznych elementów i parametrów:

1) infrastruktury sieciowej – w zakresie przepustowości i obciążenia łączy (interfejsów) oraz procesorów urządzeń sieciowych;
2) serwerów usług wewnętrznych NKB (serwery plików, wydruków, itp.) – w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie kwartalnym;
3) serwerów aplikacyjnych i baz danych – w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie kwartalnym.

4. Administrator Systemu określa parametry pracy podlegające pomiarom i przeglądom oraz ustala: wartości progów, szczegółowe sposoby i okresy pomiaru.
5. Administrator Systemu podejmuje działania niezbędne do zapewnienia optymalnej pojemności wykorzystywanych elementów Systemu teleinformatycznego, w tym zapewnia:
   1) usuwanie nieaktualnych danych oraz odinstalowanie aplikacji, systemów, baz danych itp.;
   2) optymalizację procesów wsadowych i harmonogramów;
   3) optymalizację logiki aplikacji lub zapytań do bazy danych;
   4) odmowę lub ograniczenie pasma dla usług wymagających wielu zasobów, jeśli nie są one krytyczne dla bieżącej działalności.
6. W sytuacji, w której analiza pojemności lub wydajności systemów wykazuje wzrost ryzyka istotnego zakłócenia działalności NKB, Administrator Systemu niezwłocznie przekazuje te informacje Przewodniczącemu NKB oraz IOD.

Rozdział 12
Ochrona kodu źródłowego

§ 49.

1. Kody źródłowe do programów oraz związanych z nimi elementów (na przykład projekty, specyfikacje, plany weryfikacji i badania poprawności) podlegają ścisłej ochronie.
2. W szczególności stosuje się następujące zabezpieczenia:
   1) tam, gdzie to możliwe, nie należy przechowywać bibliotek programów źródłowych w systemach produkcyjnych;
   2) dostęp do bibliotek programów źródłowych jest ograniczony;
   3) biblioteki programów źródłowych i elementy z nimi związane podlegają aktualizacji;
   4) wydruki programów są przechowywane w bezpiecznym środowisku;
   5) wszystkie zapisy dotyczące dostępu do bibliotek programów źródłowych są przechowywane w Dzienniku pracy systemu;
   6) w przypadku kodu źródłowego przeznaczonego do publikacji stosuje się dodatkowe zabezpieczenia w celu zachowania jego integralności, np. podpis cyfrowy;
   7) zarządzanie kodem źródłowym programu i bibliotekami programów źródłowych, a także kopiowanie i utrzymywanie bibliotek programów źródłowych odbywa się zgodnie z procedurami ustalonymi przez Administratora Systemu.

Rozdział 13
Odbiór elementów Systemu teleinformatycznego

§ 50.

1. Kryteria odbioru nowych elementów Systemu teleinformatycznego obejmują dostarczenie co najmniej:
   1) w przypadku oprogramowania – dokumentacji technicznej oraz instrukcji dla Administratora Systemu i Użytkownika,
   2) w przypadku infrastruktury – dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury.
2. Ponadto, kryteria odbioru obejmują:
   1) wymagania wydajnościowe i pojemnościowe elementu Systemu teleinformatycznego;
   2) dokumenty potwierdzające, że instalacja nowych elementów Systemu teleinformatycznego nie będzie miała negatywnego wpływu na istniejące elementy Systemu teleinformatycznego, szczególnie w chwilach największego obciążenia (jeżeli ma zastosowanie);

3) dokumenty potwierdzające, że wpływ nowych elementów Systemu teleinformatycznego na bezpieczeństwo informacji został uwzględniony;
4) szkolenia z zakresu posługiwania się i działania nowych elementów Systemu teleinformatycznego;
5) w przypadku oprogramowania, odbiór obejmuje dodatkowo elementy określone w ust. 4 lub ust. 5 poniżej.

3. Oprogramowanie aplikacji NKB musi być dostarczane w postaci kodu wykonywalnego.
4. Odbiór oprogramowania obejmuje następujące, główne elementy:
   1) wykonanie instalacji oprogramowania;
   2) dostarczenie przez wykonawcę scenariuszy testów akceptacyjnych;
   3) wykonanie testów oprogramowania zakończone stosownym dokumentem potwierdzającym prawidłowość testów;
   4) odbiór oprogramowania potwierdzony stosownym dokumentem;
   5) odmowa odbioru oprogramowania potwierdzona stosownym dokumentem w przypadku negatywnych wyników testów, o których mowa w pkt 3;
   6) w przypadku wystąpienia jakichkolwiek rozbieżności, co do jakości produktu – przeprowadzenie wewnętrznego lub zewnętrznego audytu.
5. Każdorazowo, wraz ze zmienioną wersją oprogramowania aplikacji NKB, wykonawca dostarcza:
   1) wykaz dokonanych zmian w oprogramowaniu w stosunku do poprzedniej wersji wraz z ich opisem;
   2) aktualizację dokumentacji uwzględniającą zmiany dokonane w oprogramowaniu.

§ 51.

1. Kwestie własności oprogramowania i związanych z nim praw autorskich i praw pokrewnych są określane w umowach zawieranych przez NKB. Jeśli jest to możliwe, NKB powinna być właścicielem praw autorskich zarówno kodu źródłowego, jak i kodu wynikowego.
2. Zapewnienie odpowiedniej pomocy technicznej musi być określane w umowach. Pomoc techniczna ma zapewniać efektywne rozwiązywanie problemów związanych z danym systemem teleinformatycznym lub aplikacją w czasie określonym w umowie.
3. W przypadku podjęcia decyzji o przechowywaniu kodu źródłowego pisanego na zamówienie NKB poza jej siedzibą, konieczne jest również zawarcie umów depozytowych dotyczących takiego kodu źródłowego z podmiotami niezależnymi od dostawcy oprogramowania. Umowy te powinny określać niezależny podmiot, któremu twórca oprogramowania dostarczy kod źródłowy i wszystkie jego aktualizacje. Powinny one też określać sytuacje, w których kod źródłowy zostanie udostępniony NKB, jak na przykład upadłość lub likwidacja dostawcy oprogramowania lub niewywiązywanie się przez niego z postanowień umowy dotyczących aktualizacji oprogramowania.

Rozdział 14

Zarządzanie zmianami w Systemie teleinformatycznym

§ 52.

1. Zarządzanie zmianami w Systemie teleinformatycznym ma na celu zapewnienie poprawnego i bezpiecznego działania tego systemu.
2. Zarządzanie zmianami polega na koordynacji, nadawaniu priorytetów, zatwierdzaniu, planowaniu zasobów i przeprowadzaniu oceny ryzyka w związku ze zmianami dokonywanymi w Systemie teleinformatycznym.
3. Zmiany powinny być dokonywane jedynie w niezbędnym zakresie oraz ściśle nadzorowane.
4. Każda zmiana w Systemie teleinformatycznym musi być udokumentowana.
5. Zasady wskazane w niniejszym paragrafie odnoszą się do:
   1) zmian infrastruktury technicznej elementów Systemu teleinformatycznego, sprowadzających się do wprowadzenia nowego elementu infrastruktury, zmodyfikowania lub usunięcia istniejącego elementu infrastruktury, poprawiania błędu w infrastrukturze, przy czym:
      a) zmiana infrastruktury regularna – oznacza zmianę, która nie wymaga natychmiastowego

wdrożenia;

b) zmiana infrastruktury awaryjna – stosowana w sytuacjach awaryjnych, gdzie czas implementacji zmiany jest krytyczny z punktu widzenia realizacji zadań NKB, w tym ciągłości jej działania, dokonywana z pominięciem lub uproszczeniem niektórych etapów (np. testów);

2) zmian aplikacyjnych będących poprawkami (w tym usuwanie błędów) albo modyfikacjami, przy czym:

a) zmiany aplikacyjne regularne – oznaczają zmiany, które nie wymagają natychmiastowego wdrożenia;

b) zmiany aplikacyjne awaryjne – wprowadzane w stanie pilnej konieczności z powodu zagrożenia działania danej aplikacji;

3) zmian w sposobie lub zakresie świadczenia usług przez Podmiot zewnętrzny.

6. Za proces zarządzania zmianami w poszczególnych obszarach jest odpowiedzialny Właściciel aktywów, zaś za ich realizację Administrator Systemu, chyba że co innego wynika z charakteru wprowadzanej zmiany.
7. Każda zmiana regularna jest poprzedzona udokumentowanym:
   1) opisem zmiany;
   2) opisem przyczyny zmiany (wraz z podaniem przepisów prawa powszechnie obowiązującego uzasadniających zmianę – jeżeli ma zastosowanie);
   3) opisem rodzaju wymaganych działań;
   4) przeprowadzeniem oceny ryzyka związanego z wprowadzeniem zmiany;
   5) harmonogramem wprowadzanych zmian;
   6) opracowaniem procedury wyjścia ze zmiany, opisującej sposób przywrócenia systemu do stanu sprzed zmiany;
   7) wykonaniem Kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń (jeżeli ma zastosowanie);
   8) przetestowaniem zmian.
8. Czynności, o których mowa w ust. 7 dokonuje Właściciel aktywów w porozumieniu z Administratorem Systemu.
9. W przypadku braku możliwości przetestowania zmian, Administrator Systemu informuje Właściciela aktywa o potencjalnych konsekwencjach niepowodzenia wdrożenia zmiany.
10. Przed każdą dokonywaną zmianą Administrator Systemu, w porozumieniu z IOD dokonuje analizy czy zmiana ma wpływ na treść istniejącej dokumentacji bezpieczeństwa informacji oraz w razie potrzeby, dokonuje jej aktualizacji.
11. Jeżeli zmiana ma charakter awaryjny, dokumentacja, o której mowa w ust. 7 może być opracowana najpóźniej w przeciągu 7 dni od dokonania zmiany.
12. Zmiana mająca charakter awaryjny, którą trzeba wprowadzić niezwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności NKB wymaga zgody Właściciela aktywa.
13. Dokonywane zmiany podlegają rejestracji w Dzienniku pracy systemu.
14. Po dokonaniu zmian w platformach produkcyjnych Administrator Systemu przeprowadza przegląd krytycznych aplikacji biznesowych oraz testuje je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.
15. W przypadku zmian w oprogramowaniu dostarczanym przez Podmiot zewnętrzny należy uwzględnić ewentualną konieczność pozyskania odpowiednich zgód na wprowadzenie zmian.

§ 53.

1. Transakcje używane dla celów kontrolnych, testowych, szkoleniowych lub innych celów nieprodukcyjnych, muszą być odseparowane od transakcji używanych w środowisku produkcyjnym.
2. Za każdym razem, kiedy działanie oprogramowania opracowanego w NKB nie zakończy się w oczekiwany sposób, Użytkownik powinien w widoczny sposób zostać poinformowany o wystąpieniu błędu.

3. Narzędzia i programy służące do testowania mogą być używane wyłącznie przez upoważnionych Członków NKB dla celów testowych lub rozwojowych.
4. Środowisko produkcyjne powinno być odseparowane od środowiska testowego i programistycznego. Jeśli nie jest to możliwe, musi być zapewnione pełne rozdzielenie zasobów sprzętowych i dyskowych lub zagwarantowana minimalna dostępność zasobów niezbędnych do funkcjonowania środowiska produkcyjnego.
5. Wprowadzanie zmian bezpośrednio do środowiska produkcyjnego może być wykonane wyłącznie po uzyskaniu akceptacji Właściciela aktywa. Wprowadzanie poprawek podlega dokumentowaniu w Dzienniku pracy systemu.
6. Poziom uprawnień do modyfikacji danych i systemu osób pracujących w środowiskach produkcyjnym, testowym i programistycznym musi być zróżnicowany. Najszersze uprawnienia mogą posiadać osoby pracujące w środowisku programistycznym. Uprawnienia w środowiskach testowym i produkcyjnym muszą być ściśle ograniczone.
7. Członkowie NKB zajmujący się opracowywaniem oprogramowania wykorzystywanego do prowadzenia działalności operacyjnej nie mogą mieć dostępu do informacji użytkowanych w środowisku produkcyjnym, z wyjątkiem informacji niezbędnych do prawidłowego opracowania oprogramowania oraz sytuacji awaryjnych, w zakresie do tego niezbędnym. Dostępem do Kont awaryjnych zarządza Administrator Systemu.
8. Testy akceptacyjne nowych lub zmodyfikowanych aplikacji nie mogą być przeprowadzane przez osoby zajmujące się opracowywaniem programów.
9. Wszystkie opracowywane aplikacje muszą być ulokowane na przeznaczonych do tego celu serwerach, nie na stacjach roboczych.
10. W trakcie prac rozwojowych należy testować funkcje bezpieczeństwa.

§ 54.

Po wprowadzeniu zmiany należy poinformować wszystkich odbiorców systemu lub aplikacji, w których dokonano zmian funkcjonalnych, zmieniających sposób użytkowania systemu lub aplikacji

§ 55.

1. Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna systemów podlegają ochronie, zgodnie z Procedurą klasyfikowania informacji oraz postępowania z określonymi grupami informacji w NKB.
2. Osobą odpowiedzialną za aktualność i kompletność dokumentacji jest Administrator Systemu.
3. Dokumentacja systemów jest udostępniana na zasadzie wiedzy koniecznej. Udostępnienie dokumentacji jest rejestrowane.

§ 56.

1. Administrator Systemu zobowiązany jest do monitorowania pojawiania się poprawek do poszczególnych usług sieciowych, systemów operacyjnych i aplikacji NKB.
2. Administrator Systemu obowiązany jest do wprowadzania poprawek w oparciu informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych i aplikacji, oraz od profesjonalnych podmiotów zajmujących się tematyką bezpieczeństwa informacji i systemów teleinformatycznych.

§ 57.

1. Administrator Systemu odpowiada za okresową aktualizację oprogramowania (np. oprogramowanie systemowe, aplikacyjne, bazodanowe).
2. O ile jest to technicznie możliwe, aktualizacja powinna być przeprowadzana automatycznie i na bieżąco.
3. Oprogramowanie obsługiwane na podstawie umów serwisowych powinno być aktualizowane zgodnie z postanowieniami tych umów.
4. Po wprowadzeniu aktualizacji należy monitorować stabilność oprogramowania. W przypadku uzasadnionych wątpliwości co do poprawności funkcjonowania oprogramowania po aktualizacji,

Administrator Systemu może podjąć decyzję o rezygnacji z aktualizacji, oraz o zgłoszeniu tego faktu dostawcy oprogramowania, odnotowując to w dokumentacji oprogramowania wraz z uzasadnieniem.

Rozdział 15

Konserwacja i naprawy sprzętu komputerowego lub innych urządzeń

§ 58.

1. Konserwacja sprzętu komputerowego lub innych urządzeń stanowiących element Systemu teleinformatycznego ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tego systemu, zapobieganie utracie, uszkodzeniu lub naruszeniu bezpieczeństwa.
2. Sprzęt komputerowy i inne urządzenia podlegają konserwacji zgodnie z zaleceniami producentów.
3. Konserwacja i naprawy mogą być prowadzone jedynie przez uprawnionych Członków NKB lub Podmioty zewnętrze świadczące odpowiednie usługi na podstawie umowy lub w ramach rękojmi lub gwarancji.
4. W przypadku, gdy na nośnikach, stanowiących integralną część sprzętu komputerowego lub innych urządzeń przekazywanych do naprawy lub konserwacji, znajdują się informacje podlegające ochronie, sprzęt lub urządzenia naprawiane są pod nadzorem Administratora Systemu. W przypadku gdy taki nadzór nie jest możliwy, informacje podlegające ochronie są, po zapewnieniu możliwości ich odtworzenia, skutecznie usuwane z nośnika.
5. W przypadku gdy informacje, o których mowa w ust. 4, są przechowywane na nośnikach nie stanowiących integralnej części sprzętu komputerowego lub innego urządzenia, nośnik należy wymontować i na czas naprawy lub konserwacji przechowywać w sposób odpowiedni do rodzaju informacji przechowywanych na nośniku.
6. Wszelkie konserwacje i naprawy są odnotowywane w dzienniku pracy danego sprzętu komputerowego lub innego urządzenia.

Rozdział 16

Instalacja i ochrona okablowania

§ 59.

1. W NKB przyjęto następujące zasady instalacji i ochrony okablowania:
   1) sposób instalacji okablowania uwzględnia ochronę okablowania przed nieautoryzowanym dostępem lub uszkodzeniem, w szczególności poprzez prowadzenie kabli w rurach kablowych, listwach PCV, podłogach technologicznych;
   2) okablowanie, w miarę możliwości, nie jest prowadzone przez ogólnie dostępne strefy; w przypadku prowadzenia okablowania przez takie miejsca stosowane są środki uniemożliwiające bądź ograniczające dostęp do okablowania przez osoby nieupoważnione;
   3) przy projektowaniu przebiegu linii sieci teleinformatycznej poza strefami administracyjnymi wykorzystywane są w maksymalnym stopniu rozwiązania wykorzystujące technologie światłowodowe;
   4) w instalacji okablowania oddzielono kable zasilające od okablowania komunikacyjnego w celu unikania zakłóceń;
   5) w instalacji okablowania zastosowano jednoznaczne i wyraźne oznakowanie umożliwiające identyfikację kabli i sprzętu w celu zmniejszenia ryzyka takich błędów, jak niewłaściwe połączenie lub zastosowanie nieodpowiedniego kabla;
   6) kable komunikacyjne wyposażone są w zabezpieczenia odgromowe;
   7) prowadzi się kompletną i aktualną dokumentację połączeń fizycznych i logicznych w celu zmniejszenia prawdopodobieństwa błędów.
2. Pomieszczenia, w których znajdują się panele połączeniowe, węzły telekomunikacyjne i szafy dystrybucyjne objęte są systemem kontroli dostępu.
3. Niewykorzystywane segmenty sieci strukturalnej są odłączane od sieci teleinformatycznej.
4. W przypadku systemów wskazanych w procesie szacowania ryzyka jako kluczowe, stosuje się dodatkowe zabezpieczenia obejmujące:

1) stosowanie zapasowych (awaryjnych) dróg komunikacyjnych lub mediów transmisyjnych zapewniających odpowiedni poziom bezpieczeństwa;
2) korzystanie z kabli światłowodowych.

5. Badanie właściwości transmisyjnych okablowania strukturalnego przeprowadzane jest przez Administratora Systemu nie rzadziej niż raz na 2 lata.

Rozdział 17

Eksploatacja urządzeń zasilających

§ 60.

1. Wszystkie urządzenia Systemu teleinformatycznego są zasilane napięciem o parametrach zgodnych z wymaganiami producenta.
2. Urządzenia, o których mowa w ust. 1, zasilane są z wydzielonej instalacji elektrycznej.
3. Urządzenia, o których mowa w ust. 1, od których ciągłości pracy zależne jest realizowanie podstawowych zadań NKB, zasilane są z gwarantowanych źródeł.
4. Gwarantowane zasilanie uzyskiwane jest przez zastosowanie dywersyfikacji zewnętrznych źródeł energii elektrycznej z samoczynnym załączaniem rezerwy (SZR), zastosowanie zasilaczy bezprzerwowych (UPS) lub zastosowanie awaryjnych agregatów prądotwórczych.
5. Dobór urządzeń podtrzymujących zasilanie pod względem wydajności mocowej poprzedzane jest przeprowadzeniem udokumentowanego bilansu mocy.
6. Każde urządzenie sieci teleinformatycznej jest opatrzone tabliczką, z której wynika skąd dane urządzenie jest zasilane, zawierającą nazwę rozdzielnicy lub tablicy zabezpieczeń oraz nazwę pola w rozdzielnicy lub bezpiecznika na tablicy zabezpieczeń.
7. Stan zasilania zasobów sieci teleinformatycznej, którym nadano status zasobu kluczowego, jest na bieżąco monitorowany przez Administratora Systemu. Jakość zasilania pozostałych zasobów sieci teleinformatycznej wymaga okresowego sprawdzania, nie rzadziej niż raz na rok.
8. Zasilacze bezprzerwowe, zasilające kluczowe zasoby sieci teleinformatycznej, raportują stan swojej pracy (zasilanie z sieci, zasilanie z baterii) oraz parametry baterii (jej stopień naładowania i przewidziany czas pracy z baterii przy danym obciążeniu) systemom operacyjnym serwerów. W przypadku, gdy stopień naładowania baterii osiągnie w czasie pracy z baterii poziom, którego przekroczenie nie gwarantuje podtrzymania ciągłości pracy, system operacyjny wymusza automatyczne zamknięcie aplikacji i baz danych oraz kontrolowane wyłączenie serwera.
9. W przypadku, gdy automatyczne raportowanie nie jest technicznie możliwe Administrator Systemu dokonuje okresowych, nie rzadziej niż raz na tydzień, oględzin polegających na sprawdzeniu wskazań paneli sterujących (według instrukcji techniczno-eksploatacyjnych). Oględziny muszą być odnotowywane w Dzienniku pracy systemu.
10. Elementy systemu zasilania gwarantowanego podlegają okresowym przeglądom i konserwacjom w zakresie określonym przez producenta.
11. Akumulatory podlegają wymianie po okresach eksploatacji przewidzianych w instrukcjach użytkowania.
12. Serwisowanie urządzeń zasilających przeprowadzane jest wyłącznie przez autoryzowane Podmioty zewnętrzne.
13. Przeglądy, konserwacje i serwisowanie podlegają odnotowaniu w Dzienniku pracy systemu.

Rozdział 18

Kontrola licencjonowanego oprogramowania

§ 61.

1. Dla wszystkich systemów i aplikacji użytkowanych w NKB Administrator Systemu prowadzi wykaz licencjonowanego oprogramowania zawierający:
   1) informacje o oprogramowaniu;
   2) informacje o licencjach wraz z okresami ich ważności;
2. Dodatkowo, w wykazie zamieszcza się informacje o wykorzystywanym oprogramowaniu bezpłatnym, ze wskazaniem informacji o oprogramowaniu oraz podstawy dopuszczenia

do użytkowania.

3. Administrator Systemu na bieżąco monitoruje i aktualizuje wykaz.
4. IOD nadzoruje poprawność i kompletność wykazu, o którym mowa w ust. 1.
5. Wzór wykazu oprogramowania określa Załącznik nr 3 do Polityki.

§ 62.

1. Weryfikacja licencjonowanego oprogramowania jest przeprowadzana okresowo oraz doraźnie.
2. Okresowo, nie rzadziej niż raz w roku, Administrator Systemu weryfikuje stacje robocze i udostępnione udziały sieciowe Użytkowników pod kątem obecności nieautoryzowanego oprogramowania.
3. Weryfikacja doraźna jest dokonywana:
   1) w przypadku otrzymania informacji o naruszeniu lub podejrzeniu naruszenia przepisów prawa powszechnie obowiązującego, regulacji wewnętrznych, obowiązków umownych lub innych zasad dotyczących korzystania z oprogramowania;
   2) na wniosek Przewodniczącego NKB, Właściciela aktywa, IOD lub uprawnionych organów publicznych;
   3) w przypadku otrzymania zgłoszenia od Członka NKB o pojawieniu się lub podejrzeniu pojawienia się w Systemie teleinformatycznym nieautoryzowanego oprogramowania.
4. Do przeprowadzenia weryfikacji zgodności zainstalowanego oprogramowania z posiadanymi licencjami, a także zgodności z konfiguracją standardową, Administrator Systemu może stosować narzędzia programowe umożliwiające w szczególności:
   1) automatyczne sprawdzanie stacji roboczych i serwerów;
   2) centralne zarządzanie spisem licencjonowanego oprogramowania;
   3) automatyczne ostrzeganie przed przekroczeniem liczby licencji.
5. W przypadku wykrycia nieautoryzowanego oprogramowania Administrator Systemu niezwłocznie:
   1) o ile to możliwe, zabezpiecza dowody istnienia nieautoryzowanego oprogramowania;
   2) usuwa oprogramowanie z Systemu teleinformatycznego;
   3) przekazuje informacje o zdarzeniu IOD wraz z rekomendacją podjęcia odpowiednich działań.

Rozdział 19

Przeglądy Systemu teleinformatycznego

§ 63.

1. Administrator Systemu odpowiada za planowanie i przeprowadzenie okresowych przeglądów Systemu teleinformatycznego w celu weryfikacji prawidłowości jego funkcjonowania oraz spełniania przez niego wymogów i celów bezpieczeństwa.
2. Przeglądy powinny być przeprowadzane w taki sposób, aby wywierały jak najmniejszy wpływ na bieżącą działalność NKB oraz na ciągłość działania Systemu teleinformatycznego.
3. Dla każdego przeglądu jest opracowywany plan, zawierający co najmniej:
   1) określenie typu przeglądu, na przykład:
      a) przegląd uprawnień,
      b) przegląd dokumentacji,
      c) testy penetracyjne (wewnętrzne lub zewnętrzne), testy Podatności technicznych,
      d) przegląd legalności oprogramowania;
   2) termin przeglądu;
   3) zakres przeglądu;
   4) osoby przeprowadzające przegląd.
4. W przypadku testów, o których mowa w ust. 3 pkt 1 lit c należy podjąć odpowiednie środki ostrożności w celu uniknięcia naruszenia bezpieczeństwa Systemu teleinformatycznego.
5. Każdy z typów przeglądów określonych w ust. 3 pkt 1 powinien być przeprowadzony co najmniej raz w roku.
6. Raport z przeglądu jest przekazywany Przewodniczącemu NKB.
7. W szczególnie uzasadnionych przypadkach Administrator Systemu, za zgodą Przewodniczącego

NKB może przeprowadzić pozaplanowy przegląd.

Rozdział 20
Szkolenia

§ 64.

1. Szkolenia Użytkowników Systemu teleinformatycznego mają na celu uzyskanie przez nich odpowiedniego poziomu wiedzy i umiejętności, które pozwolą właściwie użytkować i chronić System teleinformatyczny NKB i jego elementy.
2. Szkolenia, o których mowa w ust. 1, prowadzi się na zasadach określonych w Polityce bezpieczeństwa informacji, zaś ich tematyka obejmuje w szczególności:
   1) przygotowanie Użytkowników do właściwego korzystania z powierzonych Aktywów (instrukcje użytkowania sprzętu, systemów operacyjnych, aplikacji, itp.);
   2) sposoby postępowania w przypadku zdarzenia związanego z naruszeniem bezpieczeństwa informacji;
   3) sposoby postępowania w sytuacjach awaryjnych i kryzysowych.
3. Warunkiem uzyskania podstawowego dostępu do Systemu teleinformatycznego (Konto domenowe i Konto pocztowe) przez Członka NKB jest odbycie szkolenia wstępnego przeprowadzanego przez Administratora Systemu.

Rozdział 21
Postanowienia końcowe

§ 65.

1. Nie rzadziej niż raz w roku Administrator Systemu opracowuje i przekazuje Przewodniczącemu NKB raport z funkcjonowania Systemu teleinformatycznego. Szczegółowy termin przekazania raportu określa Administrator Systemu.
2. Raport uwzględnia w szczególności:
   1) informacje o wykrytych nieprawidłowościach, błędach lub innych zdarzeniach, które mają lub mogą mieć wpływ na bezpieczeństwo informacji;
   2) informacje o działaniach podjętych w celu zapewnienia lub zwiększenia bezpieczeństwa Systemu teleinformatycznego i jego elementów w NKB;
   3) rekomendacje dotyczące usprawnień organizacyjnych, mających na celu zwiększenie bezpieczeństwa Systemu teleinformatycznego i jego elementów w NKB.

§ 66.

Szczegółowe zasady postępowania z Urządzeniami przenośnymi określa Instrukcja użytkowania urządzeń przenośnych, stanowiąca Załącznik nr 4 do Polityki.

§ 67.

Integralną część Polityki stanowią załączniki:

1) Załącznik nr 1 – Wniosek o nadanie lub odebranie dostępu do systemu teleinformatycznego;
2) Załącznik nr 2 – Regulamin użytkownika systemu teleinformatycznego;
3) Załącznik nr 3 – Wzór wykazu oprogramowania;
4) Załącznik nr 4 – Instrukcja użytkowania urządzeń przenośnych.

Załącznik nr 1
do Polityki bezpieczeństwa teleinformatycznego
w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

.....
Data sporządzenia wniosku

Wniosek

☐ **w sprawie dostępu do konta użytkownika komputera NKB** *(konto użytkownika NKB, logowanie do komputera)*

☐ **w sprawie dostępu do konta pocztowego @nkb.gov.pl** *(adres email, grupa dystrybucyjna/skrzynka funkcyjna)*

☐ **w sprawie dostępu do sieciowego zasobu danych** *(np. dysk .....:, itp.)*

☐ **w sprawie dostępu do systemów** *(np. CMS i inne)*

☐ **o przedłużenie ważności posiadanych uprawnień** *(dla zmiany okresu umowy lub innego stosunku prawnego wypełnić tylko Część I pkt 2a)*

Część I *(wypełnia Wnioskodawca)*

Wybierz element.

1. **Dane osoby, której dotyczy wniosek:**

a) Imię i nazwisko: .....
Stanowisko/ funkcja:
.....
Rodzaj umowy lub innego stosunku prawnego: ....., okres trwania od:
..... do.....

b) **NADANIE** uprawnień dostępu do zasobów/systemów *(odpowiednie zaznaczyć lub podać)*
Nazwa dostępu, zasobu lub systemu:
☐ konto komputerowe ☐ adres email
☐ e-mail grupy dystrybucyjnej/skrzynki funkcyjnej.....
☐ EZD z uprawnieniami: ☐ członek NKB, ☐ kancelaria, ☐ archiwum, ☐ podpis elektroniczny
☐ Inne.....
Zarządzanie treścią stron www (CMS):
☐ NKB.gov.pl ☐ bip.NKB.gov.pl ☐ Inne strony.....
Zasoby dyskowe:
☐ dostęp do odczytu.....
☐ dostęp do odczytu i zapisu .....

c) **ODEBRANIE** uprawnień dostępu do zasobów/systemów *(odpowiednie zaznaczyć lub podać)*
Nazwa dostępu, zasobu lub systemu:
☐ konto komputerowe ☐ adres email
☐ e-mail grupy dystrybucyjnej/skrzynki funkcyjnej .....
☐ EZD z uprawnieniami: ☐ członek NKB, ☐ kancelaria, ☐ archiwum, ☐ podpis elektroniczny

☐ Inne .....
Zarządzanie treścią stron www (CMS):
☐ nkb.gov.pl ☐ bip.nkb.gov.pl
☐ Inne strony.....
☐ Zasoby dyskowe .....

.....
data i podpis Przewodniczącego NKB)

Zatwierdzam:

.....

data i podpis Przewodniczącego NKB

Część II (wypełnia pracownik Działu Kadr i Płac ABM)

Powyższe potwierdzam pod względem poprawności danych osobowych, rodzaju umowy, stanowiska/ funkcji i okresu umowy lub innego stosunku prawnego.

.....

Data i podpis

Część III (wypełnia pracownik Działu IT ABM)

Potwierdzam wykonanie.

.....

Data i podpis

Załącznik nr 2
do Polityki bezpieczeństwa teleinformatycznego
w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Regulamin użytkownika Systemu teleinformatycznego w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Obowiązuje od:	**18.07.2023 r.**
Wersja:	**1.0**

Spis treści

Rozdział 1

Postanowienia ogólne

§ 1.

1. Regulamin użytkownika Systemu teleinformatycznego w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych (dalej: Regulamin) określa podstawowe zasady korzystania przez Użytkowników z Systemu teleinformatycznego w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych (dalej: NKB) .
2. Do przestrzegania postanowień Regulaminu zobowiązani są wszyscy Członkowie NKB, a także wszelkie inne osoby, które w ramach wykonywanych zadań mają dostęp do Systemu teleinformatycznego.
3. Regulamin, choć jego przestrzeganie jest obowiązkowe, nie zwalnia Użytkowników z obowiązku zapoznania się i stosowania pozostałych regulacji wewnętrznych NKB odnoszących się do zasad bezpieczeństwa informacji oraz korzystania z Systemu teleinformatycznego, w szczególności Polityki bezpieczeństwa informacji, Polityki ochrony danych osobowych oraz Instrukcji użytkowania urządzeń przenośnych.
4. Ilekroć w Regulaminie jest mowa o Członkach NKB, jego postanowienia stosuje się odpowiednio do innych Użytkowników.

§ 2.

1. Definicje użyte w Regulaminie oznaczają:
   1) ABM – Agencja Badań Medycznych;
   2) Administrator Systemu – pracownik lub komórka organizacyjna ABM, Członek NKB, któremu powierzono nadzór nad Systemem teleinformatycznym;
   3) Aktywa – wszystko co ma wartość dla NKB. Aktywa dzielą się na informacje, dane oraz tzw. Aktywa wspierające (w szczególności sprzęt, budynki i pomieszczenia, oprogramowanie, zasoby ludzkie);
   4) Członek NKB –Przewodniczący NKB lub inny członek NKB;
   5) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi;
   6) Informacja podlegająca ochronie – informacja podlegająca ochronie na podstawie przepisów prawa powszechnie obowiązującego (na przykład dane osobowe, tajemnica przedsiębiorstwa) lub regulacji wewnętrznych NKB (na przykład informacje chronione w rozumieniu Procedury klasyfikowania informacji oraz postępowania z określonymi grupami informacji);
   7) IOD - Inspektor Ochrony Danych;
   8) Konto – część Systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), która jest przypisana do identyfikatora Użytkownika;
   9) Nośnik danych – urządzenie wymienne i przenośne umożliwiające zapis, modyfikację lub odczyt danych, takie jak: pendrive, dysk przenośny, dysk wewnętrzny, karta pamięci, taśma magnetyczna, nośnik optyczny itp.;
   10) Przewodniczący NKB – Przewodniczący NKB, Zastępca Przewodniczącego NKB lub osoba przez niego upoważniona;
   11) System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. System teleinformatyczny obejmuje między innymi sprzęt komputerowy, urządzenia przenośne, oprogramowanie systemowe, systemy (podsystemy), sieć, aplikacje;
   12) Urządzenie przenośne – informatyczne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie lub wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią, takie jak laptop, smartfon, tablet lub Nośnik danych;
   13) Użytkownik - Członek NKB lub inna osoba realizująca zadania na rzecz NKB na podstawie umowy lub innego stosunku prawnego, która w związku z realizacją tych zadań przetwarza informacje.

2. W braku odmiennych definicji, określenia użyte w Regulaminie mają znaczenie nadane im w Polityce bezpieczeństwa teleinformatycznego.

§ 3.

1. Użytkownicy są zobowiązani w szczególności do:
   1) przestrzegania postanowień Regulaminu;
   2) stosowania się do zaleceń Administratora Systemu, oraz IOD, dotyczących korzystania z Systemu teleinformatycznego;
   3) informowania Administratora Systemu oraz IOD o wszelkich (rzeczywistych lub potencjalnych) przypadkach naruszenia postanowień Regulaminu lub innych zasad użytkowania Systemu teleinformatycznego, w trybie określonym we właściwych regulacjach wewnętrznych NKB.
2. W przypadku wątpliwości odnośnie do stosowania postanowień Regulaminu Użytkownik może zwrócić się z pytaniem do Administratora Systemu, na adres: it@abm.gov.pl.
3. W przypadku gdy pytanie, o którym mowa w ust. 2, dotyczy zagadnień pozostających we właściwości innej upoważnionej osoby (na przykład IOD), Administrator Systemu przekazuje zgłoszenie do tej osoby.

Rozdział 2
Standard wyposażenia stanowiska Użytkownika

§ 4.

1. Stanowisko komputerowe Użytkownika jest wyposażone w sposób umożliwiający prawidłową realizację powierzonych mu zadań.
2. Standardowe wyposażenie stanowiska komputerowego, w przypadku komputera stacjonarnego, obejmuje:
   1) monitor LCD;
   2) komputer o konfiguracji sprzętowej niezbędnej do prowadzenia prac biurowych (system operacyjny, pakiet narzędzi biurowych, zabezpieczenia antywirusowe);
   3) klawiaturę;
   4) mysz;
   5) drukarkę lub dostęp do drukarki sieciowej.
3. Standardowe wyposażenie stanowiska komputerowego, w przypadku komputera przenośnego, obejmuje:
   1) komputer przenośny typu laptop o konfiguracji sprzętowej niezbędnej do prowadzenia prac biurowych (system operacyjny, pakiet narzędzi biurowych, zabezpieczenia antywirusowe);
   2) monitor LCD;
   3) zasilacz;
   4) klawiaturę;
   5) mysz;
   6) drukarkę lub dostęp do drukarki sieciowej.
4. W uzasadnionych przypadkach, wynikających z potrzeby realizacji zadań przez danego Użytkownika, Administrator Systemu może zastosować inną konfigurację komputera Użytkownika lub typ komputera.
5. Administrator Systemu prowadzi ewidencję sprzętu komputerowego.

Rozdział 3
Ogólne zasady korzystania z Systemu teleinformatycznego

§ 5.

1. Użytkownik może korzystać z udostępnionych mu Aktywów stanowiących element Systemu teleinformatycznego wyłącznie do wykonywania zadań służbowych.
2. Wykorzystywanie Aktywów stanowiących element Systemu teleinformatycznego, będących własnością NKB, w celach niezwiązanych z powierzonymi obowiązkami, jest dopuszczalne wyłącznie w szczególnie uzasadnionych przypadkach i wymaga zgody Przewodniczącego NKB

oraz Administratora Systemu.

3. Zabrania się podłączania do sieci teleinformatycznej jakichkolwiek urządzeń niebędących własnością NKB.
4. Użytkownik ponosi odpowiedzialność za powierzone Aktywa oraz sposób korzystania z nich.

§ 6.

Użytkownicy mogą korzystać wyłącznie z przydzielonych im stanowisk komputerowych. Korzystanie z innego stanowiska komputerowego dopuszczalne jest jedynie za zgodą bezpośredniego przełożonego lub w przypadkach określonych w odrębnych regulacjach wewnętrznych NKB (na przykład w planach ciągłości działania).

§ 7.

1. Użytkowników obowiązuje zakaz testowania lub podejmowania prób poznania metod zabezpieczenia Systemu teleinformatycznego.
2. Użytkownicy nie mogą samodzielnie dokonywać jakiejkolwiek zmiany konfiguracji Systemu teleinformatycznego.

Rozdział 4
Uprawnienia dostępu dla Użytkowników

§ 8.

1. Przydzielanie uprawnień do korzystania z Systemu teleinformatycznego realizowane jest w szczególności w oparciu o zasady:
   1) przywilejów koniecznych – prawa dostępu są ograniczone wyłącznie do takich informacji, które są niezbędne do realizacji powierzonych obowiązków;
   2) wiedzy koniecznej – Użytkownicy posiadają wiedzę o informacjach ograniczoną do zagadnień, które są konieczne do realizacji powierzonych obowiązków;
   3) domniemanej odmowy – wszystkie działania, które nie są dozwolone należy co do zasady uznać za zabronione.
2. Każdy Użytkownik otrzymuje dostęp wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań.
3. Dostęp jest przydzielany po nadaniu Użytkownikowi unikalnego identyfikatora i Hasła dostępu lub innych danych uwierzytelniających Użytkownika.
4. Przed uzyskaniem dostępu do Systemu teleinformatycznego NKB, Użytkownik jest informowany przez bezpośredniego przełożonego o zakresie przyznawanych mu uprawnień.
5. Jeżeli w trakcie korzystania z zasobów Systemu teleinformatycznego Użytkownik stwierdzi, że posiadane uprawnienia wykraczają poza przyznane lub że zostały przyznane mu uprawnienia naruszające zasady określone w ust. 1 pkt 1, zobowiązany jest niezwłocznie zgłosić ten fakt Administratorowi Systemu. Niedokonanie zgłoszenia może zostać potraktowane jako świadome lub celowe naruszenie uprawnień dostępu.
6. W przypadku określonym w ust. 5 zabronione jest testowanie lub wykorzystywanie nadmiarowych uprawnień.

§ 9.

1. Użytkownik powinien zabezpieczyć opracowywane przez siebie dane przed utratą i nieautoryzowanym użyciem bądź modyfikacją, w szczególności poprzez umieszczenie danych na serwerze plików (fileserver).
2. Niedopuszczalne jest umieszczanie na serwerze plików danych niezwiązanych z wykonywanymi obowiązkami służbowymi.
3. Zabronione jest:
   1) umożliwianie dostępu do Systemu teleinformatycznego osobom nieupoważnionym;
   2) rejestrowanie się w Systemie teleinformatycznym identyfikatorem innego Użytkownika;
   3) korzystanie z Konta innego Użytkownika;
   4) przenoszenie danych uzyskanych w związku z wykonywanymi zadaniami służbowymi

na prywatne Nośniki danych, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne;
5) podejmowanie prób sprawdzania, testowania i omijania zabezpieczeń Systemu teleinformatycznego;
6) nieuprawnione udzielanie informacji o zasadach ochrony Systemu teleinformatycznego NKB, w tym o identyfikatorach używanych w tym systemie;
7) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w Systemie teleinformatycznym;
8) nieuprawnione niszczenie danych gromadzonych w Systemie teleinformatycznym;
9) świadome wprowadzanie błędnych danych do Systemu teleinformatycznego;
10) udostępnianie danych osobom nieupoważnionym;
11) podłączanie urządzeń elektrycznych do wydzielonej instalacji elektrycznej przeznaczonej dla Systemu teleinformatycznego;
12) przeglądanie stron internetowych o treściach sprzecznych z przepisami prawa powszechnie obowiązującego lub regulacjami wewnętrznymi NKB, w tym zawierających treści sprzeczne z dobrymi obyczajami;
13) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego oprogramowania;
14) korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, niemających związku z wykonywaną pracą.

Rozdział 5

Korzystanie z poczty elektronicznej

§ 10.

1. Poczta elektroniczna stanowi podstawowe narzędzie komunikacji w ramach realizacji obowiązków służbowych.
2. Dostęp do wewnętrznej poczty elektronicznej mają wszyscy Członkowie NKB oraz inne osoby powiązane z NKB, których dostęp do poczty jest niezbędny do prawidłowej realizacji zadań.
3. Każdy Użytkownik poczty elektronicznej jest zobowiązany odczytywać wiadomości kierowane na jego Konto.
4. Informowanie Członków NKB za pomocą wiadomości elektronicznych wysyłanych na ich adresy poczty elektronicznej stanowi jeden z przyjętych przez NKB trybów ogłaszania aktów wewnętrznych, obowiązujących w NKB.
5. Użytkownik poczty elektronicznej ponosi odpowiedzialność za treść i zawartość wysyłanych przez siebie wiadomości.
6. Poczta elektroniczna służy wyłącznie do celów służbowych.

§ 11.

1. Użytkownik poczty elektronicznej otrzymuje dostęp do indywidualnego Konta pocztowego o nazwie x.y@nkb.gov.pl, gdzie „x" jest imieniem Użytkownika, a „y" jego nazwiskiem, z pominięciem polskich znaków.
2. Dopuszczalne jest korzystanie z poczty elektronicznej NKB poza siecią NKB za pomocą powierzonego sprzętu, zgodnie z zgodnie z obowiązującymi w NKB regulacjami wewnętrznymi oraz za pośrednictwem przeglądarki internetowej.
3. W przypadku przesyłania za pośrednictwem poczty elektronicznej Informacji podlegających ochronie należy zabezpieczyć je przed dostępem osób nieupoważnionych (np. zabezpieczony Hasłem plik ZIP, 7-ZIP lub RAR – rozwiązanie zalecane). Hasła należy przesyłać osobnym środkiem komunikacji (np. informacja przekazana pocztą elektroniczną a Hasło w wiadomości SMS).
4. Poczta elektroniczna służy do przekazywania informacji oraz komunikacji i nie jest narzędziem służącym do przechowywania informacji i dokumentów.
5. Użytkownicy zobowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych

z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.

6. W razie ryzyka przekroczenia dopuszczalnej pojemności skrzynki należy zgłosić ten fakt Administratorowi Systemu.

§ 12.

1. Za niedozwolone użycie uznaje się jakiekolwiek wykorzystanie poczty elektronicznej prowadzące do naruszenia przepisów prawa powszechnie obowiązującego, regulacji wewnętrznych, zobowiązań umownych lub innych norm a także takie wykorzystanie poczty elektronicznej, które może skutkować lub narazić NKB na szkodę lub wpłynąć negatywnie na jej reputację.
2. Zabronione jest w szczególności:
   1) rozsyłanie z komputerów NKB oraz przyznanych Użytkownikom Kont poczty wiadomości, których treść nie jest związana z wykonywaną pracą;
   2) podejmowanie działań zmierzających do ukrycia lub zniekształcenia informacji o autorze lub adresacie wiadomości, jego miejscu zatrudnienia;
   3) podejmowanie działań skutkujących naruszeniem dóbr osobistych innych Użytkowników lub osób trzecich;
   4) wykorzystanie poczty elektronicznej w celu rozsyłania spamu lub zakłócania pracy innych elementów Systemu teleinformatycznego;
   5) używanie prywatnej skrzynki poczty elektronicznej do celów służbowych, z wyłączeniem sytuacji wyjątkowych, wymagających użycia prywatnego adresu poczty elektronicznej dla zachowania ciągłości realizacji zadań na rzecz NKB;
   6) odbieranie wiadomości z nieznanych źródeł;
   7) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   8) przesyłanie pocztą elektroniczną plików wykonywalnych typu: .bat, .com, .exe;
   9) przesyłanie pocztą elektroniczną plików multimedialnych oraz plików graficznych, chyba że jest to niezbędne do prawidłowej realizacji powierzonych zadań;
   10) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
   11) nieuprawnione czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego Użytkownika;
   12) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi Systemu;
   13) posługiwanie się służbowym adresem poczty elektronicznej w celu rejestrowania się na stronach handlowych, informacyjnych, czatach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy;
   14) wykorzystywanie poczty elektronicznej do prywatnych celów, w szczególności takich jak prowadzenie działalności gospodarczej (w tym reklama towarów lub usług) lub poszukiwanie dodatkowego zatrudnienia.

§ 13.

1. NKB nie monitoruje zawartości poczty elektronicznej Użytkowników, z zastrzeżeniem zautomatyzowanego przetwarzania przez systemy antyspamowe i antywirusowe.
2. Sprawdzenie zawartości wiadomości pocztowych przez Administratora Systemu jest dopuszczalne na wniosek Przewodniczącego NKB, za zgodą IOD:
   1) w przypadku uzasadnionego podejrzenia naruszenia przez Użytkownika przepisów prawa powszechnie obowiązującego, postanowień Regulaminu lub innych regulacji wewnętrznych NKB;
   2) na wezwanie uprawnionego organu władzy publicznej, jeżeli obowiązek taki wynika z przepisów prawa powszechnie obowiązującego.

3. Adres poczty elektronicznej byłego Użytkownika może być użyty wyłącznie na potrzeby przekazania automatycznej informacji o nowym adresie poczty elektronicznej do kontaktów z NKB przez okres 3 miesięcy od dnia zakończenia stosunku prawnego łączącego Użytkownika z NKB.
4. Skrzynka pocztowa byłego Użytkownika jest utrzymywana przez okres 3 miesięcy od dnia zakończenia stosunku prawnego łączącego użytkownika z NKB, chyba, że przepisy prawa powszechnie obowiązującego stanowią inaczej. Terminy te mogą ulec przedłużeniu w przypadku dochodzenia roszczeń lub obrony przed roszczeniami przez NKB, powstałych w związku z realizacją zadań przez Użytkownika oraz innych wynikających z przepisów prawa, do momentu przedawnienia roszczeń lub innego określonego w przepisach prawa.
5. Administrator Systemu ma prawo do awaryjnego wyłączenia systemu poczty elektronicznej bez uprzedniego powiadomienia Użytkownika o tym fakcie.
6. Administrator Systemu ma prawo zablokowania Konta w poczcie elektronicznej w przypadkach jego wykorzystania w sposób niezgodny z przepisami prawa powszechnie obowiązującego, Regulaminem lub innymi regulacjami wewnętrznymi NKB oraz poinformować o tym fakcie IOD.

Rozdział 6
Ochrona Haseł i innych poufnych informacji uwierzytelniających

§ 14.

1. Hasła Użytkowników i inne poufne informacje uwierzytelniające podlegają szczególnej ochronie.
2. Użytkownik ponosi odpowiedzialność za utworzenie Hasła i jego przechowywanie.
3. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu udostępnionego Hasła.
4. Użytkownik potwierdza odbiór Haseł w sposób określony przez Administratora Systemu.
5. Każdy Użytkownik posiadający dostęp do Systemu teleinformatycznego zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich Haseł wykorzystanych do pracy w Systemie teleinformatycznym NKB;
   2) niezwłocznej zmiany Haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ich ujawnienia;
   3) niezwłocznej zmiany Hasła tymczasowego, przekazanego przez Administratora Systemu lub producenta systemu lub oprogramowania;
   4) poinformowania Administratora Systemu oraz Inspektora Ochrony Danych o podejrzeniu lub rzeczywistym ujawnieniu Hasła zgodnie z zasadami obowiązującymi w NKB;
   5) stosowania Haseł o następujących parametrach:
      a) minimalna długość Hasła powinna wynosić 12 znaków,
      b) Hasło powinno zawierać duże litery, małe litery i cyfry lub znaki specjalne,
      c) Hasła nie powinny być łatwe do odgadnięcia, w tym nie powinny być powszechnie używanymi słowami oraz nie powinny wykorzystywać dat, imion i nazwisk osób bliskich, imion zwierząt, typowych zestawów znaków, takich jak 12345, qwerty;
   6) w przypadku Haseł lub innych poufnych informacji uwierzytelniających współdzielonych z innymi Użytkownikami – zachowania tych Haseł w grupie uprawnionych Użytkowników.
6. Zabronione jest:
   1) utrwalanie Haseł w sposób umożliwiający łatwe zapoznanie się z nimi przez osobę nieuprawnioną, w tym umieszczanie ich w miejscach dostępnych dla innych osób;
   2) używanie Haseł wykorzystywanych w życiu prywatnym Użytkownika;
   3) używanie tych samych Haseł w różnych systemach operacyjnych i aplikacjach;
   4) udostępnianie Haseł innym Użytkownikom;
   5) dokonywania prób łamania Haseł;
   6) wpisywanie Haseł „na stałe" (np. w skryptach logowania).
7. W przypadku, o którym mowa w ust. 5 pkt 4, jeśli informację otrzymała jedna z wymienionych osób, osoba ta przekazuje informację pozostałym.
8. Postanowienia rozdziału stosuje się odpowiednio do innych poufnych informacji

uwierzytelniających.

§ 15.

1. Każdy Użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich używania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób nieupoważnionych.
2. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu oraz IOD. W przypadku otrzymania informacji przez jedną z osób wskazanych w zdaniu poprzednim osoba ta przekazuje informację pozostałym.

Rozdział 7

Korzystanie z oprogramowania

§ 16.

1. Użytkownicy nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej formalnie dopuszczone do użytkowania przez Administratora Systemu, w szczególności komunikatorów internetowych, edytorów tekstu, aplikacji w wersji portable. Wykaz oprogramowania dopuszczonego do użytkowania stanowi Załącznik do Regulaminu.
2. Użytkownikowi nie wolno:
   1) instalować bez zgody Administratora Systemu lub uruchamiać jakiegokolwiek innego oprogramowania niż to, które zostało mu przydzielone;
   2) pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw własności intelektualnej;
   3) kopiować i rozprowadzać bez upoważnienia oprogramowania stworzonego w NKB lub na jej potrzeby;
   4) samodzielnie usuwać udostępnionego oprogramowania.
3. W przypadku wykrycia jakichkolwiek plików lub oprogramowania innego niż to, które znajduje się wykazie, o którym mowa w ust. 1, Administrator Systemu ma prawo do natychmiastowego ich skasowania bez uzgodnienia z Użytkownikiem.
4. O przypadkach używania nieautoryzowanego oprogramowania Administrator Systemu informuje IOD.

Rozdział 8

Korzystanie z urządzeń komunikacji głosowej i wizyjnej

§ 17.

1. Każdy Użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany Informacji podlegających ochronie, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub innych miejscach, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego Hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych, na przykład za pomocą Hasła, kodu.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") Haseł dla urządzeń, o których mowa w ust. 2.
4. Drukarki nie mogą być pozostawione bez kontroli, jeśli są lub mają być w najbliższym czasie wykorzystywane do drukowania dokumentów zawierających Informacje podlegające ochronie.

Rozdział 9

Zasady „czystego biurka" oraz „czystego ekranu"

§ 18.

1. Spożywanie posiłków przy stanowiskach komputerowych oraz w pomieszczeniach, w których

znajdują się środki przetwarzania informacji (na przykład pomieszczenia serwerowni i pomieszczenia techniczne) jest zabronione.

2. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w czasie godzin pracy i poza nimi Użytkownik jest zobowiązany:
   1) przechowywać dokumenty papierowe i Nośniki danych w odpowiednio zabezpieczonych meblach biurowych;
   2) po zakończeniu pracy wylogować się z systemu i wyłączyć komputer. Nie jest dopuszczalne zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego;
   3) po zakończeniu pracy uporządkować swoje stanowisko pracy, uniemożliwiając dostęp osób nieupoważnionych do dokumentów (w szczególności zawierających Informacje podlegające ochronie);
   4) przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi lub okien podczas nieobecności w pomieszczeniu;
   5) zabezpieczać nieużywany w danym momencie komputer przed nieupoważnionym dostępem, włączając blokadę systemową; ponowny dostęp do komputera następuje po podaniu Hasła;
   6) ustawiać monitory w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu albo stosować filtr prywatyzujący;
   7) odpowiednio zabezpieczyć miejsca przyjmowania lub wysyłania korespondencji papierowej;
   8) włączać blokadę urządzeń kopiujących, zabezpieczając je w ten sposób przed nieuprawnionym użyciem;
   9) zwracać uwagę i doprowadzać do usuwania pozostawionych oryginałów lub kopii dokumentów w pobliżu drukarek;
   10) zwracać szczególną uwagą na pracujące drukarki pozostawione bez nadzoru.
3. W przypadku nieobecności na stanowisku pracy Użytkownik zobowiązany jest zakończyć aktywne sesje i wylogować się lub uruchomić wygaszacz ekranu z opcją ponownego logowania do systemu.

Rozdział 10
Zwrot Aktywów po zakończeniu umowy lub innego stosunku prawnego

§ 19.

1. W przypadku zakończenia umowy lub innego stosunku prawnego Użytkownik jest zobowiązany do zwrotu posiadanych Aktywów NKB.
2. Komputery stacjonarne, laptopy, smartfony i Nośniki danych podlegają protokolarnemu przekazaniu przez Użytkownika do Administratora Systemu.
3. O ile inne regulacje wewnętrzne NKB nie stanowią inaczej, także inne niż wymienione w ust. 2 Aktywa podlegają zwrotowi do Administratora Systemu.
4. Przed przekazaniem komputera stacjonarnego lub laptopa dane zgromadzone na urządzeniu powinny być umieszczone przez Użytkownika na dysku sieciowym. Przed przekazaniem urządzenia kolejnemu Użytkownikowi Administrator Systemu usuwa dane zgromadzone na komputerach, profile Użytkownika, pocztę itp.
5. Po usunięciu danych zgromadzonych na smartfonach Administrator Systemu przekazuje urządzenie do Działu Administracyjnego.
6. Przed przekazaniem Nośnika danych dane zgromadzone na Nośniku danych powinny być umieszczone przez Użytkownika na dysku sieciowym. Przed przekazaniem Nośnika danych kolejnemu Użytkownikowi Administrator Systemu usuwa dane zgromadzone na Nośniku danych.

Rozdział 11
Identyfikacja i zgłaszanie zdarzeń dotyczących naruszenia bezpieczeństwa

§ 20.

1. Przed przystąpieniem do pracy Użytkownik obowiązany jest sprawdzić stanowisko komputerowe ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.

2. Wszelkie działania Użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości Systemu teleinformatycznego są zabronione.
3. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, Użytkownik powinien niezwłocznie poinformować o tym fakcie właściwe osoby (w szczególności Administratora Systemu lub IOD) w sposób określony we właściwych regulacjach wewnętrznych NKB, w szczególności w Polityce Ochrony Danych Osobowych oraz w Regulaminie zgłaszania naruszeń oraz podejmowania działań następczych w związku z tymi zgłoszeniami.

Rozdział 12
Szkodliwe oprogramowanie

§ 21.

Zabronione jest celowe opracowywanie, generowanie, kompilowanie, kopiowanie, rozpowszechnianie, uruchamianie lub próby wprowadzania kodów komputerowych, które:
1) mają zdolność samopowielania;
2) mają zdolność uszkadzania lub innego utrudniania działania pamięci komputerowej, plików systemowych lub oprogramowania;
3) służą do omijania lub przełamywania zabezpieczeń i praw dostępu;
4) wymagałyby wykorzystania większej ilości zasobów, niż jest to niezbędne do zapewnienia prawidłowego działania Systemu teleinformatycznego;
5) powodowałyby zakłócenia w działaniu Systemu teleinformatycznego.

§ 22.

1. Każdy komputer jest wyposażony w oprogramowanie antywirusowe aktualizowane automatycznie. Program antywirusowy generuje cykliczny raport o stanie bezpieczeństwa komputera lub umożliwia wgląd w terminarz zdarzeń i czynności uznanych przez program za takie, które stworzyły zagrożenie.
2. Zabronione jest instalowanie dodatkowego oprogramowania antywirusowego przez Użytkownika.
3. Jeśli wiadomość elektroniczna pochodzi z nieznanego źródła, załączniki do tej wiadomości nie powinny być otwierane, nie należy także otwierać odnośników (tzw. linków) w tekście lub dołączonych banerów reklamowych. Faktyczny adres należy odczytać w polu „Od", nie sugerując się ewentualnym podobieństwem przesyłki do pochodzącej ze znanego źródła. Podejrzaną przesyłkę należy przesłać do Administratora Systemu na adres e-mail it@abm.gov.pl, po czym usunąć ze skrzynki.
4. O fakcie wykrycia złośliwego oprogramowania (wirus, robak, rootkit, trojan, backdoor, exploit, keylogger, dialer, bądź inne oprogramowanie szpiegujące) należy niezwłocznie powiadomić Administratora Systemu oraz IOD. Do czasu usunięcia złośliwego oprogramowania lub otrzymania innych poleceń, pracę na komputerze należy wstrzymać.

Rozdział 13
Postanowienia końcowe

§ 23.

Nieprzestrzeganie postanowień Regulaminu może stanowić podstawę do zablokowania lub ograniczenia możliwości korzystania z Systemu teleinformatycznego lub wybranych zasobów oraz może pociągać za sobą inne działania wynikające z postanowień Polityki bezpieczeństwa teleinformatycznego, Regulaminu i przepisów prawa powszechnie obowiązującego.

§ 24.

1. Szczegółowe zasady postępowania z Urządzeniami przenośnymi określa Instrukcja użytkowania urządzeń przenośnych.
2. Integralną część Regulaminu stanowi Załącznik – Wykaz oprogramowania dopuszczonego do użytkowania.

Załącznik do Regulaminu
użytkownika systemu teleinformatycznego
w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Wykaz oprogramowania komputerowego dopuszczonego do użytkowania w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Lista obejmuje oprogramowanie dopuszczone do eksploatacji na stacjach roboczych użytkowników. Lista nie uwzględnia oprogramowania serwerowego, sterowników, aktualizacji i specjalnego przeznaczenia oraz ilości licencji zakupionych do oprogramowania płatnego i stanowi jedyną informację o aplikacjach dozwolonych do zainstalowania na komputerach użytkowników.

Typ oprogramowania	Producent	Nazwa	Data ważności licencji
System operacyjny	Microsoft Corporation	Windows 10 lub nowszy wraz z wbudowanym pakietem aplikacji	Bezterminowo
Oprogramowanie biurowe	Microsoft Corporation	Office (wersja w zależności od posiadanej licencji objęta wsparciem producenta w zakresie dystrybucji, aktualizacji i bezpieczeństwa)	Subskrypcja roczna odnawialna
Oprogramowanie biurowe	Adobe Systems Incorporated	Acrobat Reader (czytnik plików PDF)	Bezterminowo
Oprogramowanie biurowe	Adobe Systems Incorporated	Adobe Acrobat PRO	Bezterminowo
Edytor tekstu	Open Source	Notepad++	Bezterminowo
Przeglądarka internetowa	Microsoft Corporation	Internet Explorer, Microsoft Edge	Bezterminowo
Przeglądarka internetowa	Google LLC	Google Chrome	Bezterminowo
Aplikacja narzędziowa	Igor Pavlov	7-Zip	Bezterminowo
Aplikacja narzędziowa	philandro Software GmbH	AnyDesk	Bezterminowo
Aplikacja do wideokonferencji	Zoom Technologies	Zoom	Bezterminowo
Aplikacja do wideokonferencji	Cisco Systems, Inc	Webex	Bezterminowo
Podpis kwalifikowany	Krajowa Izba Rozliczeniowa S.A.	Szafir	Bezterminowo
Podpis kwalifikowany	Ministerstwo Spraw Wewnętrznych i Administracji	e-Dowód	Bezterminowo
Podpis kwalifikowany	Certum	SimplySign, SmartSign	Bezterminowo
Podpis kwalifikowany	CenCert	PEM-HEART Signature	Bezterminowo
Podpis kwalifikowany	PWPW S.A	Sigillum Sign	Bezterminowo

Elektroniczny obieg dokumentów	**Podlaski Urząd Wojewódzki w Białymstoku**	**EZD**	**Bezterminowo**
Oprogramowanie antywirusowe	**ESET, spol. s r.o.**	**ESET Endpoint Security, Management Agent**	**Zgosdnie z licencją**
Oprogramowanie antywirusowe	**WithSecure™**	**WithSecure**	**Zgodnie z licencją**
Edytor do zarządzania danymi	**Microsoft Corporation**	**Azure Data Studio**	**Bezterminowo**

Załącznik nr 3
do Polityki bezpieczeństwa teleinformatycznego
w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Wzór wykazu oprogramowania w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Typ oprogramowania	Producent	Nazwa	Data ważności licencji

Załącznik nr 4
do Polityki bezpieczeństwa teleinformatycznego
w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Instrukcja użytkowania urządzeń przenośnych w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych

Obowiązuje od:	**18.07.2023 r.**
Wersja:	**1.0**

Spis treści

Rozdział 1

Postanowienia ogólne

§ 1.

1. Instrukcja użytkowania urządzeń przenośnych w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych (dalej: Instrukcja) określa zasady postępowania z Urządzeniami przenośnymi wykorzystywanymi w Naczelnej Komisji Bioetycznej do spraw Badań Klinicznych (dalej: NKB), w tym wykorzystywania Urządzeń przenośnych poza siedzibą NKB.
2. Każdy Użytkownik korzystający z Urządzenia przenośnego udostępnionego mu przez NKB jest zobowiązany do zapoznania się z Instrukcją i jej przestrzegania.
3. Ilekroć w Instrukcji jest mowa o Członkach NKB, jej postanowienia stosuje się odpowiednio do innych Użytkowników.

§ 2.

1. Definicje użyte w Polityce oznaczają:
   1) ABM – Agencja Badań Medycznych;
   2) Administrator Systemu – pracownik lub komórka organizacyjna ABM, Członek NKB któremu powierzono nadzór nad Systemem teleinformatycznym;
   3) Członek NKB –Przewodniczący NKB lub inny członek NKB;
   4) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi;
   5) Informacja podlegająca ochronie – informacja podlegająca ochronie na podstawie przepisów prawa powszechnie obowiązującego (na przykład dane osobowe, tajemnica przedsiębiorstwa) lub regulacji wewnętrznych NKB (na przykład informacje chronione w rozumieniu Procedury klasyfikowania informacji oraz postępowania z określonymi grupami informacji);
   6) IOD - Inspektor Ochrony Danych;
   7) Nośnik danych – urządzenie wymienne i przenośne umożliwiające zapis, modyfikację lub odczyt danych, takie jak: pendrive, dysk przenośny, dysk wewnętrzny, karta pamięci, taśma magnetyczna, nośnik optyczny itp.;
   8) System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. System teleinformatyczny obejmuje między innymi sprzęt komputerowy, Urządzenia przenośne, oprogramowanie systemowe, systemy (podsystemy), sieć, aplikacje;
   9) Urządzenie przenośne – informatyczne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie lub wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią, takie jak laptop, smartfon, tablet lub Nośnik danych;
   10) Użytkownik – Członek NKB lub inna osoba realizująca zadania na rzecz NKB na podstawie umowy lub innego stosunku prawnego, która w związku z realizacją tych zadań przetwarza informacje.
2. W braku odmiennych definicji, określenia użyte w Instrukcji mają znaczenie nadane im w Polityce bezpieczeństwa teleinformatycznego.

Rozdział 2

Zasady korzystania z Urządzeń przenośnych

§ 3.

1. Zabrania się podłączania do Systemu teleinformatycznego Urządzeń przenośnych niebędących jej własnością.

2. Nie zezwala się na wykorzystywanie Urządzeń przenośnych w celach innych niż wykonywanie obowiązków służbowych, w tym na przechowywanie na Urządzeniach przenośnych danych osobowych innych niż dane wykorzystywane w związku z realizacją przez Członków NKB obowiązków służbowych oraz w zakresie szerszym, niż jest to niezbędne do realizacji tych obowiązków.

§ 4.

1. Wymaga się, aby wszystkie dyski w laptopach będących na wyposażeniu NKB były szyfrowane. Za szyfrowanie dysków w laptopach odpowiada Administrator Systemu.
2. Laptopy podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu do laptopa (w tym dostępu do BIOS) Hasłem.
3. Wymaga się, aby na Urządzeniach przenośnych znajdowało się oprogramowanie antywirusowe.

§ 5.

1. Urządzenia przenośne typu smartfon wymagają zabezpieczenia przy użyciu kodu PIN, Hasła, symbolu lub zabezpieczeń biometrycznych.
2. Nie zezwala się na wykorzystywanie smartfonów jako celowych Nośników danych (karta pamięci, notes na Hasła itp.).

§ 6.

1. W przypadku przenoszenia poza siedzibę NKB Informacji podlegających ochronie, przechowywanych na Nośnikach danych, wymagane jest, aby Użytkownik przechowywał dane na Nośnikach danych zaszyfrowanych oprogramowaniem szyfrującym np. BitLocker.
2. Szyfrowanie Nośników danych stanowiących własność NKB przeprowadza przed pierwszym ich użyciem Administrator Systemu, zabezpieczając unikalny kod odtwarzania oraz nadając Nośnikom danych tymczasowe Hasło.
3. Użytkownik Nośnika danych jest zobowiązany zmienić Hasło tymczasowe na własne przy pierwszym użyciu Nośnika danych, przy czym zastosowane przez Użytkownika Hasło musi spełniać wymagania określone w Polityce bezpieczeństwa teleinformatycznego, Regulaminie użytkownika systemu teleinformatycznego oraz Polityce ochrony danych osobowych.
4. Niezależnie od obowiązku szyfrowania Nośników danych zaleca się przechowywanie danych na Nośnikach danych w formie plików spakowanych (ZIP, 7-ZIP, RAR itp.) zabezpieczonych Hasłem. Hasło powinno spełniać wymagania określone w ust. 3.

§ 7.

1. Zabrania się przechowywania Informacji podlegających ochronie na Urządzeniach przenośnych niezaszyfrowanych lub niebędących własnością NKB.
2. Na Urządzeniach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie mogą znajdować się Informacje podlegające ochronie.

§ 8.

1. Dane przechowywane na Urządzeniach przenośnych powinny być ograniczone do niezbędnego minimum.
2. Za wszelkie działania oraz dane zgromadzone na Urządzeniach przenośnych odpowiada ich aktualny Użytkownik.

§ 9.

1. Użytkownik ma obowiązek zachować szczególną ostrożność przy podłączaniu Urządzeń przenośnych do sieci obcych. Korzystanie z sieci publicznych jest dozwolone tylko w niezbędnych przypadkach. Zabrania się korzystania z otwartych sieci Wi-Fi hotspot.
2. W przypadku podłączania Urządzenia przenośnego do sieci obcej należy zastosować zabezpieczenie fizyczne lub programowe pełniące funkcję zapory typu firewall oraz posiadać aktywne i zaktualizowane oprogramowanie antywirusowe.

§ 10.

1. Użytkowane poza Systemem teleinformatycznym Urządzenia przenośne, przed rozpoczęciem pracy z tymi urządzeniami w Systemie teleinformatycznym, muszą zostać sprawdzone za pomocą aktualnego oprogramowania antywirusowego.
2. Użytkownik zobowiązany jest do zabezpieczenia Urządzenia przenośnego z zachowaniem szczególnej ostrożności w czasie transportu, przechowywania i używania, przy czym:
   1) laptopy zaleca się transportować w specjalnym futerale pod stałym nadzorem Użytkownika;
   2) zabrania się pozostawiania laptopa bez nadzoru lub w oddaleniu od Użytkownika;
   3) zabrania się pozostawiania laptopa w samochodzie podczas postoju w miejscu publicznym bez nadzoru;
   4) podczas jazdy samochodem zaleca się przechowywanie laptopa w miejscu niewidocznym, np. pod siedzeniem kierowcy, w zamkniętym bagażniku itd. Zabrania się przewożenia laptopa np. na siedzeniach i widocznych miejscach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach;
   5) zaleca się przewożenie Nośników danych w większych torbach lub futerałach z zamknięciem, w miejscach uniemożliwiających ich przypadkowe wysunięcie lub kradzież.
3. W przypadku kradzieży lub utraty w inny sposób Urządzenia przenośnego, Użytkownik powinien niezwłocznie powiadomić Administratora Systemu, IOD zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane. W przypadku otrzymania informacji przez jedną z osób wskazanych w zdaniu poprzednim osoba ta przekazuje informację pozostałym. W przypadku kradzieży należy ponadto niezwłocznie zawiadomić Policję oraz sporządzić notatkę służbową.
4. Zabrania się udostępniania Urządzeń przenośnych osobom nieupoważnionym.
5. W przypadku, gdy konieczne jest pozostawienie laptopa w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do zabezpieczenia danych przez wylogowanie się lub wyłączenie urządzenia. W szczególności dotyczy to zabezpieczenia komputera poza NKB na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, itp.
6. W przypadku konieczności wykonania pracy przy obecności osób nieupoważnionych, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem tych osób.

§ 11.

1. Nośniki danych są przechowywane i eksploatowane zgodnie z zaleceniami producenta, z uwzględnieniem wymagań w zakresie ochrony informacji, które są umieszczone na Nośnikach danych.
2. Wycofanie z eksploatacji Nośników danych lub przekazanie do naprawy jest poprzedzone archiwizacją danych (o ile jest taka możliwość), a następnie ich trwałym usunięciem.
3. Uszkodzone Nośniki danych zawierające Informacje podlegające ochronie są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.
4. Zasady i tryb postępowania z Nośnikami danych przekazanymi do archiwum określają odrębne regulacje wewnętrzne NKB.

§ 12.

1. Dopuszcza się wykorzystywanie Urządzeń przenośnych przez więcej niż jednego Użytkownika pod warunkiem każdorazowego usunięcia danych przed przekazaniem urządzenia innemu Użytkownikowi.
2. W przypadku określony w ust. 1 należy stosować zasady zwrotu aktywów określone w Regulaminie Użytkownika systemu teleinformatycznego.
3. Urządzenia przenośne przekazywane są kolejnym Użytkownikom bez danych wcześniejszych Użytkowników.

Rozdział 3

Postanowienia końcowe

§ 13.

Nieprzestrzeganie postanowień Regulaminu może stanowić podstawę do zablokowania lub ograniczenia możliwości korzystania z Systemu teleinformatycznego lub wybranych zasobów oraz może pociągać za sobą inne działania wynikające z postanowień Polityki bezpieczeństwa teleinformatycznego, Regulaminu i przepisów prawa powszechnie obowiązującego.