Regulamin Ochrony Informacji dla wykonawcy Narodowego Centrum Badań i Rozwoju

Opracował:	Sprawdził:	Zatwierdził:
Piotr Zerhau Dyrektor DSI Podpis:	Zbigniew Zieliński Dyrektor DAZ Podpis:	Wojciech Kamieniecki Dyrektor 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. Inspektor Ochrony Danych.
2. Administrator Bezpieczeństwa Systemu Informatycznego.

Spis treści

1 Cel

Celem dokumentu jest:

1.1 Określenie minimalnych wymagań w zakresie bezpieczeństwa informacji dla wykonawców.

1.2 Określenie minimalnych wymagań w zakresie zabezpieczeń systemu informatycznego.

2 Zakres

2.1 Postanowienia niniejszego dokumentu stosują wszyscy wykonawcy, którzy realizują prace na rzecz Centrum, związane z przetwarzaniem aktywów informacyjnych Centrum.

2.2 Postanowienia niniejszego ROI należy stosować we wszystkich umowach z wykonawcami, których przedmiot jest związany z ochroną informacji.

3 Postanowienia ogólne

3.1 ROI określa zakres obowiązków i odpowiedzialności wykonawców w zakresie bezpieczeństwa informacji. ROI obejmuje swym zakresem wszystkich wykonawców, mających dostęp do systemów informatycznych Centrum. ROI jest syntezą informacji zawartych w Polityce Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju, Polityce Bezpieczeństwa Systemu Informatycznego Narodowego Centrum Badań i Rozwoju.

3.2 Wykonawca musi spełniać wymagania niniejszego ROI przed uzyskaniem dostępu do systemu informatycznego Centrum.

3.3 Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych, których administratorem jest Dyrektor Centrum, wykonawca musi spełnić warunki:

a. podpisać zobowiązanie do zachowania poufności przetwarzanych danych na wzorze, będącym załącznikiem nr 1 do ROI.

b. w przypadku powierzenia przetwarzania danych osobowych Centrum, podpisać umowę powierzenia przetwarzania danych osobowych zgodnie ze wzorem obowiązującym w Centrum.

3.4 Pracownicy wykonawcy realizujący prace zgodnie z zawartą umową mogą przebywać na terenie Centrum jedynie pod nadzorem pracownika Centrum lub pracowników ochrony budynku Roma Office Center.

W przypadku, gdy zlecenie będzie wykonywane po godzinach pracy Centrum lub w dni wolne od pracy, kierownik KO nadzorujący bezpośrednio wykonywane prace musi zgłosić powyższy fakt Dyrektorowi DAZ. Dyrektor DAZ wystawia zlecenie na wykonanie prac i przekazuje informację o terminie i zakresie wykonywanych prac Kierownikowi Działu Technicznego Roma Office Center, który zawiadamia ochronę obiektu.

W zleceniu należy podać:

a. nazwę wykonawcy,
b. zakres wykonywanej pracy,
c. termin wykonania (data od-do, godzina od-do),
d. imię nazwisko, nr dowodu osobistego pracowników wykonujących prace,
e. imię nazwisko, tel. osoby nadzorującej prace w Centrum,
f. nr rejestracyjny samochodów – w przypadku konieczności wyrażenia zgody na wjazd na parking służbowy.

Klucze do pomieszczeń wydaje pracownik DAZ. Przebywanie oraz wykonywanie pracy pod nieobecność pracowników Centrum możliwe jest jedynie pod nadzorem pracowników ochrony.

4 Nadawanie, zmiana bądź odebranie uprawnień

4.1 W przypadku wykonawców zakres uprawnień w poszczególnych systemach i aplikacjach ustawia się adekwatnie do przedmiotu umowy i zakresu powierzonych danych osobowych.

4.2 Lista użytkowników ze strony wykonawcy powinna być dostarczona przez osoby wskazane w umowie jako odpowiedzialne za jej realizację.

4.3 Po każdej zmianie użytkowników ze strony wykonawcy, jest on zobowiązany do przekazania listy użytkowników ze wskazaniem zmian w ich zakresie uprawnień.

4.4 Rejestrowanie/wyrejestrowanie użytkowników wykonawcy systemu informatycznego Centrum oraz nadawanie/zmiana/odebranie uprawnień jest realizowane przez pracowników DSI zgodnie ze schematem postępowania:

a. Na podstawie postanowień umowy z wykonawcą a także w wyniku konsultacji z osobą wskazaną w umowie jako odpowiedzialną za jej realizację z ramienia Centrum, ABSI ustala niezbędny zakres uprawnień dla poszczególnych użytkowników będących przedstawicielami wykonawcy.

b. Z wnioskiem o nadanie/zmianę/odebranie uprawnień do systemu informatycznego występuje pracownik Centrum skazany w umowie z wykonawcą jako osoba odpowiedzialna za jej realizację z ramienia Centrum. Zakres uprawnień na wniosku musi być zgodny z zaleceniami ABSI, wniosek składany jest z zachowaniem regulacji wewnętrznych opisanych w dokumentach wewnętrznych Centrum.

c. Podczas rejestracji użytkownika będącego przedstawicielem wykonawcy nadawany jest unikalny identyfikator użytkownika oraz ustawiane jest hasło tymczasowe niezbędne do logowania po raz pierwszy do systemu informatycznego (hasła nadawane są zgodnie z zasadami opisanymi w niniejszej procedurze) dla użytkownika zewnętrznego systemu informatycznego.

d. O nadaniu/zmianie/odebraniu uprawnień właściwych identyfikatorów w odpowiednich systemach informatycznych i nadaniu właściwych uprawnień ABSI informuje wykonawcę za pośrednictwem pracownika Centrum wskazanego w umowie z wykonawcą jako odpowiedzialnego za realizację umowy z ramienia Centrum.

5 Metody i środki uwierzytelniania

Dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do systemu informatycznego.

Hasła użytkowników

5.1 Hasła użytkowników do systemów informatycznych powinny podlegać następującym zasadom:

a. hasło składa się z minimum 8 znaków,

b. hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np.!@#),

c. hasło musi być zmieniane minimum co 30 dni,

d. kolejne hasła muszą być różne, zapamiętywanych jest 6 ostatnich haseł,

e. hasła należy przechowywać w sposób gwarantujący ich poufność.

5.2 Zabrania się udostępniania haseł innym osobom.

5.3 Zabrania się tworzenia haseł na podstawie:

a. cech i numerów osobistych (np. dat urodzenia, imion itp.),

b. sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),

c. identyfikatora użytkownika.

5.4 Zabrania się tworzenia haseł łatwych do odgadnięcia.

5.5 Logowanie anonimowe do systemu informatycznego jest zabronione dla użytkowników.

5.6 Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora.

5.7 W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko użytkownikowi.

5.8 W przypadku systemów informatycznych, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego złożoności, obowiązkiem użytkownika jest zmiana hasła zgodnie z zasadami określonymi w powyższych punktach.

5.9 Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.

5.10 Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie użytkownikowi.

5.11 Hasła nie powinny być przechowywane w formie dostępnej dla osób nieupoważnionych:

a. w plikach,

b. na kartkach papieru w miejscach dostępnych dla osób trzecich,

c. w skryptach,

d. w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.

5.12 W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, hasła muszą być natychmiast zmienione przez użytkownika lub AS.

5.13 Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy również po upływie jego ważności.

5.14 Zmiany hasła dokonuje użytkownik. W przypadku, gdy użytkownik zapomniał hasła, właściwy AS ustawia hasło tymczasowe użytkownikowi z wymuszeniem jego zmiany podczas pierwszego logowania.

5.15 Hasła użytkowników nie powinny być przekazywane ani przesyłane za pomocą telefonu, faksu czy tez poczty elektronicznej w formie jawnej.

6 Dostęp zdalny

6.1 W DSI prowadzony jest elektroniczny wykaz osób i wykonawców posiadających dostęp zdalny do zasobów systemu informatycznego Centrum.

6.2 Dostęp zdalny wykonawców, możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym ROI.

6.3 Wykonawca we własnym zakresie udziela pełnomocnictw swoim pracownikom powierzając im zadania.

6.4 Dostępu zdalnego udziela się na zasadach i na czas określony zapisami umowy.

6.5 Zakres dostępu zdalnego może zostać ograniczony lub zwiększony decyzją ABSI, po przeanalizowaniu potrzeb określonych postanowieniami umowy z wykonawcą, a także w wyniku konsultacji z pracownikiem Centrum wskazanym w umowie jako osoba odpowiedzialna za jej realizację.

6.6 Pracownik Centrum wskazany w umowie z wykonawcą, jako osoba odpowiedzialna za jej realizację wnioskuje o dostęp zdalny w zakresie wskazanym przez ABSI a także zgodnie z wewnętrznymi regulacjami opisanymi w dokumentach Centrum.

6.7 W ramach dostępu zabrania się wykonawcy trwale usuwać dane, przeprowadzać jakiekolwiek operacje na dyskach mogące prowadzić do ich uszkodzenia lub utraty danych, w szczególności ich formatowania. Przedstawiciel wykonawcy wykonujący prace, przystępując do czynności, o których wie, że w konsekwencji doprowadzić one mogą do zniszczenia danych, musi poinformować przedstawiciela Centrum i dopiero po jego akceptacji może podjąć te czynności.

6.8 Dla środowisk produkcyjnych (oddanych do eksploatacji) wykonawca, przed przystąpieniem do prac, przedstawia scenariusz planowanych prac wraz z oceną ryzyka podejmowanych czynności. Wykonawca odpowiada za odstępstwa od przedstawionego scenariusza. Scenariusz powinien obejmować:

a. Kto będzie prowadził prace.

b. Kiedy, przewidywany czas trwania.

c. Zakres wykonywanych prac.

d. Informację czy wymagana jest przerwa w pracy użytkowników.

e. Potencjalne ryzyka podejmowanych czynności.

6.9 Pracownik lub przedstawiciel wykonawcy wykonujący prace, przystępując do czynności, co do których istnieje wysokie ryzyko utraty danych, informuje o ryzyku pracownika Centrum wskazanego w umowie z wykonawcą jako osoby odpowiedzialnej za jej realizację ABSI.

6.10 Po formalnej, pisemnej akceptacji ryzyka przez ABSI, pracownik wykonawcy może rozpocząć realizację czynności objętej wskazanym ryzykiem.

6.11 Wykonywanie prac polegających na standardowej obsłudze serwisowej, prac nad rozwojem programu będącego w fazie wdrażania nie wymaga każdorazowego ustalenia warunków realizacji czynności, będącej ich częścią. W ramach wykonywania tych czynności obowiązują warunki uzgodnione wcześniej. W szczególności nie wymagają każdorazowego ustalenia warunków realizacji te czynności, które wynikają z przedmiotu umowy i nie są objęte ryzykami opisanymi w pkt. 8-10. Wykonywanie czynności niestandardowych wymaga każdorazowo określenia warunków.

6.12 Zabrania się podejmowania czynności zmierzających do penetrowania zasobów sieci Centrum, chyba, że czynności dotyczą realizacji umowy na testy bezpieczeństwa, testy penetracyjne, itp. Każde przeprowadzenie testów bezpieczeństwa lub penetracyjnych musi być realizowane za uprzednią zgodą ABSI.

6.13 ABSI w porozumieniu z właściwymi administratorami ogranicza zasoby dostępne dla sesji zdalnej, do niezbędnego minimum, chyba, że wymagałoby to rozległej ingerencji w konfigurację urządzeń dostępowych.

6.14 ABSI wraz z właściwymi administratorami ustalają wymagane zasoby. Wykonawca zobowiązuje się do wykorzystywania tylko i wyłącznie ustalonych zasobów nawet, jeśli dostępne są inne niż tylko wymagane.

6.15 Na potrzeby realizacji umowy ABSI może udzielić dostępu zdalnego do następujących środowisk:

a. Testowych,

b. produkcyjnych.

6.16 Zabrania się dostępu zdalnego z komputerów dostępnych publicznie np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci miejskie, itp.

7 Zasady zabezpieczeń stacji roboczych

7.1 Do systemu informatycznego mogą być podłączane wyłącznie komputery i urządzenia zgodne z minimalnymi wymaganiami bezpieczeństwa, w szczególności:

a. System antywirusowy jest zainstalowany w systemie operacyjnym i jego sygnatury są aktualne.

b. System operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń.

c. Firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez użytkowników komputera.

d. Zainstalowane na komputerze oprogramowanie pochodzi z godnych zaufania źródeł.

e. Oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania.

f. Oprogramowanie nie łamie Ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r.

8 Stosowanie zabezpieczeń kryptograficznych

W celu ochrony poufności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne. Miejsca stosowania kryptografii powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi, w szczególności należy stosować zabezpieczenia kryptograficzne:

8.1 Na dyskach twardych komputerów przenośnych.

8.2 Na pendrive'ach.

8.3 Na nośnikach kopii zapasowych przechowywanych poza systemem informatycznym Centrum.

8.4 Na urządzeniach typu smartfon oraz tablet w aplikacjach, które przechowują dane objęte ochroną np. dane osobowe.

8.5 Tunelach VPN.

8.6 Wiadomościach poczty elektronicznej, w których przesyłane są dane objęte ochroną, w szczególności dane osobowe.

8.7 Zakres stosowanych rozwiązań kryptograficznych powinien obejmować minimum dane znajdujące się na nośnikach, które objęte są ochroną ze względu na wymagania utrzymania odpowiedniego poziomu poufności.

8.8 Rozwiązania kryptograficzne powinny wykorzystywać algorytm AES o długości klucza min. 128 bit.

9 Reagowanie na incydenty

9.1 Każde naruszenie bezpieczeństwa informacji należy każdorazowo zgłaszać do ABSI lub jeżeli naruszenie w jednoznaczny sposób dotyczy przetwarzania danych osobowych do bezpośredniego przełożonego oraz IOD. Zgłoszenia należy dokonać za pośrednictwem poczty elektronicznej, za potwierdzeniem odbioru na adres [helpdesk@ncbr.gov.pl] z tematem wiadomości „Naruszenie bezpieczeństwa informacji".

9.2 Jeśli zdarzenie jest ewidentnym naruszeniem bezpieczeństwa, osoby wskazane w punkcie powyżej mogą zdecydować o natychmiastowym odebraniu uprawnień w systemach informatycznych użytkownikom wykonawcy i bez zbędnej zwłoki przekazują informację o blokadzie dostępu osobie upoważnionej ze strony wykonawcy.

9.3 Upoważnione osoby wykonawcy zabezpieczają ślady (np. logi systemowe) naruszenia bezpieczeństwa.

9.4 W szczególnych przypadkach ABSI informuje organy ścigania o zaistniałej sytuacji.

9.5 Pracownik DSI sporządza notatkę dotyczącą naruszenia bezpieczeństwa i kieruje ją do ABSI Centrum.

9.6 Ostatnim etapem zamykania naruszenia bezpieczeństwa jest usunięcie skutków naruszenia bezpieczeństwa oraz wprowadzenie dodatkowych zabezpieczeń (np. zmieniając konfigurację) w porozumieniu z uprawnionym przedstawicielem wykonawcy.

9.7 Każdy incydent związany z naruszeniem bezpieczeństwa informacji musi być zarejestrowany w rejestrze incydentów prowadzonym przez ABSI/IOD.

10 Postanowienia końcowe

10.1 Za nadzór nad przestrzeganiem postanowień ROI odpowiada:

a. ze strony wykonawcy uprawniony przedstawiciel wykonawcy,

b. ze strony Centrum ABSI.

10.2 Naruszając ROI wykonawca może podlegać sankcjom karnym, cywilnym oraz wynikającym z przepisów art. 107 i art. 108 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych

11 Terminologia

Użyte w ROI pojęcia i definicje oznaczają:

11.1 **ABSI** - Administrator Bezpieczeństwa Systemów Informatycznych.

11.2 **ADO - Administrator Danych Osobowych** – Narodowe Centrum Badań i Rozwoju reprezentowane przez Dyrektora Centrum.

11.3 **AM** - Administrator Merytoryczny – Właściciel zasobu sieciowego, aplikacji lub zbioru danych osobowych. Lista Administratorów Merytorycznych wraz z obszarami odpowiedzialności znajduje się w intranecie w zakładce „Dokumenty" https://intranet.ncbr-local.lan/2012-02-27-11-26-16/dzial-uslug-it.

11.4 **AS** – Administrator Systemu - osoba odpowiedzialna za nadzorowanie i utrzymywanie systemu informatycznego.

11.5 **Aktywo informacyjne -** wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością NCBR lub wykorzystywane bądź administrowane.

11.6 **Centrum** - Narodowe Centrum Badań i Rozwoju.

11.7 **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest osoba fizyczna, której tożsamość można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

11.8 **Dyrektor Centrum** - Dyrektor Centrum, Zastępca Dyrektora Centrum lub osoba upoważniona.

11.9 **DAZ** – Dział Administracji i Zakupów.

11.10 **DSI** – Działa Systemów Informatycznych.

11.11 **IOD** – Inspektor Ochrony Danych, osoba wyznaczona przez ADO zgodnie z art. 37 RODO, odpowiedzialna za monitorowanie przestrzegania zasad ochrony danych osobowych u ADO.

11.12 Kierownik KO – kierownik komórki organizacyjnej – Główny Księgowy, dyrektor działu lub biura, zastępca dyrektora działu lub biura, kierownik sekcji, samodzielne stanowisko podległe bezpośrednio Dyrektorowi Centrum.

11.13 **KO** – dział, biuro, sekcja, zespół, samodzielne stanowisko pracy podległe bezpośredni Dyrektorowi Centrum.

11.14 **Pracownik** - osoba pozostająca w stosunku pracy z Centrum; postanowienia niniejszego regulaminu dotyczące Pracownika stosuje się także do współpracownika tj. - osoby współpracującej z Centrum na podstawie umowy cywilnoprawnej.

11.15 **Przetwarzanie danych osobowych** – operacje wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, np. zbieranie, utrwalanie, organizowanie,

porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

11.16 **RODO** – rozporządzenie Parlamentu Europejskiego z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

11.17 **ROI** – Regulamin Ochrony Informacji dla Wykonawcy.

11.18 **System Informatyczny** - jest to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

11.19 **Wykonawca –** podmiot zewnętrzny w stosunku do NCBR świadczący usługi na rzecz NCBR

12 Dokumenty związane

12.1 Polityka Bezpieczeństwa Informacji Narodowego Centrum Badań i Rozwoju.

12.2 Polityka Bezpieczeństwa Danych Osobowych Narodowego Centrum Badań i Rozwoju.

13 Załączniki

Załącznik nr 1 - wzór zobowiązania do zachowania poufności przetwarzanych danych wraz ze wzorem oświadczenia pracownika (firmy zewnętrznej) o zachowaniu poufności informacji chronionych.

14 Rejestr zmian

Lp.	Data	Opis	Dotyczy stron(y)	Wprowadzający zmianę

Załącznik nr 1 do Regulaminu ochrony informacji dla wykonawcy Narodowego Centrum Badań i Rozwoju

Wzór zobowiązania do zachowania poufności przetwarzanych danych

UMOWA O ZACHOWANIU POUFNOŚCI INFORMACJI

(zwana dalej „Umową")

zawarta w dniu […] w […] pomiędzy:

Narodowym Centrum Badań i Rozwoju z siedzibą w Warszawie (00-695 Warszawa), adres: ul. Nowogrodzka 47a, działającym na podstawie ustawy z dnia 30 kwietnia 2010 roku o Narodowym Centrum Badań i Rozwoju posiadającym REGON: 141032404 oraz NIP: 701-007-37-77, zwanym dalej „**NCBR**" lub „**Stroną ujawniającą**" reprezentowanym przez:

……

a

Panią/Panem …… zamieszkałą/zamieszkałym w…… (…-…), przy ul. …….., posiadającą/posiadającym PESEL: ……., legitymującą/legitymującym się dowodem osobistym serii: …. numer ….., wydanym przez: ……., ważnym do: ……, prowadzącą/prowadzącym działalność gospodarczą pod firmą „……", przy ul. …….., posiadającą/posiadającym NIP: …….. oraz REGON: ……..,
zwanym dalej „**Odbiorcą Informacji Poufnych**" lub „**Odbiorcą**"
(*wydruk z Centralnej Ewidencji i Informacji o Działalności Gospodarczej Odbiorcy stanowi Załącznik nr 1 do Umowy*)

lub

…… z siedzibą w ……, adres: ul. …….., (…-…) wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy w ……., …. Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: ……, posiadającą NIP: ……. oraz REGON: ……., kapitał zakładowy w wysokości: ……., opłacony w całości, zwanym dalej „**Odbiorcą Informacji Poufnych**" lub „**Odbiorcą**", reprezentowanym przez: Panią/a ……
(*wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru przedsiębiorców KRS Odbiorcy stanowi Załącznik nr 1 do Umowy*)

lub

…… z siedzibą w ……., adres: ul. ……., (…-…), wpisanym do Rejestru Instytutów Naukowych Polskiej Akademii Nauk pod numerem rejestru …….., NIP: ……., REGON: ……,
zwanym dalej „**Odbiorcą Informacji Poufnych**" lub „**Odbiorcą**", reprezentowanym przez: Panią/a ……

działającą/ego na podstawie pełnomocnictwa nr …… z dnia ……
(*wydruk z Rejestru Instytutów Naukowych oraz kopia pełnomocnictwa do reprezentowania Odbiorcy stanowią załącznik nr 1 do Umowy*),

lub

…… z siedzibą w …….. adres: ul. ……, (…-…) wpisanym do Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy w ……., …. Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: ……, posiadającym NIP: ……. zwanym dalej „**Odbiorcą Informacji Poufnych**” lub „**Odbiorcą**”, reprezentowanym przez:
Panią/a ……
działającą/ego na podstawie pełnomocnictwa nr …… z dnia ……
(*wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru przedsiębiorców KRS Odbiorcy stanowi Załącznik nr 1 do Umowy*)

lub

…… z siedzibą w ……, adres: ul. ……..,
…-… ……, wpisaną do Rejestru Instytucji Szkolnictwa wyższego prowadzonego w ramach systemu POLon pod numerem rejestru ……., NIP: ……., zwanym dalej „**Odbiorcą Informacji Poufnych**” lub „**Odbiorcą**”, reprezentowanym przez:
Panią/a ……
działającą/ego na podstawie pełnomocnictwa nr …… z dnia ……
(*wydruk z Rejestru Instytucji Szkolnictwa wyższego systemu POLon Odbiorcy oraz kopia pełnomocnictwa do reprezentowania Odbiorcy stanowią załącznik nr 1 do Umowy*)

lub

…… z siedzibą w ……, adres: ul. ……., …-…
……, wpisanym do Rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz publicznych zakładów opieki zdrowotnej, prowadzonego w ramach Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy w ……., …. Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS ……., NIP: ……., REGON: ……, zwanym dalej „**Odbiorcą Informacji Poufnych**” lub „**Odbiorcą**” reprezentowanym przez:
Panią/a ……
działającą/ego na podstawie pełnomocnictwa nr …… z dnia ……
(wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru KRS Odbiorcy Informacji Poufnych oraz kopia pełnomocnictwa do reprezentowania Odbiorcy stanowią załącznik nr 1 do Umowy)
zwanymi dalej łącznie „**Stronami**” a pojedynczo „**Stroną**”.

Preambuła

Zważywszy, że celem Stron jest uregulowanie wzajemnych stosunków w zakresie przekazywania przez NCBR informacji poufnych do Odbiorcy w związku z wykonywaniem umowy dotyczącej …….. (dalej jako „Umowa główna") oraz zapewnienie bezpieczeństwa i ochrony takich informacji, Strony zgodnie postanawiają, co następuje:

§ 1.

1. Przedmiotem Umowy jest zobowiązanie się przez Odbiorcę do zachowania poufności i nieujawniania jakichkolwiek informacji przekazywanych przez NCBR i pozyskanych w trakcie realizacji Umowy głównej, niezależnie od formy ich uzyskania, bez konieczności ich oznaczenie przez NCBR jako poufne w chwili udostępnienia (dalej jako: Informacje Poufne").
2. W szczególności, do Informacji Poufnych zaliczane będą wszelkie informacje i dokumenty o charakterze technicznym, technologicznym, handlowym lub związane z działalnością NCBR oraz wszelkie inne informacje posiadające ekonomiczną wartość, które nie są powszechnie znane.
3. Odbiorca zobowiązuje się do:
   1) zachowania w tajemnicy wszelkich informacji przekazywanych przez Stronę ujawniającą w związku z wykonywaniem Umowy głównej, jak i wszelkich informacji zebranych w trakcie negocjacji poprzedzających jej zawarcie, niezależnie od formy w jakiej zostały przekazane;
   2) ujawnienia Informacji Poufnych wyłącznie osobom, którymi się posługuje lub którym powierza wykonanie Umowy głównej w celu i w zakresie niezbędnym do jej wykonania;
   3) poinformowania osób, o których mowa w § 1 ust. 3 pkt 2 Umowy, o poufnym charakterze informacji, pouczenia w sprawie ich traktowania jako poufnych oraz odebrania od nich oświadczenia, którego wzór stanowi Załącznik nr 1 do Umowy;
   4) niewykorzystywania, niekopiowania, niepowielania, nierozpowszechniania jakiejkolwiek Informacji Poufnej lub jej części, za wyjątkiem przypadków gdy jest to niezbędne dla wykonania Umowy głównej.
4. Nie stanowią Informacji Poufnej informacje:
   1) które są dostępne publicznie lub staną się publicznie dostępne w inny sposób niż poprzez naruszenie obowiązku zachowania poufności;
   2) które w momencie ujawnienia były już w posiadaniu Odbiorcy lub jego pracownika, członka organu lub doradcy, pod warunkiem, iż nie zostały objęte obowiązkiem zachowania poufności oraz że zostały one uzyskane bez naruszenia prawa;
   3)
   4) które zostały otrzymane od stron trzecich zgodnie z prawem i bez naruszenia jakiegokolwiek zobowiązań do zachowania poufności;w stosunku, do których NCBR oświadczy na piśmie, że nie uznaje ich za Informacje Poufne;
5. Nie stanowi naruszenia Informacji Poufnej ujawnienie dokonane zgodnie z wymogami prawa, w tym na wniosek lub wezwanie uprawnionych sądów lub organów, w zakresie i w granicach dozwolonych prawem, na podstawie postanowienia lub wezwania sądu

lub decyzji administracyjnej albo w celu dochodzenia roszczeń. Przed ujawnieniem informacji zgodnie ze zdaniem poprzednim, Odbiorca powiadomi NCBR pisemnie o otrzymaniu takiego wniosku lub wezwania, określając formę i cel ujawnienia, chyba że przekazanie takiej wiadomości jest zabronione na podstawie obowiązujących przepisów prawa. Gdyby uprzednie powiadomienie NCBR o otrzymaniu wniosku lub wezwania nie było w okolicznościach sprawy możliwe, Odbiorca powiadomi NCBR niezwłocznie po ustaniu okoliczności uniemożliwiających powiadomienie.

6. Ujawnienie Informacji Poufnych osobie trzeciej jest dopuszczalne wyłącznie po uzyskaniu uprzedniej pisemnej zgody NCBR i na warunkach przez NCBR określonych.
7. Odbiorca ponosi wobec Strony ujawniającej odpowiedzialność za naruszenie obowiązków w zakresie zachowania w tajemnicy Informacji Poufnych, również w przypadku, gdy naruszenie jest dokonane przez osobę trzecią, o której mowa w § 1 ust. 3 pkt 2 Umowy, za której działania lub zaniechania Odbiorca odpowiada jak za własne.
8. Odbiorca zapewnia, że dysponuje właściwymi zabezpieczeniami umożliwiającymi ochronę Informacji Poufnych przed dostępem i bezprawnym ich wykorzystaniem przez osoby nieuprawnione.
9. W zakresie możliwości posługiwania się osobami trzecimi lub powierzania im wykonania Umowy głównej, wiążące dla Stron są jej postanowienia.

§ 2.

Dla uniknięcia wątpliwości Strony potwierdzają, iż Umowa nie skutkuje przeniesieniem jakiegokolwiek prawa do Informacji Poufnych na Odbiorcę uzyskującego te informacje.

§ 3.

1. Odbiorca zobowiązuje się do zachowania w poufności Informacji Poufnych oraz wykorzystania Informacji Poufnych wyłącznie dla celów realizacji Umowy głównej oraz do podjęcia w stosunku do Informacji Poufnych co najmniej takich środków ostrożności oraz takich samych środków zabezpieczających, jak te podejmowane w stosunku do własnych informacji poufnych.
2. Odbiorca zobowiązuje się do przechowywania Informacji Poufnych w bezpiecznym środowisku oraz zobowiązuje się nie kopiować, nie powielać, ani w jakikolwiek inny sposób nie utrwalać i nie rozpowszechniać Informacji Poufnych lub ich części, z wyjątkiem przypadków wewnętrznego użytku, gdy jest to niezbędne dla celów realizacji Umowy głównej.
3. W przypadku, gdy przekazywane Informacje Poufne będą stanowić informacje chronione przez przepisy powszechnie obowiązującego prawa, Odbiorca zobowiązuje się do przestrzegania stosownych regulacji prawnych w zakresie ochrony takich informacji.
4. Odbiorca oświadcza, że jest świadomy zagrożeń dotyczących bezpieczeństwa związanych z przesyłaniem informacji pocztą elektroniczną lub z użyciem Internetu, oraz że będzie odpowiedzialny za ochronę w zakresie informacji przesyłanych

w formie elektronicznej i ochrony przed wirusami oraz za zapewnienie, aby informacje takie nie były kierowane pod niewłaściwy adres.

5. Odbiorca zobowiązuje się do przestrzegania przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2018 r. poz. 1000, ze zm.). oraz rozporządzenia Parlamentu Europejskiego z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1) i zobowiązuje się nie wykorzystywać ani nie przetwarzać w jakikolwiek sposób danych osobowych, do których uzyska dostęp w wyniku realizacji współpracy dla celów innych niż wykonywanie umowy wskazanej w preambule.
6. Odbiorca ponosi pełną i wyłączną odpowiedzialność za będące następstwem jego zachowań szkody wyrządzone niezgodnym z Umową przetwarzaniem danych osobowych, w szczególności szkody wyrządzone utratą, niewłaściwym przechowywaniem lub posłużeniem się dokumentami, które są nośnikiem danych osobowych.
7. W przypadku, gdy Odbiorca wykonuje Umowę główną przy udziale osób trzecich, z zastrzeżeniem § 1 ust. 9 Umowy, postanowienia poprzedzających ustępów rozciągają się także na te osoby, przy czym Odbiorca ponosi pełną i wyłączną odpowiedzialność za działania lub zaniechania osób, którymi się posługuje lub którym powierza wykonanie powyższej umowy, jak za działania lub zaniechania własne.
8. Odbiorca dopuści do przetwarzania danych osobowych wyłącznie osoby posiadające stosowne upoważnienia do przetwarzania danych osobowych. W tym celu NCBR upoważnia Odbiorcę do wystawiania imiennych upoważnień do przetwarzania danych osobowych, przy czym Odbiorca zobowiązuje się niezwłocznie informować NCBR o osobach upoważnionych.

§ 4.

Umowa obowiązuje przez cały okres obowiązywania Umowy głównej, jak również przez okres … (słownie: ….) lat po jej wykonaniu albo wygaśnięciu lub … (słownie:…) lat po jej rozwiązaniu, odstąpieniu lub wypowiedzeniu.

§ 5.

9. Odbiorca na żądanie NCBR zwróci niezwłocznie wszelkie materiały, dokumenty, inne opracowania (na piśmie, w formie elektronicznej lub innej) oraz zniszczy wszystkie materiały, które zawierają Informacje Poufne i wykasuje z pamięci swoich komputerów, edytorów tekstów i podobnych środków wszystkie materiały stanowiące Informacje Poufne, włączając każdą kopię, w zakresie w jakim pozwala na to konfiguracja systemów teleinformatycznych. Ponadto Odbiorca, bez żądania NCBR, zwróci lub zniszczy materiały, dokumenty, nośniki zawierające Informacje Poufne odpowiednio najpóźniej z upływem okresu, o którym mowa w § 4 Umowy.
10. Na żądanie Strony ujawniającej Odbiorca niezwłocznie dostarczy jej pisemne oświadczenie potwierdzające dokonanie czynności wskazanych w ust. 1 powyżej.

§ 6.

11. W przypadku naruszenia przez Odbiorcę jakichkolwiek zobowiązań wynikających z niniejszej Umowy, NCBR będzie miał prawo do żądania natychmiastowego zaniechania naruszenia i usunięcia jego skutków. Wezwanie do zaniechania naruszeń i usunięcia jego skutków powinno być wysłane Odbiorcy w formie pisemnej z wyznaczeniem co najmniej terminu 14 (słownie: czternastu) dni do ustosunkowania się do niego.
12. W przypadku naruszenia przez Odbiorcę obowiązków dotyczących Informacji Poufnych, w tym danych osobowych, NCBR może żądać od Odbiorcy zapłaty kary umownej w wysokości ……. PLN (słownie: ……) za każdy przypadek naruszenia. Odbiorca zobowiązuje się do uregulowania kary w terminie 14 (słownie: czternastu) dni kalendarzowych od dnia doręczenia Odbiorcy wezwania do zapłaty/noty obciążeniowej w formie pisemnej.
13. NCBR zastrzega sobie prawo dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych Kodeksu cywilnego.

§ 7.

1. Umowa wchodzi w życie w dniu podpisania jej przez Strony.
2. Umowa podlega prawu polskiemu.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Strony zgodnie oświadczają, że wszelkie spory powstałe w związku z realizacją niniejszej Umowy będą starały się rozstrzygać w sposób polubowny. W przypadku, gdy Strony nie osiągną porozumienia w sposób wskazany w zdaniu poprzedzającym, wszelkie spory wynikające w związku z realizacją Umowy zostaną rozstrzygnięte przez sąd powszechny właściwy miejscowo dla siedziby NCBR.
5. Niniejsza Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
6. Integralną część Umowy stanowią:

    1) Załącznik nr 1 - wydruk z Centralnej Ewidencji i Informacji o Działalności Gospodarczej Odbiorcy/ wydruk informacji odpowiadającej odpisowi aktualnemu z rejestru przedsiębiorców KRS Odbiorcy/ wydruk z Rejestru Instytutów Naukowych oraz kopia pełnomocnictwa do reprezentowania Odbiorcy/ wydruk z Rejestru Instytucji Szkolnictwa wyższego systemu POLon;

    2) Załącznik nr 2 - Oświadczenie o zobowiązaniu do zachowania poufności (Wzór).

…….. ……..

Strona ujawniająca **Odbiorca Informacji Poufnych**

(data i podpis) (data i podpis)

Załącznik nr 1 do Umowy o zachowaniu poufności informacji

z dnia …….

/WZÓR/

OŚWIADCZENIE

O ZOBOWIĄZANIU DO ZACHOWANIA POUFNOŚCI

Warszawa, dnia …… r.

Niniejszym oświadczam, że znana mi jest treść Umowy o zachowaniu poufności informacji

z dnia …… zawartej pomiędzy
……

a

……

i wynikające z niej zobowiązania do utrzymywania w tajemnicy ujawnionych Informacji Poufnych oraz zobowiązuje się do ich przestrzegania.

Niniejszym zobowiązuję się jako pracownik …….. (nazwa firmy)/zleceniobiorca/Wykonawca* …….. do zachowania w tajemnicy wszelkich Informacji Poufnych, które zostały mi ujawnione w związku z moim uczestnictwem w wykonywaniu …….., na warunkach określonych w Umowie o zachowaniu poufności. Jestem świadomy, że naruszenie powyższych zobowiązań może skutkować odpowiedzialnością cywilną i karną na podstawie obowiązujących przepisów prawa.

……

(data i podpis)

* niepotrzebne skreślić