Polityka Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju

Opracował:	Sprawdził:	Zatwierdził:
Zbigniew Zieliński Dyrektor DAG Podpis:	Leszek Grabarczyk Z-ca Dyrektora Centrum Podpis:	Jerzy Kątcki Z-ca Dyrektora Centrum Podpis:
Dokument jest nadzorowany i opublikowany w formie elektronicznej. Niniejszy dokument jest aktualny w dniu wydruku. Użytkownik egzemplarza jest zobowiązany do śledzenia zmian w dokumencie po terminie wydruku.		

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja, usuwanie, dodawanie:

1. Administrator Danych - Dyrektor Centrum.
2. Pełnomocnik Dyrektora Centrum ds. Systemu Zarządzania Bezpieczeństwa Informacji
3. Administrator Bezpieczeństwa Informacji.

Zakres dostępu do dokumentu – odczyt:

4. Wszyscy upoważnieni pracownicy/współpracownicy, wykonawcy, stażyści i praktykanci.
5. Podmioty i instytucje upoważnione na podstawie przepisów prawa.

Spis treści

1 Wstęp

Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym istotne aktywa oraz sposoby reagowania na zagrożenia dla tych aktywów. Zapewnienie odpowiedniej wiedzy zarządzających jednostką oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Pracownicy obsługujący systemy przetwarzające informacje są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania aktywów instytucji.

Zastosowanie niniejszej Polityki Bezpieczeństwa Informacji powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do kategorii danych, jednocześnie dopasowane do poziomu zagrożeń występujących dla przetwarzanych i przechowywanych informacji objętych ochroną. W szczególności ochrona powinny być adekwatna do oszacowanych ryzyk.

W celu zapewnienia bezpieczeństwa informacji wprowadza się spójny system zarządzania bezpieczeństwem informacji.

Niniejszy dokument Polityki Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju (NCBR) jest jednym z elementów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Narodowym Centrum Badań i Rozwoju. Polityka Bezpieczeństwa Informacji jest aktem wewnętrznego stosowania wprowadzanym przez Dyrektora Centrum.

Polityka Bezpieczeństwa Informacji opisuje ogólne zasady ochrony informacji obowiązujące w NCBR, zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania bezpieczeństwem informacji. Polityka określa również warunki, jakie muszą spełniać systemy informatyczne przetwarzające informacje w NCBR.

2 Cel

Celem Polityki Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju jest zapewnienie właściwej ochrony zasobów oraz ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju.

3 Deklaracja kierownictwa

Dyrekcja NCBR przywiązuje dużą wagę do ochrony informacji przetwarzanych i przechowywanych w Centrum. W związku z czym rozumie konieczność zapewnienia odpowiedniego poziomu ochrony informacji w realizowanych zadaniach zarówno dla zachowania wysokiego poziomu bezpieczeństwa informacji, a także w celu spełnienia wymagań prawnych w odniesieniu do ochrony informacji, ustanawia System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z wymogami normy PN-ISO/IEC 27001, którego nadrzędny dokument stanowi niniejsza Polityka Bezpieczeństwa Informacji. NCBR jest w pełni zaangażowana i wspiera procesy zmierzające do zapewnienia bezpieczeństwa informacyjnego. Wprowadzając Politykę Bezpieczeństwa Informacji, deklaruje, że wdrożony System Zarządzania Bezpieczeństwem Informacji będzie podlegał ciągłemu doskonaleniu zgodnie z wymaganiami normy PN-ISO/IEC 27001. Zakres zarządzania bezpieczeństwem informacji obejmuje wszystkie kluczowe obszary działalności NCBR.

Głównym celem ustanowienia SZBI jest odpowiednie zabezpieczenie przetwarzanych przez NCBR informacji, ze szczególnym uwzględnieniem bezpieczeństwa przetwarzanych informacji z zachowaniem ich poufności, dostępności oraz integralności. Poufność informacji oznacza, że dostęp do informacji posiadają jedynie osoby upoważnione. Integralność określa jakość informacji w aspekcie kompletności, spójności i wiarygodności danych. Dostępność oznacza dostępność informacji dla osób upoważnionych wtedy, kiedy potrzebują tych danych do przetwarzania.

Ponadto celem wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji jest:

1. Zagwarantowanie właściwej ochrony informacji, w tym odpowiedniego poziomu bezpieczeństwa informacji bez względu na jakim nośniku jest zapisana.
2. Zapewnienie ciągłości procesów przetwarzania informacji.
3. Ograniczenie występowania zagrożeń dla bezpieczeństwa informacji.
4. Zapewnienie właściwego funkcjonowania wszystkich systemów informatycznych.
5. Właściwe reagowanie na incydenty bezpieczeństwa informacji.

Realizacja przyjętych celów powinna być zrealizowana poprzez:

1. Wskazanie sposobu organizacji systemu zarządzania bezpieczeństwem informacji.
2. Wyznaczenie zadań i odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji.
3. Wyznaczenie właścicieli dla aktywów i zasobów informacyjnych, którzy odpowiadają za zapewnienie adekwatnego poziomu bezpieczeństwa przetwarzanych informacji.
4. Wdrożenie i utrzymanie niezbędnych zabezpieczeń organizacyjnych i technicznych.
5. Zapoznanie się przez wszystkich pracowników/współpracowników, wykonawców i osoby realizujące zadania na zlecenie NCBR z właściwymi politykami i procedurami bezpieczeństwa informacji obowiązującymi w związku z wykonywanymi obowiązkami.
6. Przegląd i utrzymanie aktualnych polityk i procedur oraz pozostałej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
7. Reakcja na zagrożenia i incydenty dla bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
8. Ciągłe podnoszenie świadomości pracowników w obszarze bezpieczeństwa informacji.
9. Ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy PN-ISO/IEC 27001 i zaleceniami wszystkich zainteresowanych stron.

4 Zakres

4.1 Zakres stosowania Polityki Bezpieczeństwa Informacji

Niniejszy dokument dotyczy wszystkich komórek organizacyjnych NCBR oraz wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, a także innych osób uzyskujących dostęp do informacji przetwarzanych w NCBR (np. współpracowników, ekspertów, konsultantów, pracowników firm zewnętrznych realizujących prace na rzecz NCBR oraz organizacji związanych).

Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).

Z dokumentem polityki zapoznają się wszystkie osoby mające dostęp do informacji.

Zasady zawarte w niniejszym dokumencie muszą być przestrzegane przez wszystkie osoby mające dostęp do informacji.

4.2 Zakres Systemu Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji w NCBR obejmuje wszystkie lokalizacje i wszystkie zadania realizowane przez Centrum z wyłączeniem Kancelarii Tajnej, która działa na podstawie odrębnych przepisów.

5 Terminologia

Pojęcia używane w Polityce Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju oraz innych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji są zdefiniowane w dokumencie ***Wspólny słownik pojęć używanych w Narodowym Centrum Badań i Rozwoju.***

6 Organizacja bezpieczeństwa informacji

Zarządzanie bezpieczeństwem informacji w NCBR odbywa się na poziomach:

Na poziomie strategicznym – prowadzone jest zarządzanie strategią rozwoju i doskonalenia SZBI w odniesieniu do zmieniającego się otoczenia prawnego i technologicznego jak również w oparciu o wyniki analizy ryzyka. W procesy decyzyjne tego poziomu zaangażowane jest kierownictwo.

Na poziomie taktycznym – tworzone są standardy bezpieczeństwa informacji oraz zasady kontroli ich wypełniania w stosowanych rozwiązaniach i systemach informatycznych oraz przestrzegania w praktyce używania tych rozwiązań i systemów. W te procesy decyzyjne zaangażowane jest kierownictwo poszczególnych komórek organizacyjnych związanych z zarządzaniem bezpieczeństwem informacji.

Na poziomie operacyjnym – prowadzona jest administracja bezpieczeństwem informacji pod kątem pełnego stosowania standardów bezpieczeństwa oraz rozwiązywania sytuacji zakłóceń wynikających z naruszenia tych standardów.

6.1 Procesy zarządzania bezpieczeństwem informacji

6.1.1 Zarządzanie ryzykiem

Strategicznym elementem zarządzania aktywami i bezpieczeństwem informacji w NCBR jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem. Wyniki analizy ryzyka stanowią podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia zabezpieczeń informacji NCBR.

Analiza ryzyka prowadzona jest zgodnie z procedurą zarządzania ryzykiem opisaną w dokumencie ***Procedura identyfikacji i klasyfikacji aktywów oraz zarządzania ryzykiem w Narodowym Centrum Badań i Rozwoju***. Procedura bazuje na wytycznych normy PN-ISO/IEC 27005:2014 oraz przyjętej przez Narodowe Centrum Badań i Rozwoju metodyce szacowania i analizy ryzyka opisanej w ***Procedurze PZ3-1 Zarządzanie ryzykiem***.

6.1.1.1 Analiza ryzyka

Podstawowym kryterium oceny ryzyk jest eliminacja ryzyk o maksymalnej wartości z obszarów o największym ryzyku oraz eliminowanie ryzyk związanych z niezgodnością z regulacjami prawnymi. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla zagrożeń o ryzyku większym niż ustalony poziom ryzyka akceptowalnego oraz dla zagrożeń związanych z niezgodnością z przepisami prawa. Analiza ryzyka jest przeprowadzana regularnie, nie rzadziej niż raz do roku, ryzyka są regularnie raportowane do

Kierownictwa oraz do zainteresowanych stron. Analiza ryzyka przeprowadzana jest również po wprowadzeniu zmian mających wpływ na system bezpieczeństwa informacji.

6.1.1.2 Dobieranie i stosowanie zabezpieczeń

Cele stosowania zabezpieczeń i zabezpieczenia są dobierane na podstawie:

1. Zapisów obowiązujących aktów prawnych.
2. Wyników przeprowadzonej analizy ryzyka w bezpieczeństwie informacji.
3. Dobrych praktyk uznanych w obrocie profesjonalnym.

Zabezpieczenia wybierane są w obszarach:

1. Fizycznym.
2. Organizacyjnym.
3. Technicznym.

W doborze celów stosowania zabezpieczeń i zabezpieczeń Narodowe Centrum Badań i Rozwoju wykorzystuje zalecenia wynikające z Polskiej Normy PN-ISO/IEC 27002. Cele zabezpieczeń i zabezpieczenia są zawarte w ***Deklaracji stosowania zabezpieczeń Narodowego Centrum Badań i Rozwoju***.

6.1.2 Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji

Monitorowanie Systemu Zarządzania Bezpieczeństwem Informacji jest realizowane poprzez:

1. Wykonywanie audytów wewnętrznych i zewnętrznych.
2. Wykonywanie przeglądów dokonywanych przez Dyrektora Centrum.

Działania powyższe prowadzone są zgodnie z ***Procedurą audytu i przeglądu Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju***.

6.1.3 Utrzymanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji jest udoskonalany poprzez podjęcie następujących działań:

1. Przeprowadzanie działań korygujących oraz ocena ich skuteczności.
2. Przeprowadzanie działań zapobiegawczych oraz ocena ich skuteczności.
3. Informowanie zainteresowanych stron o działaniach i udoskonaleniach.

Działania powyższe prowadzone są zgodnie z ***Procedurą audytu i przeglądu Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju***.

6.1.4 Nadzór nad dokumentacją i zapisami

Nadzór nad dokumentacją jest prowadzony poprzez:

1. Utrzymywanie i nadzorowanie dokumentacji systemowej.
2. Utrzymywanie i nadzorowanie zapisów systemowych.

Działania powyższe prowadzone są zgodnie z ***Procedurą PZ3-4 Nadzór nad dokumentacją opisującą procesy.***

6.1.5 Zarządzanie dostępem

Dostęp do aktywów oraz zasobów informacyjnych NCBR jest realizowany za pomocą zatwierdzonych sposobów postępowania oraz mechanizmów kontrolnych w obszarach fizycznego dostępu do informacji oraz danych w Systemach Informatycznych.

Działania powyższe prowadzone są zgodnie z ***Procedurą kontroli dostępu do budynków i pomieszczeń w Narodowym Centrum Badań i Rozwoju*** w zakresie bezpieczeństwa dostępu fizycznego oraz ***Procedurą kontroli dostępu do systemu informatycznego w Narodowym Centrum Badań i Rozwoju.***

6.1.6 Zarządzanie incydentami

Zarządzanie incydentami związanymi z bezpieczeństwem informacji jest realizowane za pomocą następujących działań:

1. Monitorowania i wykrywania naruszeń bezpieczeństwa w obszarach fizycznego dostępu.
2. Monitorowania i wykrywania naruszeń bezpieczeństwa w systemach informatycznych.

Działania powyższe prowadzone są zgodnie z ***Procedura zarządzania incydentami naruszenia bezpieczeństwa informacji w Narodowym Centrum Badań i Rozwoju.***

6.2 Zakres i budowa dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

W zakres dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji wchodzą:

1. Polityka Bezpieczeństwa Informacji
2. Deklaracja Stosowania
3. Polityki grup informacji chronionych
4. Procedury
5. Szczegółowe polityki
6. Opisy przyjętych metod postępowania
7. Plany
8. Regulaminy, zasady
9. Formularze
10. Standardy
11. Zarządzenia

Dokumentacja Systemu Zarządzania Bezpieczeństwa Informacji składa się z trzech poziomów:

1. Polityki Bezpieczeństwa Informacji
2. Polityki grupy informacji
3. Polityki systemu informatycznego

6.2.2 Poziom całej jednostki

Niniejszy dokument ***Polityki Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju***, określa wymagania i zasady bezpieczeństwa informacji obowiązujące w NCBR oraz sposób organizacji Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju.

6.2.3 Poziom grup informacji chronionych

Dokumentacja grup informacji chronionych składa się z:

1. ***Polityki Bezpieczeństwa Danych Osobowych Narodowego Centrum Badań i Rozwoju.***

6.2.4 Poziom systemów informatycznych

Dokumentacja Systemów Informatycznych składa się z ***Polityki Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju,*** która opisuje wymagania i zasady bezpieczeństwa dla systemów informatycznych***.***

W razie potrzeby, gdy wymagania są realizowane również w odrębnych systemach informatycznych, dla tych systemów informatycznych wymagania i zasady bezpieczeństwa są opisywane w politykach poszczególnych Systemów Informatycznych.

6.2.5 Dokumentacja procedur, instrukcji i regulaminów

Procedury, instrukcje, regulaminy i inne dokumenty Systemu Zarządzania Bezpieczeństwem Informacji tworzone są w celu szczegółowego opisu zasad opisanych w poszczególnych politykach. Podział dokumentacji jest zalecany z uwagi na stosowanie zasady wiedzy koniecznej.

6.3 Zasady zarządzania bezpieczeństwem informacji

Zarządzanie bezpieczeństwem informacji w NCBR jest podzielone na trzy poziomy zgodnie z podziałem dokumentacji:

- Polityka Bezpieczeństwa Informacji – określenie wymagań bezpieczeństwa
- Grupa Informacji – uszczegółowienie wymagań dla grup informacji
- System Informatyczny – spełnienie wymagań bezpieczeństwa przez systemy informatyczne

Na poziomie Polityki Bezpieczeństwa Informacji wskazane są role:

- Głównego Administratora Informacji - Dyrektor NCBR
- Pełnomocnika Dyrektora Centrum ds. Systemu Zarządzania Bezpieczeństwa Informacji Administratora Bezpieczeństwa Informacji

Na poziomie grup informacji wskazane są role:

- Kierownika Komórki Organizacyjnej
- Administratora Bezpieczeństwa Informacji

Na poziomie systemów informatycznych wskazane są role:

- Dyrektor DAG
- Administratora Bezpieczeństwa Systemów Informatycznych,

Relacje pomiędzy rolami są przedstawione na schemacie w załączniku nr 1 do Polityki Bezpieczeństwa Informacji.

6.3.1 Odpowiedzialność za bezpieczeństwo informacji

1. Dyrekcja NCBR, w szczególności Dyrektor Centrum, jest odpowiedzialny za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz wskazanych w nim odpowiednich zabezpieczeń. Głównym Administratorem Informacji jest Dyrektor Centrum, który w szczególności:
   a. Wprowadza, zarządza i sprawuje nadzór nad działaniem SZBI,
   b. Określa rodzaje zasobów podlegających ochronie,
   c. Decyduje o celach i środkach przetwarzania danych,
   d. Jest Administratorem Danych Osobowych.
2. Kierownicy Komórek Organizacyjnych odpowiadają za:
   a. Przestrzeganie zasad ochrony informacji przez nich samych jak i przez podległych im pracowników,
   b. Identyfikowanie i dokumentowanie zagrożeń dla bezpieczeństwa informacji,
   c. Definiowanie oraz realizację działań zapobiegających zagrożeniom,
   d. Zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy,
   e. Przeszkolenie pracowników w zakresie przepisów prawa oraz wewnętrznych zasad Narodowego Centrum Badań i Rozwoju dotyczących ochrony informacji,
   f. Poprawność merytoryczną danych gromadzonych za pomocą systemów informatycznych,
   g. Postępowanie zgodne z opisanymi i przyjętymi zasadami celem bezpiecznego przetwarzania danych osobowych i innych informacji,
   h. Wnioskowanie o nadanie, zmianę lub odebranie uprawnień,
   i. Stosowanie się do zasad na rzecz zabezpieczenia zasobów, nad którymi sprawuje nadzór,
   j. Zapewnienie użytkownikowi stanowiska pracy zgodnie z powierzonymi obowiązkami,
   k. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń bezpieczeństwa,
   l. Współpracę z osobami pełniącymi role odpowiedzialne za bezpieczeństwo informacji w SZBI oraz innymi Kierownikami Komórek Organizacyjnych w zakresie realizacji zadań dotyczących bezpieczeństwa informacji,
   m. Opiniowanie Polityki Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju i Polityki Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju,
   n. Opiniowanie i wnioskowanie o zmiany do Regulaminu Użytkownika Systemów Informatycznych Narodowego Centrum Badań i Rozwoju,
   o. Nadzorowanie przestrzegania Regulaminu Użytkownika Systemów Informatycznych Narodowego Centrum Badań i Rozwoju,
   p. Monitorowanie i wnioskowanie o zmianę parametrów pracy systemów informatycznych w celu identyfikacji wszelkich nieprawidłowości w pracy systemów.

3. Administrator Systemów/Informatyk jest odpowiedzialny za:
   a. Monitorowanie oraz zapewnienie ciągłości działania Systemu Informatycznego,
   b. Nadzór nad utrzymaniem właściwej konfiguracji i wydajności Systemu Informatycznego,
   c. Nadzór nad instalowaniem i konfigurowaniem sprzętów, systemów i aplikacji,
   d. Nadzór nad administracją oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
   e. Współpracę z dostawcami aplikacji,
   f. Nadzorowanie wdrożonych aplikacji,
   g. Nadzór nad dokumentacją dla Systemów Informatycznych,
   h. Nadzór nad standardami bezpieczeństwa dotyczących Systemów Informatycznych,
   i. Nadzór nad procedurami określającymi zarządzanie Systemem Informatycznym,
   j. Wnioskowanie o zmiany do Polityki Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju i Regulaminu Użytkownika Systemów Informatycznych Narodowego Centrum Badań i Rozwoju,
   k. Nadzór nad wykonywaniem oraz wykonywanie i odtwarzanie kopii bezpieczeństwa,
   l. Zarządzanie funkcjonalnością systemu,
   m. Prowadzenie ewidencji nadanych uprawnień dostępu do Systemów Informatycznych,
   n. Nadzór nad prowadzeniem oraz prowadzenie dokumentacji dla Systemów Informatycznych,
   o. Utrzymanie właściwej konfiguracji i wydajności oraz ciągłości pracy Systemów Informatycznych,
   p. administrowanie oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
   q. Prowadzenie dzienników systemowych,
   r. Zarządzanie kopiami zapasowymi danych aplikacji i systemów, w tym danych osobowych,
   s. Prowadzenie rejestrów incydentów w systemach,
   t. Zarządzanie infrastrukturą i zasobami sieci ,
   u. Zarządzanie kopiami zapasowymi urządzeń sieciowych,
   v. Instalowanie i konfigurowanie urządzeń aktywnych i infrastruktury sieciowej,
   w. Utrzymanie właściwej konfiguracji i wydajności sieci,
   x. Administrowanie infrastrukturą i zasobami sieci w stopniu umożliwiającym zachowanie bezpieczeństwa sieci i zabezpieczenie danych przed nieupoważnionym dostępem,
   y. Prowadzenie dokumentacji dla infrastruktury sieciowej,
   z. zapewnienie ciągłości działania i odpowiedniej dostępność usług uruchomionych w ramach infrastruktury informatycznej.

4. Odpowiedzialność za bezpieczeństwo informacji w NCBR ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi w szczególności winien:
   a. Stosować zasady opisane w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz innych dokumentach wewnętrznych,
   b. Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych,
   c. Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,
   d. Chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione,
   e. Utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Narodowym Centrum Badań i Rozwoju,
   f. Stosować się do szczegółowych zaleceń w zakresie bezpiecznej obsługi systemów informatycznych.
5. Pełnomocnik Dyrektora Centrum ds. Systemu Zarządzania Bezpieczeństwem Informacji jest odpowiedzialny za:
   a. Nadzór nad realizacją Polityką Bezpieczeństwa Informacji,
   b. Nadzór nad dokumentacją SZBI na etapie jej opracowywania, weryfikacji, aktualizacji, udostępniania i przechowywania,
   c. Zapewnienie, że procesy potrzebe w SZBI są ustanowione, wdrożone i utrzymywane,
   d. Nadzór nad planowaniem prac dotyczących SZBI oraz ich realizacją,
   e. Przedstawianie sprawozdań do Dyrekcji NCBR dotyczących funkcjonowania SZBI oraz realizacji celów, jak również informowanie o skuteczności funkcjonującego SZBI,
   f. Nadzorowanie audytów wewnętrznych w zakresie ich realizacji a także nadzorowania zespołu audytorów wiodących,
   g. Nadzorowanie działań wdrożeniowych, korygujących oraz zapobiegawczych w SZBI,
   h. Organizację przeglądów SZBI oraz nadzór nad realizacją ustaleń wynikających z przeglądów,
   i. Powiadamianie kierownictwa o działalności niezgodnej z obowiązująca w SZBI,
   j. Nadzorowanie szkoleń z zakresu SZBI,
   k. Koordynację działań związanych z ochroną informacji w NCBR,
   l. Wprowadzanie zatwierdzonych polityk bezpieczeństwa,
   m. Prowadzenie analizy ryzyka dla bezpieczeństwa informacji,
   n. Utrzymywanie wykazu zasobów informacyjnych,
   o. Analizę raportów z wszelkich zdarzeń związanych z bezpieczeństwem wszystkich zasobów informacyjnych,
   p. Monitorowanie zachowania właściwego poziomu bezpieczeństwa informacji,

q. Sprawowanie nadzoru nad przestrzeganiem zasad ochrony informacji.

i uprawniony jest do:

a. Wydawania poleceń wszystkim pracownikom NCBR w zakresie związanym z wdrożeniem, utrzymaniem i doskonaleniem SZBI,

b. Rozstrzygania sporów dotyczących stosowania i interpretacji wymagań zawartych w dokumentacji SZBI oraz wydawania wiążących decyzji w tym zakresie,

c. Dostępu do wszystkich dokumentów występujących w NCBR, których treść może być istotna z punktu widzenia funkcjonowania SZBI,

d. Uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach SZBI,

e. Reprezentowania NCBR na zewnątrz w sprawach dotyczących SZBI, w pełnym zakresie, w zakresie współpracy z pozostałymi komórkami organizacyjnymi.

6. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za:

a. Jest administratorem bezpieczeństwa informacji zgodnie z ustawą o ochronie danych osobowych,

b. Prowadzenie rejestru osób dopuszczonych do przetwarzania danych osobowych,

c. Przygotowanie dokumentów wymagań bezpieczeństwa dla przetwarzania danych osobowych,

d. Przygotowanie dokumentów wymagań bezpieczeństwa dla systemów informatycznych przetwarzających dane osobowe,

e. Analizowanie ryzyka dla bezpieczeństwa danych osobowych,

f. Szkolenie pracowników z zakresu bezpieczeństwa danych osobowych,

7. Administrator Bezpieczeństwa Systemów Informatycznych jest odpowiedzialny za:

a. Sprawowanie nadzoru nad bezpieczeństwem Systemów Informatycznych,

b. Prowadzenie nadzoru nad przygotowaniem dokumentów polityk bezpieczeństwa dla Systemów Informatycznych, nad którymi sprawuje nadzór,

c. Prowadzenie nadzoru nad przygotowaniem dokumentów planów ciągłości działania i planów awaryjnych dla systemów informatycznych, nad którymi sprawuje nadzór,

d. Opiniowanie i wprowadzanie polityk bezpieczeństwa dla Systemów Informatycznych, nad którymi sprawuje nadzór,

e. Opracowanie, sprawdzenie i wprowadzanie planów ciągłości działania i planów awaryjnych dla systemów informatycznych, nad którymi sprawuje nadzór,

f. Opiniowanie i sprawdzanie proponowanych zmian i rozwiązań w politykach dla systemów informatycznych, nad którymi sprawuje nadzór,

g. Ocenę pracy systemów informatycznych w celu wykrycia potencjalnych zagrożeń, w szczególności identyfikacji wszelkich nieprawidłowości związanych z bezpieczeństwem Systemów Informatycznych,

h. Opiniowanie i wnioskowanie o zmiany do Regulaminu Użytkownika Systemów Informatycznych,

i. Przeprowadzanie analizy ryzyka dla Systemów Informatycznych,

j. Prowadzenie analizy podatności systemów,

k. Weryfikację zgodności informatycznych środków przetwarzania z odpowiednimi politykami bezpieczeństwa i autoryzowanie ich do stosowania w NCBR,

l. Opracowanie, sprawdzenie i wprowadzenie standardów bezpieczeństwa dotyczących Systemów Informatycznych,

m. Analizowanie raportów z wszelkich zdarzeń związanych z bezpieczeństwem Systemów Informatycznych,

n. Szkolenie pracowników z zakresu bezpieczeństwa informacji w Systemach Informatycznych.

7 Bezpieczeństwo zasobów ludzkich

Narodowe Centrum Badań i Rozwoju zapewnia kompetentnych pracowników do realizacji zadań wyznaczonych w procesach. Celem zapewnienia kompetentnej kadry jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów.

Zasoby ludzkie są ważnym czynnikiem analizowanym podczas przeprowadzania okresowej analizy ryzyka.

7.1 Obsada stanowisk odpowiedzialnych za bezpieczeństwo informacji i systemów

Osoby mające za zadanie nadzorować bezpieczeństwo informacji i systemów informatycznych powinny:

1. Spełniać kryteria określone w Ustawie o ochronie danych osobowych.
2. Posiadać przeszkolenie w zakresie Systemu Zarządzania Bezpieczeństwem Informacji w Narodowym Centrum Badań i Rozwoju.
3. Posiadać doświadczenie w zakresie zarządzania bezpieczeństwem informacji.

7.2 Szkolenia osób zaangażowanych w proces przetwarzania informacji

Każda osoba zaangażowana w proces przetwarzania informacji w NCBR odbywa szkolenie z zakresu:

1. Zasad bezpieczeństwa informacji obowiązujących w NCBR.
2. Zagrożeń bezpieczeństwa informacji.
3. Skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej.
4. Stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich.

Pracownicy/współpracownicy są okresowo szkoleni z zagadnień bezpieczeństwa informacji.

Szczegółowe regulacje dotyczące prowadzenia szkoleń zostały opisane w wewnętrznych regulacjach NCBR.

7.3 Zarządzanie bezpieczeństwem zasobów ludzkich

W zakresie zarządzania bezpieczeństwem zasobów ludzkich, który służy zapewnieniu odpowiedniej ochrony zasobów, funkcjonuje sposób postępowania przed nawiązaniem zatrudnienia/współpracy, w jego trakcie oraz na zakończenie.

7.3.1 Przekazywanie informacji o zmianach w zatrudnieniu

Dział Zarządzania Zasobami Ludzkimi (DZL) oraz KKO informuje w formie pisemnej Administratora Bezpieczeństwa Informacji oraz Sekcję Teleinformatyki o zmianach w zakresie:

DZL:

1. Przyjęcia do pracy nowego pracownika/współpracownika.
2. Odejściu z pracy/zakończeniu współpracy.
3. Rozpoczęciu i zakończeniu współpracy w ramach praktyk, stażu, umowy zlecenia.

KKO:

1. Rozpoczęciu urlopu macierzyńskiego/wychowawczego i powrocie z tego urlopu.
2. Rozpoczęciu i powrocie z długoterminowego zwolnienia lekarskiego.
3. Rozpoczęciu i powrocie z dłuższej nieobecności niż 30 dni kalendarzowych.
4. Zmianie stanowiska lub komórki organizacyjnej.

7.3.2 Przed zatrudnieniem

Stosowane są następujące zasady przed rozpoczęciem wykonywania obowiązków służbowych:

1. Pracownik/współpracownik, nie będący jeszcze osobą upoważnioną, przebywając na terenie NCBR nie powinien pozostawać bez nadzoru osoby upoważnionej (przełożonego lub osoby przez niego wyznaczonej).
2. Przed przystąpieniem do wykonywania zadań pracownik/współpracownik podpisuje zobowiązanie do zachowania poufności zawarte w upoważnieniu do przetwarzania danych osobowych wydawanym przez ABI.
3. Przed przystąpieniem do wykonywania zadań pracownik/współpracownik zostaje przeszkolony w zakresie przetwarzania danych osobowych oraz otrzymuje upoważnienie do przetwarzania informacji oraz danych osobowych w NCBR.
4. Przed przystąpieniem do wykonywania zadań pracownik/współpracownik zapoznaje się z obowiązującymi regulacjami wewnętrznymi, a w szczególności z ***Regulaminem Użytkownika Systemu Informatycznego Narodowego Centrum Badań i Rozwoju***. Fakt zapoznania się z dokumentami powinien zostać potwierdzony własnoręcznym podpisem pracownika na oświadczeniu. Oświadczenie jest przechowywane przez Sekcję Teleinformatyki.

7.3.3 W trakcie zatrudnienia/współpracy

Proces nadawania nowych uprawnień, modyfikacji lub odbierania uprawnień realizowany jest na podstawie ***Procedury kontroli dostępu do systemu informatycznego Narodowego Centrum Badań i Rozwoju.***

Pracownicy/współpracownicy powinni być regularnie szkoleni i uświadamiani w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na 3 lata. Za szkolenia z zakresu bezpieczeństwa informacji odpowiada ABI.

Szkolenie dla pracowników z zakresu bezpieczeństwa informacji są przeprowadzane przez ABI każdorazowo po:

1. Zmianie przepisów dotyczących bezpieczeństwa informacji.

2. Wprowadzeniu istotnych zmian w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
3. Na wniosek Kierownika Komórki Organizacyjnej.

7.3.4 Zasady podczas zakończenia zatrudnienia

Proces odbierania uprawnień realizowany jest poprzez przez Sekcję Teleinformatyki na podstawie ***Procedury kontroli dostępu do systemu informatycznego Narodowego Centrum Badań i Rozwoju***.

8 Zarządzanie aktywami

W Narodowym Centrum Badań i Rozwoju zarządzanie aktywami jest realizowane w celu zapewnienia wymaganego poziomu bezpieczeństwa informacji. Aktywa to wszystko, co ma wartość dla NCBR, w szczególności aktywa informacyjne to wiedza lub dane, które posiadają wartość dla NCBR. Aktywa chronione dzielimy na dwie grupy: aktywa główne oraz aktywa wspomagające.

Aktywa główne:

1. Procesy i działania biznesowe.
2. Informacje.

Aktywa wspomagające:

1. Sprzęt.
2. Oprogramowanie.
3. Sieć.
4. Personel.
5. Siedziba.
6. Struktura organizacyjna.

Aktywa są chronione ze względu na wymagania wynikające z:

1. Przepisów prawa.
2. Warunków licencji.
3. Zapisów umów pomiędzy NCBR a podmiotami zewnętrznymi.
4. Regulacji wewnętrznych, z których wynika ochrona właściwych aktywów.

8.2 Zasady zarządzania aktywami informacyjnymi

Zarządzanie aktywami informacyjnymi w NCBR odbywa się zgodnie z zasadami:

1. Odpowiedzialności za aktywa. Określeni są właściciele wszystkich aktywów oraz jest im przydzielona odpowiedzialność za utrzymanie odpowiednich zabezpieczeń. Wdrożenie określonych zabezpieczeń jest delegowane przez właściciela, jednak pozostaje on nadal odpowiedzialny za właściwą ochronę aktywów.
2. Identyfikacji aktywów. Wszystkie aktywa są zidentyfikowane oraz jest sporządzony i utrzymywany spis wszystkich ważnych aktywów.

3. Akceptowalnego użycia aktywów. W dokumentach SZBI są określone zasady dopuszczalnego korzystania z informacji i zasobów związanych z przetwarzaniem informacji, które są wdrożone do stosowanie przez Dyrektora Centrum.
4. Klasyfikacji informacji. Określona jest metoda oraz sposób klasyfikacji informacji odzwierciedlający wymagania ochrony informacji na odpowiednim poziomie.
5. Oznaczania informacji. Stosowane są regulacje wewnętrzne wyznaczające zasady oznaczanie informacji i postępowania z nimi.

Zarządzanie aktywami informacyjnymi odbywa się zgodnie z postanowieniami ***Procedury identyfikacji i klasyfikacji aktywów oraz zarządzania ryzykiem w Narodowym Centrum Badań i Rozwoju***. Dla poszczególnych rodzajów informacji określone są szczegółowe zasady postępowania oraz grupy pracowników posiadające do nich dostęp.

8.3 Rodzaje przetwarzanych informacji

W Narodowym Centrum Badań i Rozwoju poszczególne informacje są chronione na podstawie przepisów prawa. W oparciu o wymagania prawne nakładane na ochronę aktywów informacyjnych dokonano podziału na właściwe klasy chronionych informacji. Najważniejsze grupy informacji objęte wymaganiami to:

1. Dane osobowe.
2. Informacje niejawne.
3. Informacje publiczne.
4. Informacje finansowe.
5. Informacje stanowiące Tajemnice Przedsiębiorstwa, w szczególności:
   a. informacje występujące w procesie wnioskowania o przyznanie dofinansowania:
   b. informacje występujące w procesie nadzoru merytorycznego i finansowego nad umowami objętymi dofinansowaniem,
   c. informacje występujące na Wykazie aktywów informacyjnych, oznaczone jako „Tajemnica Przedsiębiorstwa”.

8.3.2 Dane osobowe

Ochrona danych osobowych w NCBR realizuje wymogi następujących aktywów prawnych:

1. Ustawia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. Dz. U. z 2014 r. poz. 1182, 1662).
2. Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

Informacje do użytku wewnętrznego i do użytku służbowego należy chronić pod względem utrzymania odpowiedniego poziomu poufności, integralności i dostępności.

Ochrona danych osobowych prowadzona jest zgodnie z ***Polityką Bezpieczeństwa Danych Osobowych w Narodowym Centrum Badań i Rozwoju*** oraz ***Polityką Bezpieczeństwa Systemu Informatycznego w Narodowym Centrum Badań i Rozwoju***, także w ramach systemu definiowanego przez niniejszą ***Politykę Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju***.

8.3.3 Informacje niejawne

Ochrona informacji niejawnych w Narodowym Centrum Badań i Rozwoju realizuje wymogi następujących aktywów prawnych:

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228).

Za organizację systemu ochrony informacji niejawnych w NCBR odpowiada Sekcja Ochrony Informacji Niejawnych i Danych Osobowych (SNO), który posiada uprawnienia oraz realizuje zadania określone w przepisach o ochronie informacji niejawnych i w sprawach merytorycznych podlega bezpośrednio Głównemu Administratorowi Informacji.

Informacje do użytku wewnętrznego i do użytku służbowego należy chronić pod względem utrzymania odpowiedniego poziomu poufności, integralności i dostępności.

Informacje niejawne posiadają własny, niezależny od definiowanego przez niniejszą politykę system ochrony zgodny z wymaganiami ustawy o ochronie informacji niejawnych.

8.3.4 Informacje publiczne

Ochrona informacji publicznych w NCBR realizuje wymogi następujących aktywów prawnych:

1. Ustawa o dostępie do informacji publicznej z dnia 6 września 2001 roku o dostępie do informacji publicznych (Dz. U. Nr 112, poz. 1198 z późniejszymi zmianami).

Informacje publiczne należy chronić pod względem utrzymania odpowiedniego poziomu integralności oraz dostępności.

Zasady przetwarzania informacji publicznych są realizowane zgodnie z regulacjami wewnętrznymi w NCBR, a ochrona jest prowadzona zgodnie z niniejszą ***Polityką Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju***.

8.3.5 Informacje finansowe

Ochrona informacji finansowych w NCBR realizuje wymogi następujących aktywów prawnych:

1. Ustawa z dnia 29 września 1994 roku o rachunkowości (Dz.U.2013.330 j.t. z późniejszymi zmianami).
2. Ustawa z dnia 27 sierpnia 2009 roku o finansach publicznych (Dz. U. z 2009 nr 157, poz. 1240 z późniejszymi zmianami).

Zasady przetwarzania informacji finansowych określone są w dokumencie ***Polityka rachunkowości w Narodowym Centrum badań i Rozwoju***, a ochrona jest prowadzona zgodnie z ***Polityką Bezpieczeństwa Danych Osobowych w Narodowym Centrum Badań i Rozwoju*** **i niniejszą** ***Polityką Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju*****.**

8.4 Zasady klasyfikacji informacji

Wszelkie informacje wytworzone, przekazywane i przetwarzane w NCBR, nie oznaczone jako należące do osób trzecich, stanowią własność Centrum i podlegają ochronie.

Podział na klasy aktywów informacyjnych jest następujący:

1. Wartość WA od 0 do 3 – poziom ochrony I
2. Wartość WA od 4 do 6 – poziom ochrony II
3. Wartość WA od 7 do 9 – poziom ochrony III

4. Wartość WA od 10 do 12 – poziom ochrony IV

Za właściwe sklasyfikowanie dokumentu odpowiada jego właściciel i tylko on może dokonać zmiany w klasyfikacji.

Wycena aktywów informacyjnych, w szczególności określenie wartości aktywa WA, odbywa się zgodnie z postanowieniami ***Procedury identyfikacji i klasyfikacji aktywów oraz zarządzania ryzykiem w Narodowym Centrum Badań i Rozwoju***.

8.4.2 Sposób postępowania z informacjami

1. Informacje o poziomie ochrony I to informacje, których ujawnienie, uszkodzenie lub utrata nie powoduje strat dla NCBR.
2. Informacje o poziomie ochrony II to informacje, których ujawnienie, uszkodzenie lub utrata może wpłynąć na działalność NCBR i spowodować straty.
3. Informacje o poziomie III to informacje, których ujawnienie, uszkodzenie lub utrata może spowodować naruszenie przepisów prawa i spowodować straty dla NCBR.
4. Informacje o poziomie ochrony IV to informacje o najwyższym stopniu ochrony, które należy chronić na najwyższym poziomie.

W ramach każdego z poziomów ochrony, zdefiniowane zostały zasady postępowania z przypisanymi do nich grupami informacji. Do zasad tych zalicza się sposoby ich oznaczania, przechowywania, kopiowania, niszczenia oraz udostępniania wewnątrz i na zewnątrz NCBR. Stanowią one minimalne wymagania bezpieczeństwa dla przetwarzania grup informacji, uzupełniające wymagania wynikają ze stosowania przepisów prawa, przestrzegania warunków zdefiniowanych w umowach czy z przepisów wewnętrznych. Poszczególne informacje mogą mieć nałożone dodatkowe wymagania w zakresie zasad postępowania (np. oznaczanie czy terminy archiwizacji), określone szczegółowo przez ich właścicieli i odpowiednie regulacje prawne oraz wewnętrzne.

Poniższe tabele przedstawiają sposoby postępowania z klasami informacji na zdefiniowanych poziomach ochrony. Dla informacji w postaciach innych niż papierowa lub elektroniczna, zasady postępowania stosuje się odpowiednio.

Poziom ochrony I	
Informacje w postaci papierowej	
Oznaczanie	Nie określa się zasad oznaczania.
Przechowywanie	Nie określa się zasad przechowywania.
Kopiowanie	Nie określa się zasad kopiowania.
Niszczenie	Nie określa się zasad niszczenia.
Przekazywanie wewnątrz	Nie określa się zasad przekazywania.
Przekazywanie na zewnątrz	Nie określa się zasad przekazywania.
Wynoszenie informacji	Nie określa się zasad wynoszenia informacji.
Informacje w postaci elektronicznej	
Oznaczanie	Nie określa się zasad oznaczania.
Przechowywanie	Nie określa się zasad przechowywania.

Kopiowanie	Nie określa się zasad kopiowania.
Niszczenie	Nie określa się zasad niszczenia.
Przekazywanie wewnątrz	Nie określa się zasad przekazywania.
Przekazywanie na zewnątrz	Nie określa się zasad przekazywania.
Wynoszenie informacji	Nie określa się zasad wynoszenia informacji.
Poziom ochrony II	
Informacje w postaci papierowej	
Oznaczanie	Nie określa się zasad oznaczania.
Przechowywanie	W zamkniętych pomieszczeniach.
Kopiowanie	Nie określa się zasad kopiowania.
Niszczenie	W niszczarkach do dokumentów.
Przekazywanie wewnątrz	Za zgodą bezpośredniego przełożonego.
Przekazywanie na zewnątrz	Za zgodą bezpośredniego przełożonego.
Wynoszenie informacji	Za zgodą bezpośredniego przełożonego.
Informacje w postaci elektronicznej	
Oznaczanie	Nie określa się zasad oznaczania.
Przechowywanie	Nośniki, na których zapisane zostały kopie zapasowe powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób trzecich oraz w sposób uniemożliwiający jednoczesne zniszczenie kopii roboczych oraz zapasowych; Pozostałe nośniki należy przechowywać w zamkniętych pomieszczeniach lub w zamykanych meblach biurowych lub o wyższym stopniu zabezpieczenia.
Kopiowanie	Nie określa się zasad kopiowania.
Niszczenie	W przypadku nośników jednokrotnego zapisu należy zniszczyć w sposób uniemożliwiający odtworzenie zapisanych danych.
Przekazywanie wewnątrz	Za zgodą bezpośredniego przełożonego.
Przekazywanie na zewnątrz	Za zgodą bezpośredniego przełożonego.
Wynoszenie informacji	Za zgodą bezpośredniego przełożonego. Wynoszenie informacji w postaci elektronicznej może się odbywać jedynie na służbowych nośnikach lub komputerach przenośnych na zasadach określonych w Polityce Bezpieczeństwa Informacji.
Poziom ochrony III	
Informacje w postaci papierowej	

Oznaczanie	Nie określa się zasad oznaczania.
Przechowywanie	W zamkniętych pomieszczeniach i w zamykanych meblach biurowych.
Kopiowanie	Za zgodą właściciela informacji.
Niszczenie	W niszczarkach do dokumentów minimum P-2 (zgodnie z DIN 66399).
Przekazywanie wewnątrz	Za zgodą właściciela informacji. Podczas przekazywania dokumentów wewnątrz Centrum należy jednoznacznie określić ich odbiorcę.
Przekazywanie na zewnątrz	Za zgodą właściciela informacji oraz bezpośredniego przełożonego.
Wynoszenie informacji	Za zgodą właściciela informacji oraz bezpośredniego przełożonego.
Informacje w postaci elektronicznej	
Oznaczanie	Nie określa się zasad oznaczania.
Przechowywanie	Nośniki, na których zapisane zostały kopie zapasowe powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób trzecich oraz w sposób uniemożliwiający jednoczesne zniszczenie dokumentów roboczych oraz ich kopii zapasowych; Pozostałe nośniki należy przechowywać w meblach biurowych o solidnej konstrukcji zamykanych na klucz, w szafach metalowych bądź w sejfach. Dane przechowywane na nośnikach zewnętrznych należy przechowywać w sposób zabezpieczony przed dostępem osób trzecich: hasłem dostępu, zaszyfrowane lub zamknięte (np. w kopercie bezpiecznej).
Kopiowanie	Za zgodą właściciela informacji.
Niszczenie	W przypadku nośników jednokrotnego zapisu należy zniszczyć w sposób uniemożliwiający odtworzenie zapisanych danych. W pozostałych przypadkach należy niszczyć dane zgodnie z zasadami bezpiecznego kasowania danych z danego typu nośnika (np. przy wykorzystaniu specjalistycznego oprogramowania zapewniającego co najmniej pięciokrotne nadpisanie danych).
Przekazywanie wewnątrz	Za zgodą właściciela informacji. W przypadku przekazywania informacji przy wykorzystaniu pamięci przenośnych (np. pendrive), należy stosować wyłącznie nośniki posiadające zabezpieczenie kryptograficzne danych. Podczas wymiany informacji w obrębie sieci Narodowego Centrum Badań i Rozwoju szyfrowanie danych nie jest wymagane.
Przekazywanie na zewnątrz	Za zgodą właściciela informacji. Z wykorzystaniem Internetu co najmniej w postaci zabezpieczonej hasłem lub zaszyfrowanej, gdzie hasło przekazujemy za pomocą osobnej wiadomości np. drogą telefoniczną lub przy użyciu wiadomości SMS lub w inny, adekwatny sposób.

Wynoszenie informacji	Za zgodą właściciela informacji i bezpośredniego przełożonego. Wynoszenie informacji w postaci elektronicznej może się odbywać jedynie na służbowych nośnikach lub komputerach przenośnych na zasadach określonych w Polityce Bezpieczeństwa Informacji.

Poziom ochrony IV	
Informacje w postaci papierowej	
Oznaczanie	Oznaczamy zgodnie z RWA. Dokumenty oznaczane są od momentu rozpoczęcia tworzenia informacji.
Przechowywanie	W meblach biurowych o solidnej konstrukcji zamykanych na klucz, w szafach metalowych bądź w sejfach.
Kopiowanie	Za zgodą właściciela informacji.
Niszczenie	Za zgodą właściciela informacji. Niszczenie w niszczarkach minimum P-3 (zgodnie z DIN 66399). Niszczenie pod nadzorem osoby upoważnionej, potwierdzone protokołem zniszczenia.
Przekazywanie wewnątrz	Za zgodą właściciela informacji. W teczkach lub w inny sposób zabezpieczone przed przypadkowym zapoznaniem się z treścią.
Przekazywanie na zewnątrz	Za zgodą właściciela informacji. Oznaczamy dodatkową klauzulą „Dokument poufny Narodowego Centrum Badań i Rozwoju”.
Wynoszenie informacji	Za zgodą właściciela informacji. Przenoszenie dokumentów w opieczętowanych kopertach lub w inny sposób gwarantujący zabezpieczenie przed dostępem osób trzecich.
Informacje w postaci elektronicznej	
Oznaczanie	Oznaczamy zgodnie z regulacjami wewnętrznymi. Wszystkie nośniki przenośne jak i dokumenty są oznaczane od momentu rozpoczęcia tworzenia informacji.
Przechowywanie	Za zgodą właściciela informacji. Tylko na serwerach w sieci wewnętrznej Narodowego Centrum Badań i Rozwoju.
Kopiowanie	Za zgodą właściciela informacji.
Niszczenie	Za zgodą właściciela informacji.

	Przy wykorzystaniu specjalistycznego oprogramowania zapewniającego co najmniej siedmiokrotne nadpisanie danych (dla dysków twardych) lub poprzez fizyczne zniszczenie nośnika tj. zmielenie, spalenie. Niszczenie odbywa się pod nadzorem osoby upoważnionej, potwierdzone protokołem zniszczenia.
Przekazywanie wewnątrz	Za zgodą właściciela informacji. Informacji nie przesyła się pocztą elektroniczną.
Przekazywanie na zewnątrz	Za zgodą właściciela informacji. Informacji nie przesyła się pocztą elektroniczną.
Wynoszenie informacji	Za zgodą właściciela informacji. Wynoszenie informacji w postaci elektronicznej może odbywać się jedynie na służbowych nośnikach danych posiadających zabezpieczenia kryptograficzne danych.

9 Kontrola dostępu

Zarządzanie kontrolą dostępu jest realizowane poprzez:

1. Nadzór nad dostępem do budynków i pomieszczeń. Szczegółowe zasady kontroli dostępu zostały opisane w ***Procedurze kontroli dostępu do budynków i pomieszczeń Narodowego Centrum Badań i Rozwoju.***
2. Kontrolę dostępu do obszarów przetwarzania danych osobowych. Szczegółowe zasady kontroli dostępu zostały opisane w ***Procedurze kontroli dostępu do budynków i pomieszczeń Narodowego Centrum Badań i Rozwoju oraz Regulaminie Użytkownika Systemu Informatycznego.***
3. Kontrolę dostępu do sieci i systemów informatycznych. Szczegółowe zasady kontroli dostępu zostały opisane w ***Procedurze kontroli dostępu do systemu informatycznego Narodowego Centrum Badań i Rozwoju***
4. Zasady nadawania uprawnień dla użytkowników. Szczegółowe zasady nadawania uprawnień dla użytkowników zostały opisane w ***Procedurze kontroli dostępu do systemu informatycznego Narodowego Centrum Badań i Rozwoju***
5. Zarządzanie hasłami i innymi danymi uwierzytelniającymi. Szczegółowe zasady zarządzania hasłami i innymi danymi uwierzytelniającymi zostały opisane w ***Procedurze kontroli dostępu do systemu informatycznego Narodowego Centrum Badań i Rozwoju***
6. Politykę czystego biurka. Szczegółowe wymagania polityki czystego biurka zostały zapisane w ***Regulaminie Użytkownika Systemu Informatycznego Narodowego Centrum Badań i Rozwoju***
7. Politykę czystego ekranu. Szczegółowe wymagania polityki czystego biurka zostały zapisane w ***Regulaminie Użytkownika Systemu Informatycznego Narodowego Centrum Badań i Rozwoju***
8. Kontrolę systemów i aplikacji. Szczegółowe wymagania opisane zostały w ***Polityce Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju***
9. Zabezpieczenia kryptograficzne. Szczegółowe wymagania opisane zostały w ***Polityce Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju***

10 Bezpieczeństwo fizyczne i środowiskowe

Narodowe Centrum Badań i Rozwoju dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego i środowiskowego w celu zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub zakłóceniami. Najistotniejsze jest zapewnienie wszystkich trzech podstawowych aspektów bezpieczeństwa informacji: poufności danych oraz integralności i dostępności. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z wyznaczeniem stref bezpieczeństwa, zasadami pracy oraz administrowaniem prawami dostępu do nich. Kluczowe systemy techniczne i teleinformatyczne wyposażone są w systemy utrzymujące optymalne warunki środowiskowe i podtrzymujące zasilanie.

Szczegóły opisane zostały w dokumencie ***Procedura kontroli dostępu do budynków i pomieszczeń Narodowego Centrum Badań i Rozwoju, Polityce Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju*** *oraz odpowiednich zasadach bezpieczeństwa informacji*.

11 Zarządzanie systemami i sieciami

Narodowe Centrum Badań i Rozwoju stosuje zasady utrzymania oraz użytkowania Systemów Informatycznych. Bezpieczeństwo Systemów Informatycznych jest zapewnianie poprzez stosowanie odpowiednich zabezpieczeń w odniesieniu do poufności, integralności i dostępności przetwarzanej w nich informacji.

W Narodowym Centrum Badań i Rozwoju stosowane są następujące zasady bezpieczeństwa w celu skutecznej realizacji powyżej wymienionych założeń:

1. Wszystkie Systemy Informatyczne przed dopuszczeniem do wykorzystania muszą spełniać minimalne wymagania bezpieczeństwa i standardy wymienione w ***Polityce Bezpieczeństwa Systemu Informatycznego.***
2. Wdrażanie, eksploatacja oraz utrzymanie Systemów Informatycznych jest realizowane za pomocą kompetentnych i świadomych zagadnień bezpieczeństwa pracowników oraz firm zewnętrznych.
3. Prowadzona jest kontrola wprowadzanych zmian zgodnie z ***Procedurą zarządzania zmianami oraz konfiguracją systemu informatycznego.***
4. Prace testowe i rozwojowe są prowadzone na oddzielnych urządzeniach i środowiskach; prowadzenie prac rozwojowych i testowych może być realizowane przez firmy zewnętrzne na podstawie odpowiednich umów dotyczących rozwoju i utrzymania oprogramowania i aplikacji.
5. Nadzorowanie usług dostarczanych przez strony trzecie a w szczególności wszelkich wprowadzanych do nich zmian.
6. Stosowana jest ochrona przed kodem złośliwym oraz kodem mobilnym.
7. Kopie zapasowe są tworzone zgodnie z przyjętymi zasadami oraz stosownie do tych zasad testowane.
8. Stosowanie zasad postępowania z nośnikami danych opisane w ***Polityce Bezpieczeństwa Systemu Informatycznego.***
9. Monitorowanie aktywów informacyjnych oraz zasobów Systemów Informatycznych w celu wykrycia naruszeń bezpieczeństwa informacji oraz ich zapobieganiu.
10. W sytuacji wykrycia incydentu naruszenia bezpieczeństwa stosuje się wdrożone zasady postępowania oraz mechanizmy reagowania na incydenty.

Szczegółowe zasady zarządzania systemami i sieciami opisane zostały w dokumencie ***Polityka Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju.***

12 Pozyskiwanie, rozwój i utrzymanie systemów informatycznych

Narodowe Centrum Badań i Rozwoju zapewnia, że pozyskanie, rozwój i utrzymanie systemów informatycznych jest realizowane w sposób gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa.

Powyższy cel pozyskiwania, rozwoju i utrzymania systemów informatycznych uzyskuje się w NCBR poprzez:

1. Stosowanie wymagań bezpieczeństwa informacji podczas zakupu lub budowy nowych Systemów Informatycznych.
2. Testowanie bezpieczeństwa nowych systemów przed dopuszczeniem ich do eksploatacji.
3. Nadzorowanie dostępu do kodów źródłowych oprogramowania.
4. Dbałość o aktualizacje oprogramowania.
5. Procedury kontroli zmian oprogramowania.
6. Minimalizowanie ryzyka utraty informacji w wyniku awarii.
7. Ochronę przed błędami, utratą, nieuprawnioną modyfikacją.
8. Stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa.
9. Zapewnienie bezpieczeństwa plików systemowych.
10. Redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych Systemów Informatycznych.
11. Niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności Systemów Informatycznych na możliwość naruszenia bezpieczeństwa.
12. Kontrolę zgodności Systemów Informatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju i utrzymania systemów informatycznych odpowiedzialny jest Administrator Bezpieczeństwa Systemów Informatycznych.

Szczegółowe regulacje opisane zostały w ***Polityce Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju.***

13 Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Zarządzanie zdarzeniami i incydentami związanymi z bezpieczeństwem informacji odbywa się w ramach procesu zarządzania incydentem w NCBR.

W celu skutecznego zarządzania incydentem stosuje się zasady:

1. Wszyscy pracownicy NCBR są zapoznani z zasadami informowania o incydentach naruszenia bezpieczeństwa.
2. Wszyscy pracownicy NCBR są zobowiązani do informowania o incydentach naruszenia bezpieczeństwa.

3. W przypadku wystąpienia klęski żywiołowej lub aktu terroru w pierwszej kolejności powiadamiane są właściwe służby, następnie ochrona budynku oraz Pełnomocnik ds. SZBI.
4. W przypadku zauważenia próby włamania, kradzieży dokumentów lub sprzętu oraz wszelkich prób niszczenia mienia powiadamiana jest ochrona budynku oraz bezpośredni przełożony lub osoba go zastępująca.
5. Jeżeli zostanie wykryty incydent związany z naruszeniem bezpieczeństwa informacji bezzwłocznie jest informowany o tym fakcie Pełnomocnik ds. SZBI.
6. Incydenty są rejestrowane w formie elektronicznej przez Pełnomocnika ds. SZBI.
7. Ochrona obiektu rejestruje incydenty we własnych dokumentach.

Szczegółowe regulacje opisane zostały w dokumencie ***Procedura zarządzania incydentami naruszenia bezpieczeństwa informacji w Narodowym Centrum Badań i Rozwoju.***

14 Zarządzanie ciągłością działania

Narodowe Centrum Badań i Rozwoju zapewnia ciągłość działania usług związanych z przetwarzaniem informacji. Dla poszczególnych obszarów i systemów krytycznych tworzone są plany postępowania w sytuacjach awaryjnych i kryzysowych. Celem stosowania zarządzania ciągłością działania jest przeciwdziałanie przerwom w funkcjonowaniu NCBR.

W celu skutecznego zarządzania ciągłością działania stosowane są zasady:

1. Opracowanie i wdrożenie planów ciągłości działania dla krytycznych elementów Systemu Informatycznego NCBR.
2. Wskazanie osób odpowiedzialnych za utrzymanie ciągłości działania Systemów Informatycznych.
3. Podział odpowiedzialności za zarządzanie ciągłością działania.

Szczegółowe regulacje opisane zostały w dokumencie ***Procedura zachowania ciągłości działania systemu informatycznego w Narodowym Centrum Badań i Rozwoju.***

15 Zgodność

Zgodność z przepisami obowiązującego prawa, warunkami przyjętych umów, zapisami odpowiednich norm oraz wewnętrznymi regulacjami jest realizowana poprzez stosowanie zasad:

1. Identyfikację wymagań prawnych w odniesieniu do bezpieczeństwa informacji.
2. Wskazanie osób odpowiedzialnych za weryfikację spełnienia wymagań bezpieczeństwa informacji.
3. Prowadzenie audytów wewnętrznych oraz zewnętrznych.
4. Nadzór nad zgodnością stosowanych urządzeń Systemu Informatycznego.

Szczegóły opisane zostały w regulacjach Systemu Zarządzania Bezpieczeństwem Informacji oraz innych wewnętrznych regulacjach NCBR.

16 Zasady rozpowszechniania

Z Polityką Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju powinna się zapoznać kadra kierownicza oraz pracownicy/współpracownicy, a także inne osoby mające dostęp do informacji (stażyści

odbywający staż, praktykanci odbywający praktykę, pracownicy firm zewnętrznych realizujących prace na podstawie odpowiednich umów).

Niniejszy dokument może być udostępniony w celu zapoznania się i zgodnego postępowania tylko uprawnionym podmiotom zewnętrznym.

Nadzór nad przestrzeganiem Polityki Bezpieczeństwa Informacji oraz dokumentów związanych pełni Główny Administrator Informacji.

Bieżący nadzór nad wypełnianiem zaleceń bezpieczeństwa pełni Pełnomocnik ds. SZBI.

Postępowanie niezgodne z niniejszą Polityką Bezpieczeństwa Informacji wiąże się ze skutkami prawnymi przewidzianymi w Regulaminie Pracy.

Zmiany w niniejszym dokumencie wprowadzane są zgodnie z ***Procedurą PZ3-4 Nadzór nad dokumentacją opisująca procesy.***

17 Odstępstwa od reguł ochrony

Odstąpienie od zasad opisanych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji jest możliwe wyłącznie po spełnieniu poniższych warunków:

1. Zwrócić się z pisemnym wnioskiem o odstąpienie od reguł ochrony i uzasadnić we wniosku powód odstąpienia od przyjętych zasad bezpieczeństwa.
2. Otrzymanie pisemnej decyzji Głównego Administratora Informacji.
3. Postępować zgodnie z wymogami obowiązującego prawa.

18 Wykaz aktów prawnych

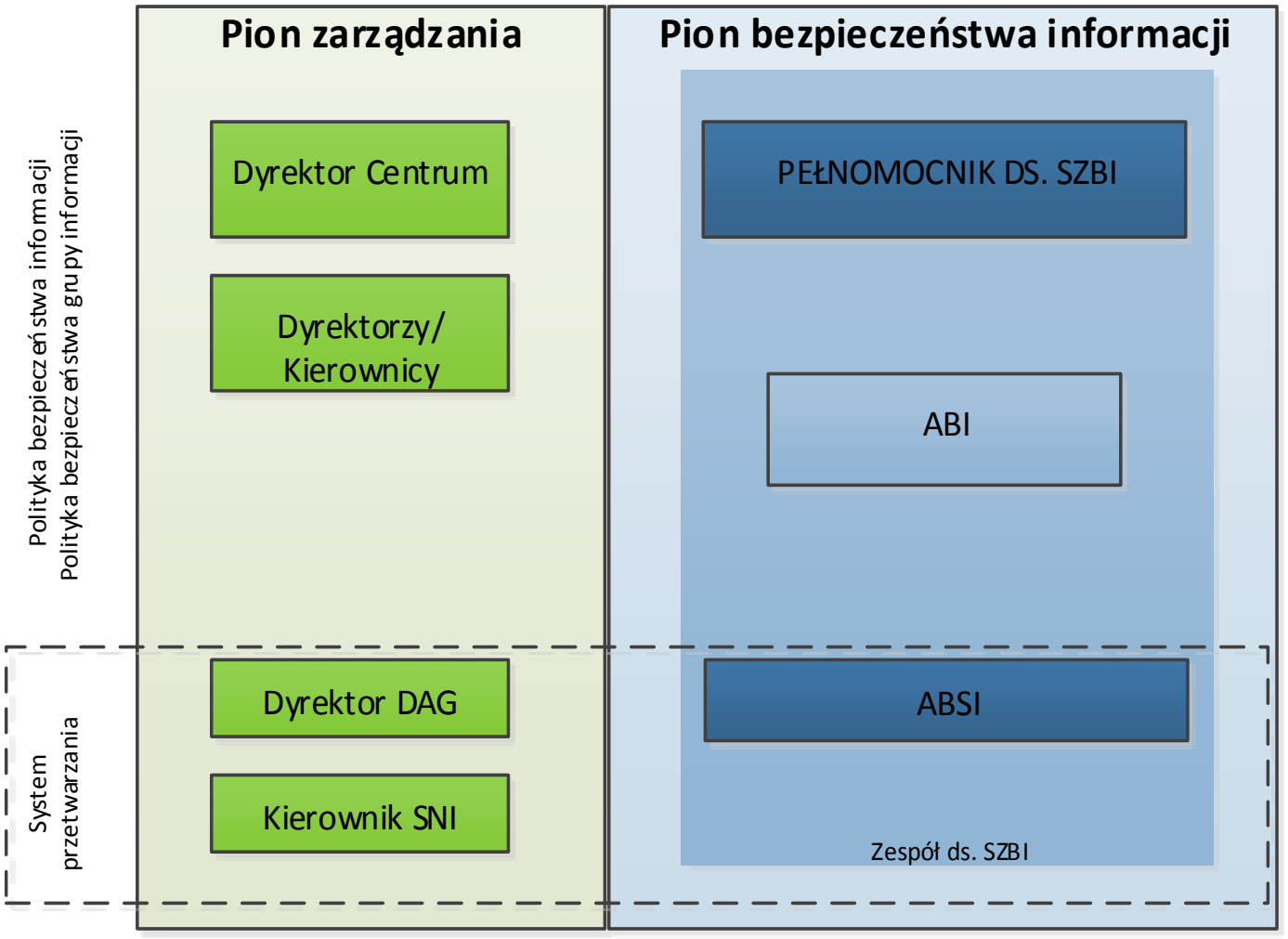
Akty prawne, z których wynikają zasady ochrony informacji stosowane w Narodowym Centrum Badań i Rozwoju, są wymienione w dokumencie ***Wykaz aktów prawnych w bezpieczeństwie informacji Narodowego Centrum Badań i Rozwoju*.**

19 Lista dokumentów związanych

1. Norma PN-ISO/IEC 27001:2014-12 Technika informatyczna - Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania
2. Wspólny słownik pojęć używanych w Narodowym Centrum Badań i Rozwoju.

20 Załączniki

20.1 Załącznik nr 1. Relacje pomiędzy rolami.



21 Rejestr zmian

Lp.	Data	Opis	Dotyczy stron(y)	Wprowadzający zmianę
