WYMAGANIA I ZALECENIA BEZPIECZEŃSTWA

DLA PODMIOTÓW WNIOSKUJĄCYCH O DOSTĘP DO

Systemu Rejestrów Państwowych

POPRZEZ APLIKACJĘ *ŹRÓDŁO*

Z WYKORZYSTANIEM SIECI DEDYKOWANEJ PESEL-NET MPLS

---

obowiązują od dnia: od dnia 1 marca 2015r.

ŹRÓDŁO
Otwórz, kliknij, załatw sprawę

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

pl.ID

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka

Ministerstwo Spraw Wewnętrznych

COI
centralny ośrodek informatyki

Spis treści

1 WYMAGANIA OCHRONY FIZYCZNEJ POMIESZCZEŃ

Użytkownicy Systemu Rejestrów Państwowych (podmioty, które uzyskały dostęp do SRP) zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182) oraz zawartym z Ministerstwem Spraw Wewnętrznych porozumieniem obowiązani są zapewnić odpowiedni poziom ochrony fizycznej pomieszczeń (zwane dalej *Pomieszczeniami*), w których są stacje robocze przeznaczone do współpracy z SRP, wyposażone m.in. w czytniki mikroprocesorowych kart kryptograficznych i drukarki oraz gdzie przetwarzane i przechowywane są dane i informacje (zwane dalej *Danymi*) pobrane z bazy danych SRP.

W celu zapewnienia odpowiedniego poziomu zabezpieczeń *Pomieszczeń* w szczególności wymagane jest:

1.1 Pomieszczenia i ich lokalizacja

1.1.1 Wymaganie minimalne

- *Pomieszczenia* powinny zapewniać takie rozmieszczenie sprzętu oraz dokumentów aby uniemożliwić dostęp do informacji osobom nie upoważnionym do dostępu do tej informacji (np. wygrodzenia, żaluzje);
- *Pomieszczenia* powinny być zlokalizowane w miejscach gdzie ryzyko ich zatopienia lub zalania jest zminimalizowane.

1.1.2 Zalecane

- *Pomieszczenia*, powinny zapewniać takie rozmieszczenie sprzętu oraz dokumentów aby uniemożliwić dostęp do informacji osobom nie upoważnionym do dostępu do tej informacji i nie powinny być pomieszczeniami przechodnimi;
- *Pomieszczenia* powinny być wyposażone w system alarmowy, czujki wilgoci oraz dymu funkcją powiadomienia do służby ochrony lub jednostek straży pożarnej, policji.

1.2 Kontrola dostępu do Pomieszczeń

1.2.1 Wymaganie minimalne

- Manualna kontrola dostępu do *Pomieszczeń* realizowana jest metodami organizacyjno-proceduralnymi (np. książka pobrań kluczy);
- Dostęp do *Pomieszczeń* mogą mieć tylko osoby upoważnione do przetwarzania danych przez podmiot uprawniony do dostępu do SRP. Inne osoby mogą przebywać w *Pomieszczeniach* jedynie w obecności osób upoważnionych, za ich wiedzą i zgodą.
- Wzór upoważnienia stanowi załącznik do niniejszego dokumentu.

1.2.2 Zalecane

- Zastosowanie systemu elektronicznej kontroli dostępu. Urządzenia automatycznej kontroli dostępu winny być nadzorowane całodobowo przez służbę ochrony i okresowo powinna być wykonywana kontrola logów urządzenia;

- Dostęp do *Pomieszczeń* mogą mieć tylko osoby upoważnione do przetwarzania danych przez podmiot uprawniony do dostępu do SRP. Inne osoby mogą przebywać w *Pomieszczeniach* jedynie w obecności osób upoważnionych, za ich wiedzą i zgodą po odnotowaniu danych osób nieupoważnionych w książce osób nieuprawnionych.
- Wzór upoważnienia stanowi załącznik do niniejszego dokumentu.

1.3 Zabezpieczenie Drzwi i Okien

1.3.1 Wymaganie minimalne

- Drzwi znajdujące się wewnątrz budynku w strefie ograniczonego dostępu (bądź dozorowanej), powinny być wyposażone w co najmniej 1 zamek atestowany (klasa C);
- Drzwi znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej powinny alternatywnie:
    - spełniać wymagania klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 lub
    - być zabezpieczone przed wyważeniem (podważeniem) oraz być wyposażone w co najmniej 1 zamek atestowany (klasa C).
- Drzwi do których dostęp jest z zewnątrz budynku, powinny:
    - spełniać wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010,
    - posiadać co najmniej jeden zamek atestowany (klasa C) lub
    - w pomieszczeniach powinien być zainstalowany system alarmowy z funkcją powiadamiania.
- Okna *Pomieszczeń* zlokalizowanych na parterze lub ostatniej kondygnacji (jeśli jest swobodny dostęp do dachu) o ile nie są zabezpieczone kratami, powinny być oklejone folią antywłamaniową lub powinny być w nich zastosowane szyby o wzmocnionej odporności na zbicie.

1.3.2 Zalecane

- Drzwi znajdujące się wewnątrz budynku w strefie ograniczonego dostępu (bądź dozorowanej) powinny być zabezpieczone przed wyważeniem i wyposażone w co najmniej 1 zamek atestowany (klasa C);
- Drzwi znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej powinny spełniać wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 oraz być wyposażone w co najmniej jeden zamek atestowany (klasa C);
- Drzwi do których dostęp jest z zewnątrz budynku powinny spełniać wymagania co najmniej klasy 3 zgodnie z normą PN-EN14351-1+A1:2010;
- Otwory okienne *Pomieszczeń* zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) powinny być okratowane lub posiadać okna spełniające wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 z szybą klasy P4.

2 WYMAGANIA ZABEZPIECZEŃ DLA SPRZĘTU ORAZ NOŚNIKÓW DANYCH

Mając na uwadze kategorię przetwarzanych danych osobowych oraz zagrożenia, należy zastosować środki bezpieczeństwa na poziomie wysokim w rozumieniu rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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. z 2004 r. Nr 100, poz. 1024).

W celu zapewnienia odpowiedniego poziomu zabezpieczeń sprzętu oraz nośników danych w szczególności wymagane jest:

2.1 Nośniki danych i informacji

2.1.1 Wymaganie minimalne

- Dokumenty i nośniki informacji zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym (np. w zamykanych na klucz szafkach);
- Karty kryptograficzne służące do logowania, należy składować w szafach wyposażonych w co najmniej 1 zamek. Zakazane jest przechowywanie wraz z kartą kodu PIN do karty oraz kodu PUK;
- Do likwidacji wydruków dokumentów i nośników informacji powinny być stosowane niszczarki zgodnie z normą DIN66399 o stopniu tajności 1 lub *Podmiot* winien posiadać stosowną umowę na niszczenie dokumentów z firmą zewnętrzną.

2.1.2 Zalecane

- *Dane* przechowywane na elektronicznych oraz papierowych nośnikach danych powinny być składowane w szafach wyposażonych w co najmniej 1 zamek atestowany (klasa A);
- karty kryptograficzne służące do logowania, powinny być składowane w metalowych szafach wyposażonych w co najmniej 1 zamek atestowany (klasa A) lub sejfach. Zakazane jest przechowywanie wraz z kartą kodu PIN do karty oraz kodu PUK;
- do likwidacji wydruków dokumentów i nośników informacji powinno się stosować niszczarki klasy DIN 2 zgodnie z normą DIN66399 o stopniu tajności 2.

2.2 Sprzęt komputerowy

Lp.	Rodzaj	Implementacja	Uwagi
1	System operacyjny	Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, 8.1	Zastosowany system operacyjny musi wspierać sterowniki urządzeń peryferyjnych niezbędnych do pracy. Data i godzina systemowa musi być zgodna z rzeczywistą.
2	JAVA	Java SE 8 Runtime Environment (JRE) Update 31 lub wersja nowsza.	Niezbędna do uruchamiania appletów w Przeglądarce Internetowej.
3	Oprogramowanie antywirusowe	Dowolny producent.	Oprogramowanie powinno posiadać aktualne definicje i bazy antywirusowe.
4	Czytnik PDF	Acrobat Reader lub inny.	W wersji aktualnej.

5	Przeglądarka Internetowa	Mozilla Firefox (>= 24) Internet Explorer (>= 10.0) Google Chrome (>= 30)	Należy stosować aktualne wersje przeglądarek zawierające wszystkie poprawki bezpieczeństwa udostępnione przez producenta. Stacja robocza musi mieć zainstalowane dodatki umożliwiające uruchamianie apletów języka Java, dla wszystkich wykorzystywanych typów przeglądarek.
6	Sterowniki urządzeń peryferyjnych	Oprogramowanie niezbędne do obsługi, kart, czytników kart kryptograficznych i drukarek.	Sterowniki do obsługi kart powinny być zainstalowane zarówno w systemie jak i przeglądarce internetowej (dot. Mozilla Firefox). Przed zainstalowaniem sterowników, należy upewnić się, że przeglądarki są już zainstalowane.
7	Czytnik kart kryptograficznych	Zgodny ze standardami: ISO/IEC 7816	

2.2.1 Wymagania minimalne

- Konta użytkowników i hasła logowanie hasłami:
  - wbudowane konto administratora należy używać tylko w przypadku wykonywania czynności administratora;
  - konta użytkownika nie mogą mieć uprawnień administratora o ile nie jest to wymagane przy bieżącej pracy;
  - długość nazwy użytkownika nie mniej niż 6 znaków;
  - długość hasła konta administratora lub użytkownika z uprawnieniami administratora nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni;
  - długość hasła konta użytkownika nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni.
- Ochrona antywirusowa:
  - oprogramowanie antywirusowe instalowane na stacjach przetwarzających dane działające w czasie rzeczywistym;
  - ustawienie oprogramowania zapewniające bieżącą aktualizację sygnatur antywirusowych.
- Usuwanie danych:
  - Po skasowaniu danych należy opróżnić „kosz” systemowy.
- Dyski i urządzenia przenośne:
  - przenośne pamięci flash oraz dyski przenośne które będą służyły do wynoszenia informacji poza obręb pomieszczenia muszą być wyposażone w oprogramowanie lub rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) lub w czytnik identyfikacji biometrycznej.
- Rozmieszczenie sprzętu:
  - stacja powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym;
  - wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na max 5 minut, wznowienie pracy wymaga podania hasła, zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska;
  - wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.

2.2.1.1 Dodatkowe minimalne wymagania dot. komputerów stacjonarnych:

- Dyski i urządzenia przenośne:
  - w przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach muszą być one wyposażone w zamknięcie na kluczyk i zamknięte gdy znajduje się w nich dysk. Po zakończonej pracy zalecane jest usunięcie dysku i jego dalsze przechowywanie w zabezpieczonej szafie.
- Rozmieszczenie sprzętu:
  - wymagane jest takie ustawienie monitora aby nie było możliwości podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione.

2.2.1.2 Dodatkowe minimalne wymagania dot. komputerów przenośnych:

Sprzęt komputerowy przenośny może być używany do pracy z SRP.
Ze względu na zwiększone ryzyko związane z utratą danych podczas przenoszenia sprzętu, stosowanie tego rozwiązania jest NIE ZALECANE i powinno być ograniczone tylko do uzasadnionych przypadków.

- Wprowadzenie w BIOS/UEFI następujących ustawień:
  - wejście i zmiana ustawień BIOS/UEFI wymaga podania hasła;
  - wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera;
  - długość hasła BIOS/UEFI nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra).
- Dyski i urządzenia przenośne:
  - dane składowane na dysku stacji przenośnej muszą być umieszczone w obszarze podlegającym szyfrowaniu lub być szyfrowane.
- Rozmieszczenie sprzętu:
  - wymagane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione.

2.2.1.3 Dodatkowe minimalne wymagania dot. środowisk wirtualnych (maszyny wirtualne):

Maszyny wirtualne mogą być używane do pracy z SRP.

Ze względu na zwiększone ryzyko związane z utratą danych podczas przenoszenia sprzętu, stosowanie tego rozwiązania jest NIE ZALECANE i powinno być ograniczone tylko do uzasadnionych przypadków.

- Zabezpieczenia serwerów/stacji udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej muszą być co najmniej na poziomie minimalnym opisanym w sekcji sprzętu komputerowego;
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego musi zostać ograniczony tylko do użytkowników maszyny wirtualnej;
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny innej osobie niż Administrator;
- Stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash **nie jest zalecane.** W przypadku konieczności stosowania takiego rozwiązania zalecane jest:
  - nośnik plików maszyny wirtualnej jest w całości zaszyfrowany;
  - należy wdrożyć regulacje zapewniające prawidłowe posługiwanie się oraz prowadzić ewidencję obsługi dysków przenośnych bądź pamięci flash;

- nośniki nie są wynoszone po za obręb *Pomieszczenia* lub muszą być wyposażone w rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 5 próbach nieudanego podania hasła do odblokowania nośnika.

2.2.2 Dodatkowe rekomendowane zalecenia

- Wprowadzenie w BIOS/UEFI następujących ustawień:
  - wejście i zmiana ustawień BIOS/UEFI wymaga podania hasła;
  - uruchomienie komputera wymaga podania hasła;
  - wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera;
  - długość hasła BIOS/UEFI nie mniej niż 10 znaków (co najmniej 1 duża litera i 1 cyfra).
- Konta użytkowników i hasła logowania:
  - każdemu użytkownikowi komputera należy założyć oddzielne konto;
  - długość hasła konta administratora lub użytkownika z uprawnieniami administratora nie mniej niż 15 (hasło złożone co najmniej: 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni;
  - długość hasła konta użytkownika nie mniej niż 10 (hasło złożone co najmniej: 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni;
  - zastąpienie logowania tradycyjnego (login i hasło) logowaniem z użyciem kart mikroprocesorowych, czytników cech biometrycznych, kluczy bezprzewodowych.
- Ochrona antywirusowa:
  - ustawienie oprogramowania zapewniające pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu.
- Aktualizacja systemu i oprogramowania:
  - włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów (opcja pobierz aktualizacje i zdecyduj kiedy/które zainstalować).
- Usuwanie danych:
  - do usuwania danych należy używać wyspecjalizowanego oprogramowania;
  - ustawić opcję automatycznego czyszczenia „kosza” systemowego.
- Kopie bezpieczeństwa:
  - składowanie kopii bezpieczeństwa powinno odbywać się w innym budynku bądź pomieszczeniach w odpowiednio zabezpieczonej szafie.
- Zasilanie awaryjne:
  - stacje powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) umożliwiające automatyczne bezpieczne zamknięcie stacji w przypadku wyczerpania się akumulatora.

2.2.2.1 Dodatkowe zalecenia dot. komputerów stacjonarnych:

- Rozmieszczenie sprzętu
  - zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione.

2.2.2.2 Dodatkowe zalecenia dot. komputerów przenośnych:

- Wprowadzenie w BIOS/UEFI następujących ustawień:

    - używanie do logowania kart mikroprocesorowych bądź czytników biometrycznych.
- Konta użytkowników i hasła logowanie hasłami:
    - długość nazwy użytkownika nie mniej niż 8 znaków;
    - należy wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.
- Dyski i urządzenia przenośne:
    - partycja lub dysk stacji przenośnej na której są składowane dane jest w całości zaszyfrowany.
- Rozmieszczenie sprzętu:
    - stacje przenośne w miejscach korzystania, należy zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe).
- Zasilanie awaryjne:
    - w przypadku pracy na zasilaniu bateryjnym stan baterii stacji przenośnej ma umożliwić bezpieczne zamknięcie systemu po zaniku zasilania sieciowego.

2.2.2.3 Dodatkowe zalecenia dot. środowisk wirtualnych (maszyny wirtualne):

- Zabezpieczenia serwerów udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej są na poziomie nie mniejszym niż Zalecane opisanym w sekcji minimalnych wymagań oraz dodatkowych zaleceń rekomendowanych**;**
- Stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash **nie jest zalecane**. W przypadku konieczności stosowania rozwiązania zalecane jest:
    - nośniki nie są wynoszone po za obręb *Pomieszczenia* lub muszą być wyposażone w rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 10 znaków (hasło złożone co najmniej: 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 3 próbach nieudanego podania hasła do odblokowania nośnika.

3 INCYDENTY BEZPIECZEŃSTWA

Przypadki naruszenia bezpieczeństwa teleinformatycznego dot. SRP należy niezwłocznie zgłaszać w formie zawiadomienia pisemnego (niezależnie od własnych polityk i procedur) do Departamentu Teleinformatyki, Ministerstwa Spraw Wewnętrznych. Wzór zgłoszenia incydentu bezpieczeństwa stanowi załącznik do niniejszego dokumentu.

- fax: 22 6028081
- adres email: incydent@msw.gov.pl

Zgłaszanie błędów i usterek:

- adres: https://pomoc.coi.gov.pl ITSM Atmosfera

Pytania lub wątpliwości prosimy kierować do Zespołu Service Desk COI:

- tel.: 42 2535499
- adres e-mail: pomoc.plid@coi.gov.pl

4 POSTANOWIENIA KOŃCOWE

Powyższe regulacje nie zwalniają użytkownika systemu z posiadania dokumentacji określonej w art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182)**.**

W przypadku naruszenia bezpieczeństwa danych osobowych odpowiedzialność za te dane, ponosi użytkownik systemu, który był zalogowany do systemu w czasie, gdy dane te zostały pobrane z SRP. Za dalsze przetwarzanie danych uzyskanych na drodze teletransmisji odpowiedzialność ponosi użytkownik systemu.

ZABRONIONE jest udostępnianie kart kryptograficznych służących do logowania innym osobom niż upoważnione a także innym użytkownikom systemu.

Załączniki:

Nr 1 – Wzór zgłoszenia incydentu bezpieczeństwa,

Nr 2 – wzór upoważnienia do przetwarzania danych