NASK

Regulamin Programu Partnerstwo dla Cyberbezpieczeństwa

REGULAMIN DO UMOWY O WSPÓŁPRACY W ZAKRESIE CYBERBEZPIECZEŃSTWA

Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa
Tel: 22 380 82 00, Fax: 22 380 82 01, E-mail: nask@nask.pl

NASK

SPIS TREŚCI

I. Definicje

1. **Centrum Cyberbezpieczeństwa** – pion w strukturze NASK, do którego zadań należy realizowanie operacyjnych zadań ustawowych przewidzianych dla NASK w ramach krajowego systemu cyberbezpieczeństwa, zadań z zakresu analiz strategicznych (poziom policy) oraz weryfikowanie tych analiz przez organizację i udział w ćwiczeniach o zakresie krajowym oraz międzynarodowym.
2. **CERT Polska** (Computer Emergency Response Team) – dział w strukturze NASK, zajmujący się monitorowaniem, koordynacją i reagowaniem na zgłoszone incydenty i zagrożenia cyberbezpieczeństwa.
3. **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez NASK.
4. **Incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.
5. **NASK** – Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy z siedzibą w Warszawie, przy ul. Kolskiej 12, wpisany do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000012938.
6. **Oświadczenie** – oświadczenie Partnera dotyczące danych kontaktowych ze wskazaniem osób, które mają uzyskać dostęp do Strefy Partnera. Wzór oświadczenia stanowi złącznik nr 1 do Regulaminu.
7. **Partner** – podmiot prywatny lub publiczny, który zawarł z NASK Umowę o współpracy.
8. **Porozumienie** – trójstronne Porozumienie o współpracy w zakresie cyberbezpieczeństwa, zawarte pomiędzy Partnerem, Skarbem Państwa – Ministrem Cyfryzacji i NASK.
9. **Program Partnerstwo dla Cyberbezpieczeństwa/Program** – działający w strukturach NASK program współpracy na zasadach partnerstwa, dobrowolny i nieodpłatny, którego głównym celem jest współpraca na rzecz podniesienia poziomu cyberbezpieczeństwa Rzeczypospolitej Polskiej.
10. **Przedstawiciel Partnera** – osoba wyznaczona w Porozumieniu do kontaktów z NASK oraz z innymi uczestnikami Programu.
11. **Strefa Partnera** – internetowy zasób teleinformatyczny NASK, służący do wymiany informacji pomiędzy Partnerami i NASK.
12. **Sieć Kontaktów** – lista Partnerów i użytkowników Strefy Partnera wraz z krótką informacją o firmie Partnera oraz jego danymi kontaktowymi.
13. **Zespół Dyżurnet.pl** – zespół w strukturze NASK działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.
14. **Zespół Programu Partnerstwo dla Cyberbezpieczeństwa/Zespół** – zespół w strukturze NASK, odpowiedzialny za współpracę z uczestnikami Programu.
15. **Zagrożenie cyberbezpieczeństwa** – potencjalna przyczyna wystąpienia incydentu.

II. Postanowienia ogólne

1. NASK zapewnia platformę współpracy oraz koordynuje działania w ramach Programu Partnerstwo dla Cyberbezpieczeństwa.
2. Regulamin określa podstawowe założenia Programu oraz zasady współpracy w jego ramach.
3. Regulamin definiuje zasady korzystania ze zdalnego dostępu do Strefy Partnera.
4. Regulamin określa zasady poufności danych kontaktowych użytkowników Strefy Partnera oraz ochrony informacji wymienianych w ramach Programu.

III. Założenia Programu Partnerstwo dla Cyberbezpieczeństwa

1. Program Partnerstwo dla Cyberbezpieczeństwa realizowany jest w celu podniesienia poziomu cyberbezpieczeństwa Rzeczypospolitej Polskiej, min. poprzez wspieranie podmiotów krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa oraz przekazywanie informacji dotyczących incydentów, podatności i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa.
2. Podstawowym założeniem Programu jest wymiana informacji z zakresu cyberbezpieczeństwa, a także informacji o Incydentach i istotnych Zagrożeniach, o charakterze wykraczającym, w ocenie Partnera, poza zdarzenia wewnętrzne u danego Partnera, lub o charakterze systemowo istotnym, jak i zapewnienie odpowiedniej reakcji i postępowania w rozwiązywaniu problemów.
3. NASK w ramach Programu organizuje cykliczne spotkania Partnerów, których celem jest wymiana wiedzy i doświadczeń w zakresie cyberbezpieczeństwa, a także może powoływać zespoły zadaniowe, mogące wypracowywać konkretne rozwiązania, min.: rekomendacje, procedury i standardy dla określonych sektorów gospodarki i grup. Dodatkowo NASK buduje i udostępnia Sieć Kontaktów w ramach Programu, które umożliwią szybkie porozumiewanie pomiędzy Partnerami, przekazuje wiedzę ekspercką, cykliczne raporty o rejestrowanych Zagrożeniach i Incydentach, a także może pomóc wspierać prowadzone aktywności z zakresu edukacji i działalności dotyczącej bezpieczeństwa w Internecie.
4. W ramach Programu, Partner może przekazywać do NASK informacje o Incydentach, informować NASK o zaobserwowanych Zagrożeniach i dzielić się wiedzą z zakresu cyberbezpieczeństwa. Partner również może zainicjować powołanie zespołu zadaniowego dla danego sektora gospodarki lub zagadnienia. Dodatkowo w celu budowania Sieci Kontaktów, Partner może przekazać do Strefy Partnera informację o swojej działalności, dane kontaktowe oraz logo.

IV. Wymiana informacji w ramach Programu Partnerstwo dla Cyberbezpieczeństwa

1. Informacje wymieniane w ramach Programu mogą dotyczyć, min.: ostrzeżeń o Incydentach i Zagrożeniach, analiz, regulacji prawnych, a także informacji o konferencjach, szkoleniach oraz ćwiczeniach dotyczących cyberbezpieczeństwa.
2. NASK zbiera i rejestruje informacje o Incydentach i Zagrożeniach, w celu tworzenia bieżącego obrazu bezpieczeństwa teleinformatycznego w Polsce, identyfikowania występujących i potencjalnych Zagrożeń oraz wskazywania optymalnych metod ich powstrzymywania i zwalczania.
3. Podstawowym narzędziem wymiany informacji pomiędzy Partnerami i NASK jest Strefa Partnera, w ramach której NASK zapewnia narzędzia służące do komunikacji, w tym bazę wiedzy, Sieć Kontaktów oraz inne narzędzia umożliwiające wymianę wiedzy na temat Incydentów i Zagrożeń.
4. Incydenty oraz Zagrożenia można zgłaszać poprzez odnośnik do formularza, który znajduje się na stronie głównej Strefy Partnera, opisany jako „Zgłoś Incydent".
5. Szkodliwe i nielegalne treści w Intrenecie można zgłaszać poprzez odnośnik do formularza Zespołu Dyżurnet.pl, opisany jako: „Zgłoś nielegalne treści".
6. W celu koordynacji reakcji na zgłoszenia oraz w celu gromadzenia informacji statystycznych, zgłoszenia o Incydentach i Zagrożeniach rejestrowane są w Systemie Ticketowym oraz innych systemach NASK.
7. Narzędzia stosowane do komunikacji w ramach Programu obejmują również:
   - e-mail – w celu zgłaszania problemów z dostępem do Strefy Partnera, kontaktów organizacyjnych, przesłania plików i informacji bezpośrednio do Zespołu, Partner może korzystać z dedykowanego aliasu: partnerzy-pdc@nask.pl;
   - telefon – telefony kontaktowe do Zespołu dostępne w standardowych godzinach pracy, w celu bezpośredniego kontaktu np. organizacyjnego, a także telefon kontaktowy dostępny w trybie „24/7/365": +48 22 380 82 74, który może być wykorzystywany do zgłaszania problemów z dostępem do pozostałych narzędzi w Strefie Partnera oraz kontaktu z pierwszą linią CERT Polska w nagłych przypadkach;
   - faks – z pierwszą linią CERT Polska można kontaktować się całodobowo pod numerem faksu +48 22 380 83 99.

V. Przyznawanie dostępu do zasobów Strefy Partnera

1. Podstawą przyznania dostępu do Strefy Partnera jest złożenie przez Partnera Oświadczenia dotyczącego danych kontaktowych ze wskazaniem osób, które mają uzyskać dostęp do Strefy Partnera. Wzór Oświadczenia stanowi Załącznik nr 1 do Regulaminu. Wszystkie osoby mające dostęp do Strefy Partnera będą widoczne w Strefie Partnera jako użytkownicy zgodnie z nadanym loginem

(nazwa firmy-pierwsza litera imienia/nazwisko), a także w Sieci Kontaktów, przypisani do konkretnej firmy.

2. Partner może również udostępnić w Strefie Partnera dane kontaktowe innych osób lub działów, np. osób zajmujących się cyberbezpieczeństwem lub funkcjonującego w jego strukturach zespołu reagowania na zagrożenia bezpieczeństwa teleinformatycznego (poziom SOC/CSIRT/CERT), w celu budowania efektywnej Sieci Kontaktów. Zgłoszenia danych kontaktowych osób fizycznych muszą być opatrzone klauzulą informacyjną dotyczącą danych osobowych, zgodnie ze wzorem Oświadczenia stanowiącego załącznik nr 1 do Regulaminu, lub mogą zostać przekazane na niniejszym wzorze.
3. Oświadczenie podpisane przez upoważnionego w Porozumieniu Pełnomocnika Partnera albo osobę upoważnioną do reprezentacji podmiotu należy przekazać pocztą elektroniczną na alias: partnerzy-pdc@nask.pl.
4. Wygenerowane dane dostępowe do Strefy Partnera przekazywane są Partnerowi na wskazane w Oświadczeniu dane kontaktowe użytkownika: login wysłany jest na imienny adres e-mail, hasło przekazywane jest SMSem na numer telefonu komórkowego.
5. Dane dostępowe mogą zostać przekazane Partnerowi lub wyznaczonej przez niego osobie szyfrowaną pocztą e-mail. W tym przypadku wymagane jest przesłanie przez Partnera klucza publicznego PGP na alias: partnerzy-pdc@nask.pl, a także pozytywne zweryfikowanie właściciela klucza.
6. Po otrzymaniu hasła dostępowego użytkownik zobowiązany jest do jego niezwłocznej zmiany. Nowo wprowadzone hasło powinno uwzględniać podstawowe zasady konstrukcji bezpiecznych haseł, a użytkownik nie powinien nikomu go udostępniać.
7. W przypadku podejrzenia utraty poufności indywidualnego hasła, użytkownik powinien dokonać niezwłocznego zgłoszenia faktu do Zespołu oraz dokonać zmiany hasła. Link do formularza zmiany hasła dostępny jest na stronie Strefy Partnera.
8. Zasoby Strefy Partnera udostępniane są Partnerowi zdalnie. Do uruchomienia bezpiecznego szyfrowanego połączenia VPN służy program FortiClient.
9. Uruchomienie komunikacji z wykorzystaniem FortiClient należy realizować zgodnie z instrukcją przesłaną przez Zespół na adres e-mail razem z danymi dostępowymi do Strefy Partnera.
10. Po zestawieniu połączenia tunelowanego, użytkownik uzyskuje dostęp do Strefy Partnera pod adresem: https://sp.nask.pl.
11. W wypadku, kiedy warunki techniczne sieci Partnera nie zezwalają na dostęp na zasadach opisanych w punktach powyżej, istnieje możliwość wyrażenia zgody na wdrożenie innych środków technicznych do uzyskania dostępu, ustalanych indywidualnie.
12. Wszelkie problemy związane z konfiguracją połączenia oraz z logowaniem należy zgłaszać na alias: partnerzy-pdc@nask.pl.

VI. Ochrona i dostępność informacji

1. Decyzje na temat obiegu informacji w ramach Programu podejmuje Dyrektor Centrum Cyberbezpieczeństwa lub upoważniony pracownik NASK.
2. Partner zobowiązany jest do zachowania w bezwzględnej poufności wszelkich informacji udostępnianych i przekazywanych w ramach Programu, w tym Sieci Kontaktów, a także informacji otrzymywanych z NASK i od innych Partnerów, oraz odpowiadają za ich nieuprawnione ujawnienie.
3. Z zastrzeżeniem pkt 4 poniżej, NASK nie udostępnia informacji o Incydentach i Zagrożeniach pozwalających zidentyfikować podmioty, których Incydent czy Zagrożenie dotyczy. Zakaz, o którym mowa w zdaniu poprzedzającym nie dotyczy obowiązku przekazania informacji właściwym organom państwowym, zgodnie z bezwzględnie obowiązującymi przepisami prawa.
4. Informacje udostępniane publicznie przez NASK mogą dotyczyć wyłącznie:
   a. ogólnego i zanonimizowanego opisu Zagrożeń dla użytkowników Internetu, bez wskazywania danych konkretnego Partnera, chyba że informacja taka została uprzednio ujawniona publicznie przez Partnera lub osobę trzecią;
   b. statystyki zdarzeń i Incydentów.
5. NASK przetwarza dane osobowe otrzymane w zgłoszeniach zgodnie z polityką prywatności NASK PIB i CSIRT NASK.

VII. Postanowienia końcowe

1. Załączniki do Regulaminu stanowią jego integralną część.
2. Wszystkie kwestie nieuregulowane w Regulaminie rozstrzyga NASK.
3. W określonych przypadkach uzasadnionych okolicznościami Dyrektor NASK lub Dyrektor Centrum Cyberbezpieczeństwa mogą odstąpić od stosowania niektórych postanowień Regulaminu.
4. NASK zastrzega sobie możliwość wprowadzania zmian w Regulaminie, o czym Partner będzie informowany w formie elektronicznej, z zachowaniem co najmniej 30-dniowego okresu przed terminem wejścia w życie zmian w Regulaminie.

VIII. Załączniki

1. Załącznik nr 1. Wzór „Oświadczenie dotyczące danych kontaktowych oraz dostępu do Strefy Partnera”.

Załącznik nr 1 do Regulaminu

Oświadczenie dotyczące danych kontaktowych oraz dostępu do Strefy Partnera

Kontakt strategiczny (sprawy operacyjne)* ***

Imię i nazwisko	E-mail	Telefon komórkowy	Strefa Partnera**

Kontakt techniczny (sprawy merytoryczne, organizacyjne)* ***

Imię i nazwisko	E-mail	Telefon komórkowy	Strefa Partnera**

Kontakt media (sprawy edukacyjne, PR)* ***

Imię i nazwisko	E-mail	Telefon komórkowy	Strefa Partnera**

Poziom operacyjny – zespół SOC/CSIRT/CERT***

E-mail	
Telefon (ogólny)	
Godziny pracy	
Inne uwagi	

Oświadczam, że wypełniłem/am obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których ww. dane osobowe bezpośrednio lub pośrednio pozyskałem w celu realizacji Porozumienia, w tym ubiegania się o udzielenie dostępu do Strefy Partnera.

---------- ----------

Miejscowość, data

Pieczęć oraz podpis osoby uprawnionej do reprezentacji Podmiotu

* Zaproponowany podział na grupy kontaktów: strategiczny, techniczny i media pozwoli na optymalizację przepływu informacji. Dla każdego można wskazać więcej niż jedną osobę. Dla grupy kontaktów techniczny i media istnieje możliwość wskazania aliasu.

** Wpisanie T lub ✓ oznacza, że dany kontakt ma mieć dostęp do Strefy Partnera. Dostęp do Strefy Partnera może zostać przydzielony konkretnej osobie.

*** Podane dane zostaną opublikowane na stronie głównej Strefy Partnera.