Polityka Bezpieczeństwa Systemu Informatycznego Centralnej Ewidencji Pojazdów i Kierowców 2.0

Wymagania, zalecenia i wytyczne bezpieczeństwa dla Stacji Kontroli Pojazdów

wersja 1.00 z dnia 03.10.2017 r.

obowiązują od dnia: 13 listopada 2017 r.

Spis treści

1. Użytkownicy Instytucjonalni – Stacje Kontroli Pojazdów

Użytkownikiem jest każda osoba lub podmiot uprawniony na podstawie przepisów prawa do dostępu do centralnej ewidencji pojazdów (CEP), centralnej ewidencji kierowców (CEK) lub centralnej ewidencji posiadaczy kart parkingowych (CEPKP), posiadająca w Systemie Informatycznym Centralnej Ewidencji Pojazdów i Kierowców 2.0 (SI CEPiK 2.0) jednoznacznie identyfikujące taką osobę lub podmiot konto.

Użytkownicy Instytucjonalni to kategoria Użytkowników SI CEPiK 2.0, którzy korzystają z systemów lub aplikacji dziedzinowych zintegrowanych z SI CEPiK 2.0 z wykorzystaniem usług sieciowych (web services).

Stacja Kontroli Pojazdów (SKP) to wydzielona kategoria Użytkowników Instytucjonalnych SI CEPiK 2.0, którzy korzystają z systemów lub aplikacji dziedzinowych zintegrowanych z SI CEPiK 2.0 z wykorzystaniem usług sieciowych (web services). SKP zgodnie z przepisami prawa posiadają dostęp do danych przetwarzanych w CEP w ograniczonym zakresie tj. z wyłączeniem danych osobowych, jedynie do danych technicznych pojazdów, danych i informacji o badaniach technicznych oraz innych określonych szczegółowo w przepisach prawa.

W dokumencie zdefiniowano wymagania, zalecenia i rekomendacje, których spełnienie pozwoli chronić system informatyczny oraz dane w nim przetwarzane przed nieuprawnionym wprowadzeniem czy modyfikacją.

WYMAGANIA – muszą być stosowane

ZALECENIA – powinny być stosowane

REKOMENDACJE – rekomenduje się stosowanie

2. Środki ochrony kryptograficznej

W SI CEPiK 2.0 stosowane są środki kryptograficznej ochrony danych. SKP, aby skorzystać z usług SI CEPiK 2.0, musi posiadać odpowiedni certyfikat dostępowy zawierający jego dane i w sposób jednoznaczny go identyfikujący. Ponadto, w związku z łączeniem się SKP z SI CEPiK 2.0 przez sieć publiczną Internet, SKP musi posiadać certyfikat umożliwiający zestawienie bezpiecznego połączenia VPN z SI CEPiK 2.0. Szczegółowy sposób uzyskania certyfikatów, ich wymiany, zasady ochrony kluczy prywatnych oraz inne informacje i wymagania związane z certyfikatami są opisane w dokumentach:

- *Polityka certyfikacji dla infrastruktury systemu informatycznego CEPiK 2.0;*
- *Polityka certyfikacji dla operatorów systemu informatycznego CEPiK 2.0.*

W ramach polityki certyfikacji dla infrastruktury systemu informatycznego CEPiK 2.0 wydawane są certyfikaty wykorzystywane przy zestawianiu połączeń VPN (certyfikaty VPN).

W ramach polityki certyfikacji dla operatorów systemu informatycznego CEPiK 2.0 wydawane są certyfikaty dla SKP służące do autoryzacji, uwierzytelniania, podpisywania komunikatów i terminowania sesji SSL (certyfikaty SSL).

Dodatkowo, w ramach polityki certyfikacji dla operatorów systemu informatycznego CEPiK 2.0 wydawane są certyfikaty dla Brokerów SKP służące do autoryzacji, uwierzytelniania i terminowania sesji SSL (certyfikaty SSL Brokera). Certyfikaty te są wykorzystywane w przypadku rozwiązań informatycznych, w których komunikacja z SI CEPiK 2.0 jest realizowana centralnie przez dostawcę takiego rozwiązania informatycznego. Rozwiązanie centralne jest w tym przypadku pośrednikiem w komunikacji SKP z SI CEPiK 2.0.

ZABRONIONE JEST EKSPORTOWANIE PRZEZ SKP KLUCZY PRYWATNYCH Z KART KRYPTOGRAFICZNYCH DO PLIKU, PRZECHOWYWANIE TAKICH PLIKÓW NA STANOWISKU KOMPUTEROWYM, W SZCZEGÓLNOŚCI IMPORTOWANIE DO PRZEGLĄDARKI INTERNETOWEJ, SYSTEMU OPERACYJNEGO LUB INNEGO OPROGRAMOWANIA. KLUCZ PRYWATNY MUSI ZNAJDOWAĆ SIĘ NA KARCIE KRYPTOGRAFICZNEJ.

NA STANOWISKU DOSTĘPOWYM SKP MOŻE BYĆ ZAIMPORTOWANY WYŁĄCZNIE KLUCZ PRYWATNY I ODPOWIADAJĄCY MU CERTYFIKAT DO POŁĄCZEŃ VPN, PRZY CZYM ZAWSZE NALEŻY ZABEZPIECZYĆ HASŁEM O WYSOKIM POZIOMIE TRUDNOŚCI MOŻLIWOŚĆ EKSPORTU TAKIEGO KLUCZA PRYWATNEGO Z SYSTEMU OPERACYJNEGO, OPROGRAMOWANIA VPN LUB URZĄDZENIA SIECIOWEGO.

ZABRONIONE JEST UDOSTĘPNIANIE KART KRYPTOGRAFICZNYCH, KODÓW PIN / PUK ORAZ CERTYFIKATÓW VPN INNYM OSOBOM LUB PODMIOTOM NIEUPRAWNIONYM DO ICH POSIADANIA.

3. Połączenie z SI CEPiK 2.0

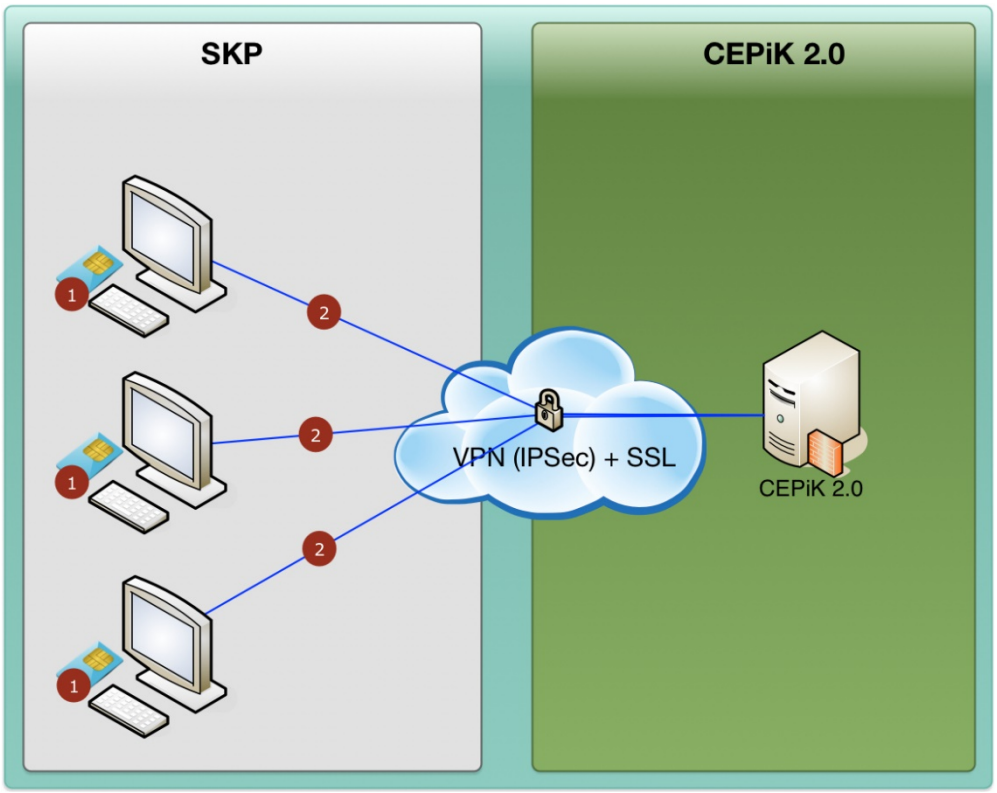
SI CEPiK 2.0 umożliwia SKP łączenie się do usług sieciowych (web services) przez sieć publiczną Internet.

SKP / Broker SKP łączące się z SI CEPiK 2.0 przez sieć publiczną Internet muszą zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu VPN. Dopiero po zestawieniu połączenia VPN Użytkownik uzyska możliwość wywołania usług sieciowych SI CEPiK 2.0. Autoryzacja i uwierzytelnienie SKP / Brokera SKP w usługach sieciowych SI CEPiK 2.0 są realizowane w oparciu o posiadany przez SKP / Brokera SKP certyfikat SSL / certyfikat SSL Brokera umieszczony na mikroprocesorowej karcie kryptograficznej. Dopuszcza się, aby certyfikat Brokera SKP był zainstalowany w systemie / aplikacji centralnej, przy czym należy wdrożyć środki techniczne i organizacyjne zabezpieczające klucz prywatny przed jego utratą i kompromitacją.

System CEPiK 2.0 wspiera rozwiązanie programowe Cisco AnyConnect i komunikację VPN typu Remote Access. Dla tych rozwiązań Service Desk dla SI CEPiK 2.0 zapewni wsparcie związane z instalacją oraz konfiguracją oprogramowania na stanowisku dostępowym.

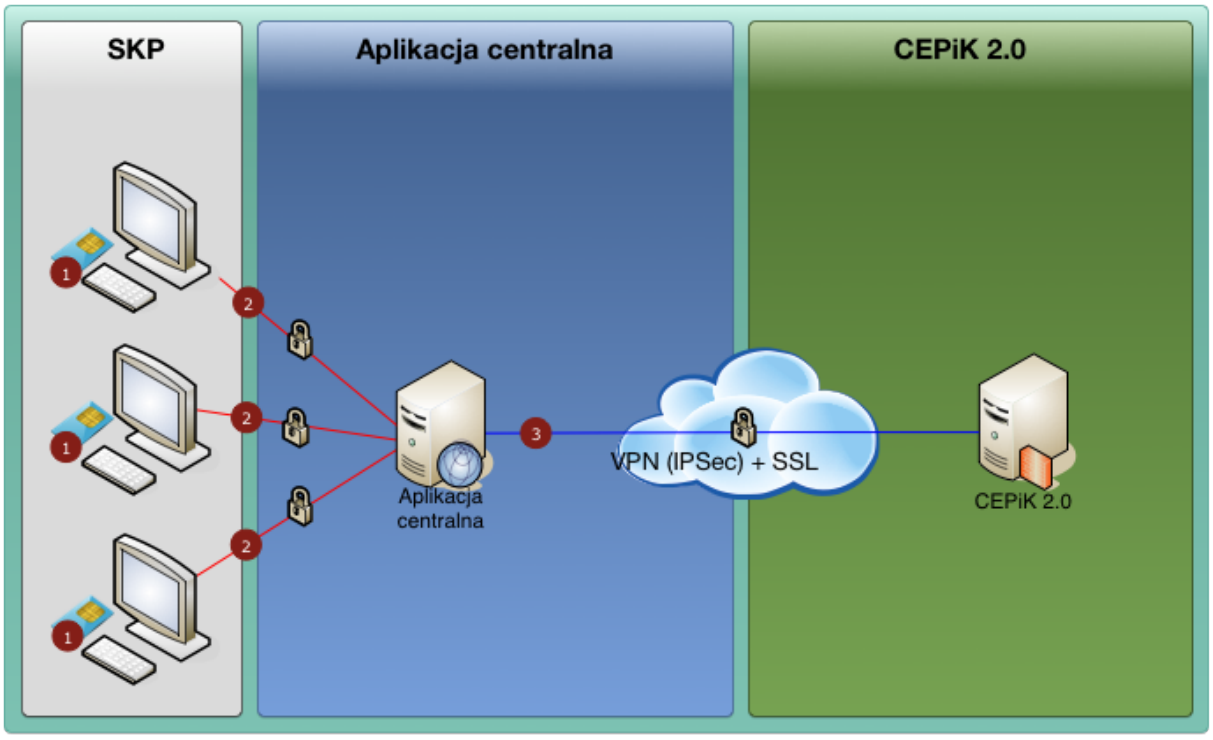
System CEPiK 2.0 wyłącznie dopuszcza połączenia VPN typu Lan-to-Lan (L2L), przy czym ich nie wspiera. Każda SKP / Broker SKP decydujący się na takie połączenie zestawia je we własnym zakresie, na podstawie podanych parametrów konfiguracyjnych połączenia. Przed implementacją takiego rozwiązania należy skontaktować się z Service Desk dla SI CEPiK 2.0 lub Biurem Programu CEPiK 2.0 w celu poinformowania o chęci skorzystania z połączenia L2L oraz otrzymania niezbędnych danych i informacji, które umożliwią konfigurację urządzeń po stronie Użytkownika. Service Desk dla SI CEPiK 2.0 nie będzie świadczył pomocy w dalszej konfiguracji połączenia po stronie Użytkownika.

Schemat podłączenia bezpośredniego SKP do CEPiK 2.0 prezentuje poniższy rysunek:



Dostęp do systemu CEPiK 2.0 dla SKP realizowany będzie poprzez sieć publiczną Internet za pomocą połączenia VPN [2]. Dodatkowo wszystkie komunikaty wymieniane pomiędzy systemami używać będą szyfrowanej transmisji wykorzystującej protokół SSL oraz symetryczny klucz szyfrujący [1]. Do poprawnej komunikacji z systemem tym kanałem wymagane będzie posługiwanie się wydanymi przez MC certyfikatem niezbędnym do połączenia VPN oraz certyfikatem SSL.

Schemat podłączenia pośredniego SKP do CEPiK 2.0 za pośrednictwem aplikacji centralnej (Brokera SKP) prezentuje poniższy rysunek:



W przypadku komunikacji SKP przez aplikację centralną pełniącą rolę brokera komunikacyjnego SKP musi posiadać certyfikat SSL, wystawiony przez MC dla Stacji Kontroli Pojazdów na kartach kryptograficznych zabezpieczonych kodem PIN [1]. SKP nie musi posiadać certyfikatu VPN.

Połączenie pomiędzy aplikacją centralną a stanowiskiem komputerowym [2] w SKP (w rozumieniu – cienki/gruby klient, połączenie terminalowe, itp.) wymaga zabezpieczenia połączenia SSL z kluczem nie krótszym niż 2048 bity. Certyfikat kliencki, którym będzie szyfrowana komunikacja – nie będzie certyfikatem zbiorczym – każda stacja łącząca się do aplikacji centralnej będzie posiadała swój certyfikat.

Za zabezpieczenie połączenia między SKP a aplikacją centralną odpowiada dostawca tej aplikacji centralnej.

Między aplikacją centralną dostawcy oprogramowania a systemem CEPiK 2.0 wymagane jest zabezpieczone połączenie VPN (IPSec) [3] zestawione z wykorzystaniem certyfikatu wydanego przez MC dla dostawcy aplikacji centralnej jako brokera komunikatów do systemu CEPiK 2.0.

Przesyłanie komunikatów poprzez aplikację centralną dostawcy wymaga, aby każdy komunikat przesyłany i odbierany z systemu CEPiK 2.0 był podpisany certyfikatem diagnosty [1] – nie obejmuje to metod do pobierania danych słownikowych, które nie wymagają podpisu cyfrowego.

Aplikacja centralna dostawcy oprogramowania musi korzystać z własnego certyfikatu SSL – o ten certyfikat wnioskuje dostawca oprogramowania.

Każda Stacja Kontroli Pojazdów, jeżeli planuje korzystać z centralnej aplikacji do przekazywania informacji do CEPiK 2.0, musi zgłosić ten fakt do MC, wskazując dostawcę oprogramowania z którego będzie korzystała – informację należy podać we wniosku o wydanie certyfikatu (w polu Podstawa prawna wnioskowania o certyfikat, obok wskazania tej podstawy) lub przesłać mailem na adres adm.cepik@mc.gov.pl dw biurocepik2.0@mc.gov.pl. Informacja ta będzie konieczna do poprawnego uwierzytelnienia użytkownika w systemie CEPiK 2.0 (bez podania tej informacji SKP nie zostaną nadane uprawnienia w systemie).

BARDZO WAŻNE: KAŻDA SKP KORZYSTAJĄCA Z APLIKACJI CENTRALNEJ / BROKERA SKP (CHMURY) MUSI POSIADAĆ Z TAKIM DOSTAWCĄ UMOWĘ REGULUJĄCĄ M.IN. ZASADY POWIERZENIA DANYCH I PRZETWARZANIA ICH W CHMURZE, KONIECZNOŚĆ SPEŁNIENIA WYMAGAŃ W ZAKRESIE INTEGRACJI Z CEPiK 2.0 (ZGODNIE Z PRZEPISAMI TO SKP JEST PODMIOTEM ZOBOWIĄZANYM) ORAZ UPOWAŻNIENIE DLA DOSTAWCY UMOŻLIWIAJĄCE PRZEKAZYWANIE PRZEZ TEGO DOSTAWCĘ DANYCH DO CEPiK 2.0 W IMIENIU DANEGO SKP.

4. Wymagania, zalecenia i rekomendacje bezpieczeństwa dla Stacji Kontroli Pojazdów

4.1. [Rekomendacje] Ochrona fizyczna *Pomieszczeń*, w których zlokalizowane będzie stanowisko komputerowe z dostępem do SI CEPiK 2.0

4.1.1. *Pomieszczenia* i ich lokalizacja

- rekomenduje się, aby *Pomieszczenia* były zlokalizowane w miejscach, gdzie ryzyko ich zatopienia lub zalania jest zminimalizowane;
- rekomenduje się, aby *Pomieszczenia* były wyposażone w system alarmowy, czujki wilgoci oraz dymu z funkcją powiadomienia do służby ochrony lub jednostek straży pożarnej, policji;

4.1.2. Kontrola dostępu do *Pomieszczeń*

- rekomenduje się, aby osoby nie będące pracownikami SKP przebywały w *Pomieszczeniach* wyłącznie w obecności osób uprawnionych, za ich wiedzą i zgodą;

4.1.3. Zabezpieczenie drzwi i okien

- rekomenduje się, aby drzwi do *Pomieszczeń* znajdujące się wewnątrz budynku w strefie ograniczonego dostępu (bądź dozorowanej), były wyposażone w co najmniej 1 zamek atestowany (zabezpieczenie i odporność na przewiercenie wg PN-EN 12209:2016-04 – klasa 3 lub odporność na włamanie wg KT/402/IMP:2014 – klasa C lub odporność na atak wg PN-EN 1303:2015-07 – klasa 2);
- rekomenduje się, aby drzwi do *Pomieszczeń* znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej alternatywnie:
    - spełniały wymagania klasy RC 2 zgodnie z normą PN-EN 1627 lub
    - były zabezpieczone przed wyważeniem (podważeniem) oraz były wyposażone w co najmniej 1 zamek atestowany (klasa 3 / klasa C / klasa 2);
- rekomenduje się, aby drzwi do *Pomieszczeń*, do których dostęp jest z zewnątrz budynku:
    - spełniały wymagania co najmniej klasy RC 2 zgodnie z normą PN-EN 1627, oraz
    - posiadały co najmniej jeden zamek atestowany (klasa 3 / klasa C / klasa 2) lub
- rekomenduje się, aby w Pomieszczeniach był zainstalowany system alarmowy z funkcją powiadamiania;
- rekomenduje się, aby otwory okienne *Pomieszczeń* zlokalizowanych na parterze lub ostatniej kondygnacji (jeśli jest swobodny dostęp do dachu) o ile nie są zabezpieczone kratami:

- były oklejone folią antywłamaniową lub
- posiadały zastosowane szyby o wzmocnionej odporności na zbicie;

4.2. Zabezpieczenia nośników danych

W celu zapewnienia odpowiedniego poziomu ochrony danych przechowywanych na nośnikach danych, w szczególności wymagane jest spełnienie poniżej określonych wymagań.

- **[wymaganie] karty kryptograficzne wykorzystywane do łączenia się z SI CEPiK 2.0, gdy nie są wykorzystywane np. po zakończonej pracy, muszą być składowane np. w zamkniętej szafie lub innym miejscu pozwalającym na zabezpieczenie dostępu do nich przed osobami nieuprawnionymi (np. sejf, zamykana szuflada);**
- [zalecenie] dokumenty i nośniki informacji należy przechowywać w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym (np. w zamykanych na klucz szafkach);
- [zalecenie] do likwidacji wydruków dokumentów i nośników informacji zaleca się stosować niszczarki zgodnie z normą DIN66399 o klasie ochrony A i stopniu bezpieczeństwa 1 lub wyższym;

ZAKAZANE JEST PRZECHOWYWANIE WRAZ Z KARTĄ KRYTOGRAFICZNĄ KODU PIN ORAZ KODU PUK (PIN ADMINISTRACYJNY) DO TEJ KARTY.

ZABRONIONE JEST UDOSTĘPNIANIE KART KRYPTOGRAFICZNYCH, KODÓW PIN / PUK ORAZ CERTYFIKATÓW VPN INNYM OSOBOM LUB PODMIOTOM NIEUPRAWNIONYM DO ICH POSIADANIA.

4.3. [Zalecenia] Zabezpieczenia urządzeń sieciowych

4.3.1. Zalecenia w zakresie konfiguracji urządzeń i oprogramowania

- urządzenia sieciowe pozwalające na zestawienie połączeń VPN powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
    - klucze prywatne do certyfikatów VPN zainstalowanych w urządzeniu musza być zabezpieczone w sposób uniemożliwiający dostęp do nich oraz ich wykorzystanie przez osoby nieuprawnione;
    - administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności);
    - administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia;
    - zaleca się wdrożenie reglamentacji dostępu do sieci np. na podstawie adresów MAC;
- zaleca się wdrożenie polityki blokowania dostępu do i z sieci publicznej Internet w czasie, w którym jest nawiązane połączenie VPN do SI CEPiK 2.0;
- oprogramowanie służące do zestawiania połączeń VPN typu Remote Access np. Cisco AnyConnect powinno być zabezpieczone w taki sposób, aby uniemożliwić dostęp do kluczy prywatnych do certyfikatów VPN osobom nieuprawnionym;

4.3.2. Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń

- urządzenia sieciowe powinny być zlokalizowane w pomieszczeniu lub przeznaczonej do tego celu szafie z ograniczonym dostępem osób trzecich. Dostęp do tego pomieszczenia lub szafy powinien mieć wyłącznie administrator urządzenia lub osoby upoważnione.

4.4. Sprzęt komputerowy stacjonarny

4.4.1. WYMAGANIA MINIMALNE

4.4.1.1. BIOS/UEFI

- 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 wynosi nie mniej niż 6 znaków (co najmniej 1 duża litera i 1 cyfra);

4.4.1.2. Konta użytkowników i hasła

- wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora;
- każdemu użytkownikowi komputera ma być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora, o ile nie jest to wymagane do bieżącej pracy;
- długość nazwy użytkownika powinna wynosić nie mniej niż 3 znaki;
- długość hasła konta administratora lub użytkownika z uprawnieniami administratora ma wynosić nie mniej niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie może być dłuższy niż 30 dni;
- długość hasła konta użytkownika ma wynosić 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;
- zaleca się wprowadzić procedury sankcjonujące zmianę PIN mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni;
- należy wprowadzić procedury sankcjonujące bezpieczne przechowywanie haseł oraz kart i PIN / PUK, w szczególności zabraniające udostępnia ich innym osobom;

4.4.1.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- zalecane jest zastosowanie zapory ogniowej (rozwiązanie sprzętowe lub programowe) oraz wdrożenie regulacji zapewniających jej bieżącą aktualizację;

4.4.1.4. Sieci Wi-Fi

- do połączenia z sieciami Wi-Fi należy używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny);

4.4.1.5. Ochrona antywirusowa

- należy obowiązkowo stosować oprogramowanie antywirusowe oraz:
    - stosować ustawienia zapewniające aktualizację sygnatur antywirusowych na bieżąco lub

    - w przypadku braku dostępu do sygnatur antywirusowych na bieżąco, wdrożyć procedury zapewniające aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu;
- zalecana jest konfiguracja ustawień oprogramowania antywirusowego zapewniająca pełne skanowanie antywirusowe komputera:
    - co najmniej raz w tygodniu w przypadku braku aktualizacji sygnatur na bieżąco lub
    - co najmniej raz w miesiącu, w przypadku aktualizacji sygnatur na bieżąco;
- konfiguracja oprogramowania antywirusowego ma wymuszać skanowanie każdego zewnętrznego nośnika danych (przenośny dysk twardy, pamięć flash) po jego podłączeniu do komputera;

4.4.1.6. Aktualizacja systemu i oprogramowania

- należy stosować systemy operacyjne oraz inne oprogramowanie tylko pochodzące z legalnego źródła, w wersjach posiadających wsparcie producenta co najmniej w zakresie poprawy błędów związanych z bezpieczeństwem;
- zalecana jest konfiguracja ustawień systemu operacyjnego zapewniająca:
    - aktualizację systemu na bieżąco, nie rzadziej niż raz na tydzień, lub
    - w przypadku braku dostępu do repozytorium poprawek online, wdrożenie procedury zapewniającej aktualizację systemu operacyjnego nie rzadziej niż raz w tygodniu;

4.4.1.7. Usuwanie danych

- po kasowaniu danych należy opróżnić „kosz" systemowy;
- zaleca się konfigurację „kosza" systemowego w taki sposób, aby nie przechowywał usuniętych plików;

4.4.1.8. Dyski i urządzenia przenośne

- w przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach, powinny 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;
- należy wdrożyć regulacje zapewniające obsługę pamięci flash oraz dysków przenośnych zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywać w bezpieczny sposób;
- przenośne pamięci flash oraz dyski przenośne, które będą służyły do wynoszenia informacji poza obręb pomieszczenia powinny być wyposażone w rozwiązanie sprzętowe lub programowe umożliwiające szyfrowanie danych z użyciem hasła nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny);

4.4.1.9. Rozmieszczenie sprzętu

- wymagane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione;

- stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieuprawnionym;
- wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut, wznowienie pracy wymaga podania hasła, obowiązkowe jest blokowanie stacji przez Użytkownika przy każdorazowym opuszczeniu stanowiska;
- wymagane jest takie ustawienie drukarki, aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione;

4.4.1.10. Kopie bezpieczeństwa

- zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii bezpieczeństwa nie rzadziej niż raz na 30 dni;

4.4.2. WYMAGANIA DODATKOWE

4.4.2.1. BIOS/UEFI

- uruchomienie komputera wymaga podania hasła;
- długość hasła BIOS wynosi nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra);

4.4.2.2. Konta użytkowników i hasła

- długość nazwy użytkownika powinna wynosić nie mniej niż 6 znaków,
- długość hasła konta administratora lub użytkownika z uprawnieniami administratora powinna wynosić nie mniej niż 12 (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni;
- długość hasła konta użytkownika powinna wynosić nie mniej niż 8 (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie powinien być dłuższy niż 30 dni;
- zalecane jest zastąpienie logowania tradycyjnego (login i hasło) logowaniem z użyciem kart mikroprocesorowych, czytników cech biometrycznych, kluczy bezprzewodowych;

4.4.2.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- zaleca się zastosowanie 2 zapór ogniowych – sprzętowej na styku z siecią publiczną Internet oraz programowej na stacji roboczej, oraz wdrożenie regulacji zapewniających ich bieżącą aktualizację;

4.4.2.4. Sieci Wi-Fi

- do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA2 i haseł o długości nie mniejszej niż 14 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny);

4.4.2.5. Ochrona antywirusowa

- zaleca się konfigurację oprogramowania zapewniającą pełne skanowanie antywirusowe stanowiska dostępowego co najmniej raz w tygodniu;

4.4.2.6. Aktualizacja systemu i oprogramowania

- zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania, zgodnie z zaleceniami producentów, a w przypadku braku dostępu do repozytorium poprawek online wdrożenie procedury aktualizacji systemu oraz oprogramowania na bieżąco;

4.4.2.7. Usuwanie danych

- zaleca się do usuwania danych, w szczególności tych zapisanych na nośnikach przenośnych, używać dedykowanego do tego celu oprogramowania;

4.4.2.8. Dyski i urządzenia przenośne

- przenośne pamięci flash oraz dyski przenośne które będą służyły do wynoszenia informacji poza obręb *Pomieszczenia* powinny 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) lub w czytnik identyfikacji biometrycznej;

4.4.2.9. Rozmieszczenie sprzętu

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

4.4.2.10. Kopie bezpieczeństwa

- zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii zapasowej nie rzadziej niż raz na 7 dni;
- składowanie kopi zapasowych powinno odbywać się w innym budynku lub pomieszczeniach w odpowiednio zabezpieczonej szafie;

4.4.2.11. Zasilanie awaryjne

- stacje robocze powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) lub wpięte do sieci gwarantowanej (z zapewnionym podtrzymaniem napięcia w przypadku utraty zasilania podstawowego) umożliwiające automatyczne bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.

4.5. Środowiska wirtualne (maszyny wirtualne)

4.5.1. WYMAGANIA MINIMALNE

- zabezpieczenia serwerów/stacji udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej muszą być co najmniej na poziomie minimalnym opisanym w rozdziale 4.4**Error! Reference source not found.**;
- uprawnienia do katalogu oraz dostęp do folderu udostępnianego należy ograniczyć tylko do użytkowników maszyny wirtualnej;
- uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż administrator;
- stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash **jest niezalecane**. W przypadku konieczności stosowania takiego rozwiązania zaleca się, aby:
    - nośnik plików maszyny wirtualnej był w całości zaszyfrowany;
    - wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami oraz prowadzić ewidencję dysków przenośnych lub pamięci flash;
    - nośniki nie powinny być wynoszone poza obszar przetwarzania danych lub muszą być wyposażone w rozwiązanie 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 maksymalnie 5 próbach nieudanego podania hasła do odblokowania nośnika.

4.6. Sprzęt komputerowy przenośny (laptop, tablet, itp.)

Sprzęt komputerowy przenośny może być używany do pracy z SI CEPiK 2.0. Ze względu na zwiększone ryzyko związane z utratą danych podczas przenoszenia sprzętu, stosowanie tego rozwiązania **jest NIEZALECANE** i powinno być ograniczone tylko do uzasadnionych przypadków.

W przypadku korzystania z komputerów przenośnych zalecane jest stosowanie zabezpieczeń opisanych w wymaganiach minimalnych oraz wymaganiach dodatkowych.

4.6.1. WYMAGANIA MINIMALNE

4.6.1.1. BIOS/UEFI

- wymagane jest stosowanie ustawień wymagań w rozdziale 4.4.1.1, przy czym długość hasła BIOS/UEFI musi być nie krótsza niż 8 znaków;

4.6.1.2. Konta użytkowników i hasła

- wymagane jest stosowanie wymagań opisanych w rozdziale 4.4.1.2;

4.6.1.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- wymagane jest stosowanie wymagań opisanych w rozdziale 4.4.1.3;

4.6.1.4. Sieci Wi-Fi

- wymagane jest stosowanie wymagań opisanych w rozdziale 4.4.1.4;
- **zabronione jest korzystanie z otwartych lub publicznych sieci Wi-Fi, które nie są siecią wewnętrzną Użytkownika**;

4.6.1.5. Ochrona antywirusowa

- wymagane jest stosowanie wymagań opisanych w rozdziale 4.4.1.5;

4.6.1.6. Aktualizacja systemu i oprogramowania

- wymagane jest stosowanie wymagań opisanych w rozdziale 4.4.1.6;

4.6.1.7. Usuwanie danych

- wymagane jest stosowanie wymagań opisanych w rozdziale 4.4.1.7;

4.6.1.8. Dyski i urządzenia przenośne

- wymagane jest stosowanie wymagań opisanych w rozdziale 4.4.1.8;
- dane składowane na dysku stacji przenośnej muszą być umieszczone w obszarze podlegającym szyfrowaniu lub być szyfrowane;

4.6.1.9. Rozmieszczenie sprzętu

- zalecane jest stosowanie wymagań opisanych w 4.4.1.9;
- **wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut, wznowienie pracy wymaga podania hasła, obowiązkowe jest blokowanie lub wyłączenie komputera przez Użytkownika przy każdorazowym opuszczeniu stanowiska**;

- należy umieszczać stację przenośną w taki sposób, aby uniemożliwić podgląd ekranu przez osoby nieuprawnione;
- zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione;
- stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe);

4.6.1.10. Kopie bezpieczeństwa

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.1.10;

4.6.1.11. Zasilanie awaryjne

- stan baterii stacji przenośnej musi umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego;

4.6.2. WYMAGANIA DODATKOWE

4.6.2.1. BIOS/UEFI

- zalecane jest stosowanie ustawień opisanych w rozdziale 4.4.2.1, przy czym długość hasła BIOS/UEFI musi być nie krótsza niż 10 znaków;

4.6.2.2. Konta użytkowników i hasła

- zalecane jest stosowanie ustawień opisanych w rozdziale 4.4.2.2;

4.6.2.3. Ochrona przed atakami zewnętrznymi (zapora ogniowa)

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.2.3;

4.6.2.4. Sieci Wi-Fi

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.2.4, przy czym do połączenia z sieciami Wi-Fi zaleca się używać co najmniej standardu WPA2 i haseł o długości nie mniejszej niż 14 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny);
- **zabronione jest korzystanie z otwartych lub publicznych sieci Wi-Fi, które nie są siecią wewnętrzną Użytkownika**;

4.6.2.5. Ochrona antywirusowa

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.2.5;

4.6.2.6. Aktualizacja systemu i oprogramowania

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.2.6;

4.6.2.7. Usuwanie danych

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.2.7;

4.6.2.8. Dyski i urządzenia przenośne

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.2.8;

- dane składowane na dysku stacji przenośnej muszą być umieszczone w obszarze podlegającym szyfrowaniu lub być szyfrowane;
- zaleca się, aby partycja lub dysk stacji przenośnej, na której są przetwarzane dane był w całości zaszyfrowany przy wykorzystaniu sprzętowego modułu szyfrowania lub programowo, przy użyciu algorytmu AES256;

4.6.2.9. Rozmieszczenie sprzętu

- zalecane jest stosowanie wymagań opisanych w 4.4.2.9;
- należy umieszczać stację przenośną w taki sposób, aby uniemożliwić podgląd ekranu przez osoby nieuprawnione;
- zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione;
- stacje przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe);

4.6.2.10. Kopie bezpieczeństwa

- wymagane jest stosowanie ustawień opisanych w rozdziale 4.4.2.10.

5. Incydenty bezpieczeństwa

Przypadki naruszenia bezpieczeństwa SI CEPiK 2.0 należy zgłaszać niezwłocznie, w formie zawiadomienia pisemnego (niezależnie od własnych polityk i procedur), do Ministerstwa Cyfryzacji:

Ministerstwo Cyfryzacji
Departament Utrzymania i Rozwoju Systemów
e-mail: sekretariat.duirs@mc.gov.pl
ul. Królewska 27
00-060 Warszawa
adres strony: www.mc.gov.pl

oraz pocztą elektroniczną do administratora systemu CEPiK 2.0 na adres e-mail: adm.cepik@mc.gov.pl

W przypadku naruszenia bezpieczeństwa danych odpowiedzialność za te dane ponosi Użytkownik systemu, który był zalogowany do systemu w czasie, gdy dane te zostały pobrane z SI CEPiK 2.0. Za dalsze przetwarzanie danych uzyskanych w drodze teletransmisji odpowiedzialność ponosi Użytkownik systemu.