OGÓLNE WARUNKI WSPÓŁPRACY
W RAMACH PROGRAMU PARTNERSTWO DLA CYBERBEZPIECZEŃSTWA

I. Postanowienia ogólne

1.1 Niniejszy dokument opisuje warunki przystąpienia do i współpracy w ramach koordynowanego przez NASK Programu Partnerstwo dla Cyberbezpieczeństwa.

1.2 Program Partnerstwo dla Cyberbezpieczeństwa stanowi narzędzie dobrowolnej współpracy i wymiany doświadczeń oraz informacji o zagrożeniach cyberbezpieczeństwa i incydentach, o którym mowa w art. 26 ust 6 pkt 2) ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 z późn. zm.).

1.3 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 przekazywania informacji dotyczących incydentów, podatności i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa.

1.4 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 oraz postępowania w rozwiązywaniu problemów.

1.5 Program Partnerstwo dla Cyberbezpieczeństwa skierowany jest do podmiotów Krajowego Systemu Cyberbezpieczeństwa.

II. Definicje

Pojęcia używane w niniejszych Ogólnych warunkach mają znaczenie nadane im poniżej:

- CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy;
- Dział Dyżurnet.pl – dział w strukturze NASK działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci;
- Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
- NASK / NASK-PIB - Naukowa i Akademicka Sieć Komputerowa Państwowy Instytut Badawczy z siedzibą w Warszawie, (01-045) Warszawa, przy ul. Kolskiej 12, NIP 521-04-17-157, REGON 010464542;

- Ogólne warunki – niniejsze Ogólne warunki współpracy w ramach Programu Partnerstwo dla Cyberbezpieczeństwa;
- Oświadczenie – oświadczenie Partnera dotyczące danych kontaktowych ze wskazaniem osób, które mają uzyskać dostęp do Strefy Partnera. Wzór oświadczenia stanowi złącznik nr 1 do Ogólnych warunków;
- Partner – partner Programu Partnerstwo dla Cyberbezpieczeństwa;
- Podmiot Krajowego Systemu Cyberbezpieczeństwa – podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 z późn. zm.);
- Program Partnerstwo dla Cyberbezpieczeństwa / Program – stworzone i utrzymywane przez NASK-PIB narzędzie dobrowolnej współpracy i wymiany doświadczeń oraz informacji o zagrożeniach cyberbezpieczeństwa i Incydentach, o którym mowa w art. 26 ust 6 pkt 2) ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 z późn. zm.);
- Przedstawiciel Partnera – osoba wyznaczona przez Partnera do kontaktów z NASK oraz z innymi uczestnikami Programu;
- Sieć Kontaktów – lista Partnerów i użytkowników Strefy Partnera wraz z krótką informacją o firmie Partnera oraz jego danymi kontaktowymi;
- Strefa Partnera – internetowy zasób teleinformatyczny NASK, służący do wymiany informacji pomiędzy Partnerami i NASK;
- Zagrożenie cyberbezpieczeństwa – potencjalna przyczyna wystąpienia Incydentu;
- Zespół – zespół odpowiedzialny za współpracę z uczestnikami Programu.

III. Zasady współpracy w ramach Programu Partnerstwo dla cyberbezpieczeństwa

3.1 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.

3.2 Dodatkowo NASK buduje i udostępnia Sieć Kontaktów w ramach Programu, które umożliwią szybkie porozumiewanie pomiędzy Partnerami, przekazuje wiedzę ekspercką, udostępnia cykliczne raporty o rejestrowanych Zagrożeniach i Incydentach, a także może pomóc wspierać prowadzone aktywności z zakresu edukacji i działalności dotyczącej bezpieczeństwa w Internecie.

3.3 W ramach Programu, Partner może przekazywać do NASK informacje o Incydentach i o zaobserwowanych Zagrożeniach oraz 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.

3.4 Narzędzia i materiały w ramach Programu udostępniane są Partnerom nieodpłatnie.

3.5 Każdy z Partnerów ponosi własne koszty udziału w Programie.

IV. Wymiana informacji w ramach Programu Partnerstwo dla Cyberbezpieczeństwa

4.1 Informacje wymieniane w ramach Programu mogą dotyczyć, min.: ostrzeżeń o Incydentach i Zagrożeniach, rekomendacji i dobrych praktyk, analiz i regulacji prawnych, a także informacji o konferencjach, szkoleniach oraz ćwiczeniach dotyczących cyberbezpieczeństwa.

4.2 NASK zbiera i rejestruje informacje o Incydentach i Zagrożeniach w celu tworzenia bieżącego obrazu cyberbezpieczeństwa na poziomie krajowym, identyfikowania występujących i potencjalnych Zagrożeń oraz wskazywania optymalnych metod ich powstrzymywania i zwalczania.

4.3 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.

4.4 Incydenty, Zagrożenia oraz szkodliwe i nielegalne treści w Intrenecie można zgłaszać poprzez odnośnik do formularza, który znajduje się na stronie głównej Strefy Partnera, opisany jako „Zgłoszenie".

4.5 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.

4.6 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: 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 kontaktu z CERT Polska w nagłych przypadkach.

V. Przyznawanie dostępu do zasobów Strefy Partnera

5.1 Warunkiem przyznania dostępu do Strefy Partnera jest:

5.1.1 akceptacja Ogólnych Warunków przez osobę uprawnioną do reprezentacji Partnera;

5.1.2 złożenie przez osobę uprawnioną do reprezentacji Partnera Oświadczenia dotyczącego danych kontaktowych ze wskazaniem osób, które mają uzyskać dostęp do Strefy Partnera. Wzór Oświadczenia stanowi Załącznik nr 1 do Ogólnych Warunków. Wszystkie osoby mające dostęp do Strefy Partnera będą widoczne w Strefie Partnera jako użytkownicy zgodnie z nadanym loginem (nazwa firmy-pierwsza litera imienia/nazwisko).

5.2 Partner może również udostępnić w Strefie Partnera dane kontaktowe innych osób lub działów swojej firmy np. osób zajmujących się cyberbezpieczeństwem, 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 Ogólnych warunków.

5.3 Oświadczenie podpisane przez osobę uprawnioną do reprezentacji Partnera należy przekazać pocztą elektroniczną na alias: pdc@nask.pl.

5.4 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.

5.5 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: pdc@nask.pl, a także pozytywne zweryfikowanie właściciela klucza.

5.6 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.

5.7 W przypadku podejrzenia utraty poufności indywidualnego hasła, użytkownik powinien dokonać niezwłocznego zgłoszenia faktu do Zespołu oraz dokonać zmiany hasła.

5.8 Zasoby Strefy Partnera udostępniane są Partnerowi na warunkach określanych przez NASK. Wszelkie problemy związane z logowaniem należy zgłaszać na alias: pdc@nask.pl.

5.9 Decyzja o udzieleniu dostępu do Strefy Partnera należy wyłącznie do NASK i nie wymaga uzasadnienia.

5.10 NASK nie ponosi odpowiedzialności za jakąkolwiek szkodę będącą wynikiem skorzystania z danych uwierzytelniających użytkownika przez inną osobę, za pozwoleniem lub bez pozwolenia użytkownika.

5.11 Uzyskując dostęp do Strefy Partnera, Partner zobowiązuje się:

- nie korzystać ze Strefy Partnera w sposób, który mógłby naruszać prawo polskie lub międzynarodowe;
- nie korzystać ze Strefy Partnera w sposób, który mógłby naruszać prawa lub interesy NASK lub pozostałych Partnerów;

- nie korzystać ze Strefy Partnera w sposób inny niż opisany w niniejszych Ogólnych warunkach.

VI. Ochrona i dostępność informacji

6.1 Decyzje na temat obiegu informacji w ramach Programu podejmuje NASK.

6.2 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 odpowiada za ich ujawnienie osobom nieuprawnionym.

6.3 Z zastrzeżeniem pkt 6.4 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.

6.4 Informacje udostępniane publicznie przez NASK mogą dotyczyć wyłącznie:

6.4.1 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;

6.4.2 statystyki Zagrożeń i Incydentów.

6.5 Obowiązek zachowania poufności, o którym mowa w niniejszym punkcie, oznacza w szczególności, że NASK i Partner będą zobowiązani:

6.5.1 chronić informacje, o których mowa w niniejszym punkcie przed ich ujawnieniem w taki sam sposób i z co najmniej taką samą starannością z jaką chronią własne informacje poufne, przez co rozumieją najwyższą staranność;

6.5.2 ograniczyć obieg informacji, o których mowa w niniejszym punkcie do osób, którym wiedza na ten temat jest niezbędna i zobowiązać ich do zachowania tych informacji w bezwzględnej poufności.

6.6 NASK przetwarza dane osobowe otrzymane w ramach Programu zgodnie z polityką prywatności NASK PIB i CSIRT NASK udostępnioną do wglądu na stronie internetowej.

6.7 Całkowita odpowiedzialność NASK wobec Partnera oraz Partnera wobec NASK, niezależnie od jej tytułu, ograniczona jest do kwoty 100.000,00 zł (słownie: sto tysięcy złotych).

VII. Zmiany

7.1 Partner oświadcza, że wyraża zgodę na zmianę Ogólnych warunków lub załączników do nich, jaka może być dokonywana okresowo przez NASK. NASK zobowiązuje się poinformować Partnera w formie elektronicznej o zmianie Ogólnych warunków lub załączników do nich z co najmniej 30-dniowym wyprzedzeniem, jak również dołoży wszelkich starań, aby skonsultować zmianę

z Partnerem przed jej wprowadzeniem. W przypadku braku akceptacji dla zmian wprowadzonych do Ogólnych warunków lub załączników do nich, Partner może wypowiedzieć Ogólne warunki z zachowaniem 14-dniowego okresu wypowiedzenia.

7.2 Wypowiedzenie Ogólnych warunków jest równoznaczne z utratą statusu Partnera Programu Partnerstwo dla Cyberbezpieczeństwa i dostępem do Strefy Partnera.

VIII. Postanowienia końcowe

8.1 NASK oraz każdy z Partnerów ma prawo wypowiedzenia Ogólnych warunków z zachowaniem 1-miesięcznego okresu wypowiedzenia.

8.2 W przypadku powzięcia uzasadnionego podejrzenia, że informacje przekazywane w ramach współpracy w Programie Partnerstwo dla Cyberbezpieczeństwa są wykorzystywane niezgodnie z celami określonymi w Ogólnych warunkach, każdy z podmiotów, które współpracują w ramach Programu Partnerstwo dla Cyberbezpieczeństwa ma prawo wezwać podmiot naruszający Ogólne warunki, za pośrednictwem NASK, do zaniechania tych naruszeń, wyznaczając mu w tym celu termin nie krótszy niż 72 godziny, a w przypadku bezskutecznego upływu wyznaczonego terminu, NASK będzie uprawniony do wypowiedzenia Ogólnych warunków ze skutkiem natychmiastowym.

8.3 Wszelkie spory mogące wyniknąć z realizacji Ogólnych warunków będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby NASK.

8.4 Ogólne warunki podlegają prawu polskiemu. W sprawach nieuregulowanych w niniejszej Umowie stosuje się przepisy Kodeksu Cywilnego.

Miejscowość, data

Podpis osoby uprawnionej do reprezentacji Podmiotu