|  |  |
| --- | --- |
|  |  |
|  |
| (miejsce na pieczęć nagłówkową podmiotu) |  |

**Ankieta dotycząca**

**spełnienia warunków, o których mowa w art. 48 ust. 1 ustawy o ewidencji ludności[[1]](#footnote-1), art. 66 ust. 2/art. 68 ust. 3 ustawy o dowodach osobistych[[2]](#footnote-2), art. 87 ust. 1 ustawy o dokumentach paszportowych[[3]](#footnote-3) oraz art. 20m ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[[4]](#footnote-4)**

Oświadczenie zawiera zapytania dotyczące spełnienia, przez podmiot ubiegający się o dostęp do danych, warunków określonych w w/w ustawach

|  |  |
| --- | --- |
| **Prowadzona dokumentacja** | |
| 1. Czy opracowana jest i wdrożona do stosowania Polityka Bezpieczeństwa zgodna z wytycznymi rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) oraz ustawą z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)? | TAK / NIE |
| 1. Czy podmiot posiada i stosuje Instrukcję zarządzania systemami informatycznymi? | TAK / NIE |
| 1. Czy istnieją procedury zabezpieczające dane w przypadku konieczności ich wyniesienia poza obszar przetwarzania na skutek zdarzeń losowych? | TAK / NIE |
| 1. Czy osoby mające dostęp do systemu uzyskały stosowne upoważnienia i zostały zapoznane z przepisami o ochronie danych osobowych. | TAK / NIE |

|  |  |
| --- | --- |
| **Miejsce, w którym realizowany będzie dostęp do SRP** | |
| 1. Gdzie będzie odbywało się przetwarzanie danych? | RP / UE / poza UE |
| 1. Czy dane będą przetwarzane w chmurze? | TAK / NIE |
| 1. W jakiej chmurze będą przetwarzane dane? | PRYWATNA / PUBLICZNA / NIE DOTYCZY |
| 1. Czy została wydzielona i zabezpieczona strefa ochronna, w której realizowany będzie dostęp do SRP? | TAK / NIE |
| 1. Czy drzwi do wydzielonej strefy ochronnej:    1. znajdujące się wewnątrz budynku w strefie ograniczonego dostępu (bądź dozorowanej), są wyposażone w co najmniej 1 zamek atestowany (klasa C).    2. znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej alternatywnie:  * spełniają wymagania klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 lub, * są zabezpieczone przed wyważeniem (podważeniem) oraz być wyposażone w co najmniej 1 zamek atestowany (klasa C).  1. do których dostęp jest z zewnątrz budynku:  * spełniają wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010, * posiadają co najmniej jeden zamek atestowany (klasa C) lub, * w pomieszczeniach jest zainstalowany system alarmowy z funkcją powiadamiania. | TAK / NIE |
| 1. Czy otwory okienne pomieszczeń strefy chronionej znajdujących się na parterze lub mających swobodny dostęp z dachu są okratowane, zabezpieczone folią antywłamaniową bądź czy posiadają szyby o zwiększonej odporności na zbicie? | TAK / NIE /  NIE DOTYCZY |
| 1. Proszę opisać, jakimi metodami organizacyjno-technicznymi realizowana jest kontrola dostępu do wydzielonej strefy ochronnej: | |
|  |  |
| Środowisko sprzętowo-systemowe, z którego realizowany jest dostęp do SRP | |
| 1. Czy na urządzeniach (np. stacje robocze, urządzenia sieciowe) zapewniających dostęp do SRP zostały zastosowane następujące minimalne zabezpieczenia: |  |
| 1. wejście i zmiana ustawień BIOS/UEFI wymaga podania hasła; | TAK / NIE |
| 1. wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera; | TAK / NIE |
| 1. długość hasła BIOS/UEFI wynosi nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra); | TAK / NIE |
| 1. każdemu użytkownikowi komputera założone jest oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora, o ile nie jest to wymagane do bieżącej pracy; | TAK / NIE |
| 1. długość nazwy użytkownika powinna wynosić nie mniej niż 6 znaki; | TAK / NIE |
| 1. długość hasła konta administratora lub użytkownika z uprawnieniami administratora wynosi nie mniej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie może być dłuższy niż 30 dni; | TAK / NIE |
| 1. długość hasła konta użytkownika wynosi nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie może być dłuższy niż 30 dni; | TAK / NIE |
| 1. zainstalowany jest system operacyjny, pochodzący z legalnego źródła i objęty wsparciem, co najmniej w zakresie aktualizacji zabezpieczeń; | TAK / NIE |
| 1. zainstalowane jest oprogramowanie antywirusowe, antymalware, działające w czasie rzeczywistym i wykonujące pełne skanowanie stacji co najmniej 1 raz w tygodniu; | TAK / NIE |
| 1. ustawione jest automatyczne uruchamianie wygaszacza ekranu na maksymalnie 5 minut, wznowienie pracy wymaga podania hasła, obowiązkowe jest blokowanie lub wyłączenie komputera przez Użytkownika przy każdorazowym opuszczeniu stanowiska; | TAK / NIE |
| 1. konfiguracja „kosza” systemowego ustawiona jest w taki sposób, aby nie przechowywał usuniętych plików (lub wprowadzone są procedury obligujące użytkowników do opróżniania „kosza” po kasowaniu danych). | TAK / NIE |
| 1. bezprzewodowa komunikacja jest trwale wyłączona na stacjach roboczych i serwerach mających dostęp do zasobów SRP?   *(Bezprzewodowe sieci, przykładowo WiFi, WiMAX, Bluetooth, nie mogą być używane do komunikacji z SRP).* | TAK / NIE |
| 1. aktualizacje są na bieżąco instalowane (aktualizacja systemu oraz przeglądarek przynajmniej w zakresie zalecanych poprawek bezpieczeństwa producentów), | TAK / NIE |
| W przypadku zaznaczenia NIE w pkt 12 ppkt a-m, proszę opisać zastosowane zabezpieczenia. | |

|  |  |
| --- | --- |
| **Sposób dostępu do SRP** |  |
| 1. Czy dostęp do danych ma być zapewniony przez Źródło czy API | Źródło/API |
| 1. Czy stanowiska dostępowe do SRP są odseparowane fizycznie od sieci lokalnej wnioskującego i Internetu?   *W przypadku wskazania w punkcie 13 tylko aplikacji „Źródło” i odpowiedzi „TAK”,*  *punkty 35, 36, 37 nie będą wpływały na ocenę. W przypadku wskazania w punkcie 13 API i odpowiedzi „TAK”, punkty: 18-25, 28, 37 nie będą wpływać na ocenę.* | TAK / NIE |
| 1. Czy w przypadku korzystania z aplikacji Źródło, ruch sieciowy pomiędzy systemem SRP, a stacjami końcowymi SRP u Interesariusza nie jest odszyfrowywany na żadnym etapie połączenia. | NIE JEST / JEST / NIE DOTYCZY |
| 1. Czy system Państwa instytucji, łączący się z SRP, jest osiągalny za pośrednictwem portalu dostępnego za pomocą przeglądarki w sieci Internet? | TAK / NIE/ NIE DOTYCZY |

|  |  |
| --- | --- |
| **Połączenia przez API (własny system) lub aplikacja „Źródło” z integracją sieci**  *Punkty 18-28 należy wypełnić tylko w przypadku wskazania API lub też wskazania aplikacji „Źródło” i jednocześnie odpowiedzi NIE w punkcie 14, w przeciwnym przypadku proszę zaznaczyć NIE DOTYCZY.* | TAK / NIE |
| 1. Proszę podać nazwę własnego systemu łączącego się z SRP (należy dołączyć dokumentację dotyczącą architektury połączenia).   …………………………………………………………………………………………………………………………  ……………………………………………………………………………………………………………………...... | |
| 1. Czy punkt przyłączenia sieci systemów integrowanych, jest wyposażony w co najmniej jeden ze środków ochrony sieci, takich jak: IPS, systemy SIEM, inny: ………………………………………………………………………………………...? | TAK / NIE |
| 1. Czy sieć wewnętrzna wnioskodawcy przeznaczona do obsługi połączeń do systemu rejestrów państwowych SRP jest dedykowana tylko do obsługi tego systemu, to znaczy czy jest co najmniej technicznie separowana od pozostałych sieci wewnętrznych i sieci publicznych (w tym sieci Internet)? | TAK / NIE / NIE DOTYCZY |
| 1. Czy styk sieci wewnętrznej SRP z siecią wewnętrzną jednostki jest zrealizowany za pomocą kaskadowego połączenia co najmniej dwóch urządzeń „Router + Firewall sprzętowy” różnych producentów? | TAK / NIE / NIE DOTYCZY |
| 1. Czy każde z urządzeń wymienionych w punkcie 20 posiada co najmniej wdrożone funkcje FW i IDS oraz czy jest objęte aktualnym, bieżącym, dostępnym dla podmiotu wsparciem producenta przynajmniej w zakresie wdrażanych na bieżąco poprawek bezpieczeństwa? | TAK / NIE / NIE DOTYCZY |
| 1. Czy podmiot przechowuje logi z urządzeń wymienionych w punkcie 12 i 20 z okresu co najmniej 12 miesięcy? | TAK / NIE / NIE DOTYCZY |
| 1. Czy dopuszczalne połączenia z/do sieci dostępowej do rejestrów państwowych SRP są ograniczone na urządzeniach Firewall poprzez odpowiednie reguły (porty TCP, UDP) i ograniczone tylko do zezwolonych połączeń z/do odpowiednich numerów IP? | TAK / NIE / NIE DOTYCZY |
| 1. Czy dostęp do integrowanej sieci informatycznej zapewnia kontrolę dostępu z uwierzytelnieniem oraz rozliczalność dostępu do tej sieci np. na poziomie urządzenia sieciowego podłączonego do sieci dostępowej systemu rejestrów państwowych z wykorzystaniem 802.1X, logowanie do urządzenia (komputera)? | TAK / NIE / NIE DOTYCZY |
| 1. Czy urządzenia (np. stacje robocze, urządzenia sieciowe) zapewniające dostęp do sieci dostępowej do SRP są co najmniej wyposażone w oprogramowanie klasy DLP (przeciwdziałające wyciekom informacji), dotyczy sytuacji gdy sieć wewnętrzna jest zintegrowana z sieciami wewnętrznymi wnioskodawcy | TAK / NIE / NIE DOTYCZY |
| 1. Czy inne stacje i serwery oddziałów wnioskodawcy funkcjonują w podsieciach odseparowanych od stacji roboczych SRP (np. poprzez osobne VLAN’y) i nie mają możliwości komunikacji z/do niej w oparciu o konfigurację zewnętrznej zapory sieciowej, chyba że infrastruktura oddziału będzie odwzorowaniem założeń dla siedziby głównej, gdzie lokalne połączenie VPN będzie traktowane jak podłączenie do Warstwy Centralnej SRP? | TAK / NIE / NIE DOTYCZY |
| 1. Czy usługi, z których korzystają użytkownicy stacji komputerowych z dostępem do sieci SRP są ograniczone tylko do niezbędnych do realizacji określonych wymagań, wynikających z wykazanego interesu faktycznego i/lub przepisów prawa? | TAK / NIE / NIE DOTYCZY |
| 1. Czy wnioskodawca posiada zespół monitorujący infrastrukturę w zakresie bezpieczeństwa, reagujący na bieżąco na incydenty i anomalie w godzinach roboczych? | TAK / NIE / NIE DOTYCZY |
|  |  |
| **Połączenia wykorzystujące APN do podłączenia stacji mobilnych**  *Punkty 29-33 wypełniać tylko w przypadku wskazania APN, w przeciwnym przypadku proszę zaznaczyć NIE DOTYCZY.* | TAK / NIE |
| 1. Jaki APN wykorzystywany jest do połączeń mobilnych? | PRYWATNY / PUBLICZNY |
| 1. Czy dostęp realizowany na bazie sieci Internet za pośrednictwem sieci komórkowych (publicznych APN) wymaga zestawienia sprzętowego połączenia VPN do siedziby użytkownika? (Cały ruch sieciowy z urządzenia mobilnego, w szczególności dostęp do treści w sieci Internet, musi przechodzić przez powyższe połączenie VPN przez urządzenie sieciowe w siedzibie użytkownika, być logowany i filtrowany centralnie przez te urządzenia sieciowe zgodnie z przyjętymi lokalnie zasadami - np. filtrowanie i blokowanie niebezpiecznych stron). | TAK / NIE / NIE DOTYCZY |
| 1. Czy połączenie routera do urządzenia mobilnego odbywa się za pomocą wtyku USB lub za pomocą kabla sieciowego? (W routerze musi być trwale wyłączona transmisja bezprzewodowa np. WiFi/Bluetooth - jeśli udostępnia on takie rodzaje transmisji). | TAK / NIE / NIE DOTYCZY |
| 1. Czy stacje mobilne uzyskują jedynie ograniczony, pośredni dostęp do zasobów SRP? (Dostęp realizowany jest poprzez dedykowaną aplikację podmiotu (w tym przypadku działająca na Serwerze Aplikacji), limitującą funkcje i zakres danych do niezbędnego minimum (np. tylko do odczytu, ograniczony zakres pól, uzyskiwanych odpowiedzi etc.)). | TAK / NIE / NIE DOTYCZY |
| 1. Czy karty w ramach prywatnego APN są aktywowane tylko na okres ich wykorzystywania, i dezaktywowane przykładowo po zakończeniu czynności, powrocie do placówki, w przypadku urlopu użytkownika etc.? | TAK / NIE / NIE DOTYCZY |
|  |  |
| **Rozliczalność** | |
| 1. Czy wnioskodawca posiada i stosuje mechanizmy umożliwiające identyfikację i rejestrację osób uzyskujących dostęp do danych oraz rejestrujące zakres udostępnianych danych, dokładną datę i godzinę udostępniania? (na potrzeby badania w przyszłości ewentualnych incydentów bezpieczeństwa)? | TAK / NIE |
| 1. Czy logi dotyczące rozliczalności czynności, miejsc, stanowisk dostępowych, użytkowników itd. będą przechowywane przez okres co najmniej 2 lat? | TAK / NIE |
| 1. Czy wnioskodawca rejestruje cel pozyskania danych (np. poprzez odnotowywanie sygnatury sprawy)? | TAK / NIE |
| 1. Czy infrastruktura przyłączeniowa wnioskodawcy będzie podlegać cyklicznemu audytowi: w przypadku podmiotów komercyjnych nie rzadziej niż raz na 2 lata, a w przypadku podmiotów publicznych nie rzadziej niż raz na 3 lata?   (Celem audytu jest zbadanie zgodności dokumentacji technicznej systemu Wnioskodawcy ze stanem faktycznym oraz ocenę faktycznej konfiguracji zabezpieczeń wraz z testami penetracyjnymi. Audyt musi być przeprowadzany przez podmiot zewnętrzny (przedsiębiorca komercyjny lub ABW) i wykonywany przez certyfikowanych audytorów systemów i sieci IT). | TAK / NIE |

|  |
| --- |
| (Data, pieczęć i podpis wypełniającego)  (osoba/osoby uprawniona do reprezentowania podmiotu wnioskującego) |

1. ustawa z dnia 24 września 2010 r. o ewidencji ludności [↑](#footnote-ref-1)
2. ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych [↑](#footnote-ref-2)
3. ustawa z dnia 27 stycznia 2022 r. o dokumentach paszportowych [↑](#footnote-ref-3)
4. ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne [↑](#footnote-ref-4)