zalecenia, rekomendacje i wytyczne bezpieczeństwa

dla stacji kontroli pojazdów

wersja z dnia 15 czerwca 2016 r.

1. Wprowadzenie

Niniejszy dokument dotyczy wyłącznie Stacji Kontroli Pojazdów, które korzystają z własnych aplikacji w celu dostępu do systemu CEPiK 2.0.

2. Poziom bezpieczeństwa

System informatyczny CEPiK 2.0 jest systemem z zaimplementowanymi środkami bezpieczeństwa na poziomie wysokim[1]. Każdy Użytkownik systemu CEPiK 2.0 obowiązany jest stosować środki bezpieczeństwa na poziomie wysokim, z zastrzeżeniem Stacji Kontroli Pojazdów, dla których ze względu na brak dostępu do danych osobowych zdefiniowane zostały odrębne wymagania i zalecenia.

3. Kategorie użytkowników

Użytkownikiem systemu CEPiK 2.0 jest każdy podmiot uprawniony do dostępu do systemu i posiadający w systemie konto identyfikujące ten podmiot, oraz każda osoba uprawniona do dostępu do systemu posiadająca w systemie spersonalizowane konto. W systemie CEPiK 2.0 wyróżnia się następujące rodzaje użytkowników:

- Użytkownicy Instytucjonalni (UI),
    - Stacje Kontroli Pojazdów,
- Użytkownicy Indywidualni (UIn, operatorzy),
- Administratorzy (ASI),
- Operatorzy systemów POJAZD i KIEROWCA,
- Użytkownicy e-usług.

Użytkownicy Instytucjonalni to kategoria użytkowników obejmująca podmioty uprawnione do dostępu do danych przetwarzanych w systemie CEPiK 2.0, które do komunikacji z systemem CEPiK 2.0 wykorzystują własne systemy i aplikacje. Integracja z systemem CEPiK 2.0 jest realizowana przez integrację tych systemów i aplikacji z interfejsami API i usługami web services systemu CEPiK 2.0.

Wydzieloną podgrupą Użytkowników Instytucjonalnych są stacje kontroli pojazdów, które ze względu na swoją specyfikę działania oraz obowiązujące przepisy prawa m.in. ustawę Prawo o ruchu drogowym, nie są uprawnione do dostępu do danych osobowych. W związku z tym zalecany dla tych podmiotów poziom zabezpieczeń jest odpowiedni do specyfiki danych podlegających ochronie.

[1] Środki bezpieczeństwa na poziomie wysokim zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

4. Stacje Kontroli Pojazdów

4.1.Środki ochrony kryptograficznej

W systemie CEPiK 2.0 stosowane są środki kryptograficznej ochrony danych. Każda SKP musi posiadać odpowiedni certyfikat, aby móc skorzystać z usług systemu CEPiK 2.0. Szczegółowy sposób uzyskania certyfikatów, ich wymiany, sposób ochrony kluczy prywatnych oraz inne informacje i wymagania związane z certyfikatami są opisane w dokumentach:

- Polityka certyfikacji dla infrastruktury CEPiK;
- Polityka certyfikacji dla operatorów CEPiK.

W ramach polityki certyfikacji dla infrastruktury CEPiK wydawane są certyfikaty dla SKP służące do zestawiania połączeń VPN (certyfikaty VPN).

W ramach polityki certyfikacji dla operatorów CEPiK wydawane są certyfikaty dla stacji kontroli pojazdów służące do autoryzacji, uwierzytelniania, podpisywania komunikatów i zestawiania SSL (certyfikaty SSL).

UWAGA: Na potrzeby uruchomienia systemu CEPiK 2.0 zostaną wykorzystane certyfikaty SSL, które SKP już dziś posiadają w obecnym systemie CEPiK. Obecne certyfikaty będą odnawiane, co pozwoli SKP płynnie przejść z CEPiK do CEPiK 2.0. Nowe certyfikaty SSL dla SKP będą wydawane po upływie terminu ważności certyfikatów, które SKP mają i wykorzystają na potrzeby wdrożenia CEPiK 2.0.

4.2.Połączenie z systemem CEPiK 2.0

SKP ma możliwość połączenia się z systemem CEPiK 2.0 przez sieć publiczną Internet.

SKP łączący się z systemem CEPiK 2.0 przez siec publiczną Internet musi zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu VPN. Dopiero po zestawieniu połączenia VPN SKP ma możliwość wywołania usług systemu CEPiK 2.0. Autoryzacja i uwierzytelnienie Użytkownika w usługach systemu CEPiK 2.0 są realizowane w oparciu o posiadany przez SKP certyfikat SSL umieszczony na mikroprocesorowej karcie kryptograficznej.

System CEPiK 2.0 wspiera w SKP rozwiązania programowe Cisco VPN Client oraz Cisco AnyConnect i komunikację VPN typu Remote Access. Dla tych rozwiązań Service Desk zapewni wsparcie związane z instalacją oraz konfiguracją oprogramowania. Komunikacja VPN typu Lan-to-Lan, jeżeli wystąpi, jest realizowana przez SKP na własny koszt i odpowiedzialność – Service Desk nie będzie obsługiwał zgłoszeń dla tego typu połączeń.

4.3.Rozliczalność

System CEPiK 2.0 zapewnia pełną rozliczalność działań SKP w systemie. Każde działanie SKP podlega odnotowaniu w podsystemie logowania CEPiK 2.0. SKP jest identyfikowany w oparciu o certyfikat SSL wydany dla SKP. Dodatkowo aplikacja SKP musi przekazywać do systemu CEPiK 2.0, w przekazywanych komunikatach, dane identyfikujące diagnostę realizującego daną czynność (np. badanie techniczne). Szczegółowy sposób przekazywania danych identyfikacyjnych diagnosty jest określony w dokumentacji opisującej sposób działania usług web services systemu CEPiK 2.0 dla SKP.

4.4.Podpisywanie komunikatów

Każdy komunikat przekazywany do systemu CEPiK 2.0 przez aplikację SKP musi być opatrzony podpisem elektronicznym. Szczegółowe wymagania związane z podpisywaniem komunikatów są określone w dokumentacji opisującej sposób działania usług web services systemu CEPiK 2.0 dla SKP.

5. Zalecenia i wytyczne dla Stacji Kontroli Pojazdów

5.1.Ochrona fizyczna

Niniejszy rozdział opisuje zalecenia i wytyczne w zakresie ochrony fizycznej pomieszczeń oraz urządzeń wykorzystywanych do komunikacji z systemem CEPiK 2.0.

5.1.1. Pomieszczenia i ich lokalizacja

- Zaleca się, aby pomieszczenia, w których zlokalizowane są urządzenia teleinformatyczne, były zlokalizowane w miejscach, gdzie ryzyko ich zatopienia lub zalania jest zminimalizowane.
- Zaleca się, aby pomieszczenia były wyposażone w czujniki zadymienia.

5.1.2. Zabezpieczenie drzwi i okien

- Zaleca się, aby drzwi do pomieszczeń, w których przechowywany jest sprzęt teleinformatyczny, były zabezpieczone przed wyważeniem (podważeniem) oraz wyposażone w bezpieczny zamek.
- Zaleca się, aby otwory okienne pomieszczeń, w których przechowywany jest sprzęt teleinformatyczny, zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) były okratowane lub zabezpieczone w inny, równoważny sposób (np. folią antywłamaniową).

5.2.Zabezpieczenia urządzeń oraz nośników danych

Niniejszy rozdział opisuje zalecenia i wytyczne w zakresie zabezpieczenia nośników danych oraz urządzeń wykorzystywanych do komunikacji z systemem CEPiK 2.0, których uwzględnienie SKP powinien rozważyć w celu zapewnienia minimalnego poziomu ochrony tych urządzeń, jeżeli producenci aplikacji dla SKP nie określają własnych wymagań związanych z ochroną zasobów informatycznych, z których te aplikacje korzystają.

5.2.1. Urządzenia i oprogramowanie służące do nawiązania połączeń VPN przez sieć publiczną Internet

5.2.1.1. Zalecenia w zakresie konfiguracji urządzeń i oprogramowania

- Zaleca się wdrożyć reglamentację dostępu do sieci np. na podstawie adresów MAC.
- Zaleca się stosowanie, gdzie jest to możliwe, polityki blokowania ruchu sieciowego do i z sieci publicznej Internet w czasie, w którym jest nawiązane połączenie VPN.
- Oprogramowanie służące do zestawiania połączeń VPN (typu Remote Access tj. Cisco VPN Client lub Cisco AnyConnect) powinno być zabezpieczone w taki sposób, aby uniemożliwić dostęp do kluczy prywatnych osobom nieuprawnionym.
- Oprogramowanie służące do zestawiania połączeń VPN (typu Remote Access) powinno wymuszać blokowania dostępu do i z sieci publicznej Internet do danej stacji komputerowej w czasie, w którym jest nawiązane połączenie VPN (jest to wymuszone przez konfigurację urządzeń po stronie systemu CEPiK).

5.2.1.2. Zalecenia w zakresie bezpieczeństwa fizycznego urządzeń

- Jeżeli jest to możliwe, urządzenia sieciowe powinny być zlokalizowane w pomieszczeniu lub wentylowanej szafie (urządzenia komunikacyjne, serwerowe) z ograniczonym dostępem osób trzecich. Dostęp do tego pomieszczenia lub szafy powinien mieć wyłącznie administrator urządzenia lub osoby upoważnione.

5.2.2. Sprzęt komputerowy stacjonarny

- Zaleca się wprowadzenie w BIOS następujących ustawień:
  - wejście i zmiana ustawień BIOS wymaga podania hasła,
  - uruchomienie komputera wymaga podania hasła,
  - wyłączona możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera,
  - długość hasła BIOS wynosi nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra).
- Konta użytkowników i hasła:
  - wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora,
  - każdemu użytkownikowi komputera powinno być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora,
  - 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,
  - zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni,
  - zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.
- Ochrona przed atakami zewnętrznymi (zapora ogniowa):
  - zalecane jest zastosowanie zapory ogniowej (sprzętowe lub programowe rozwiązanie) oraz wdrożenie regulacji zapewniających jego bieżącą aktualizację.
- Sieci Wi-Fi:
  - do połączenia z sieciami Wi-Fi zaleca się 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).
- Ochrona antywirusowa:
  - zaleca się aby oprogramowanie antywirusowe instalowane na stacjach miało włączoną ochronę w czasie rzeczywistym,
  - zaleca się konfigurację oprogramowania zapewniającą bieżącą aktualizację sygnatur antywirusowych,
  - zaleca się konfigurację oprogramowania zapewniającą pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu.
- Aktualizacja Systemu i oprogramowania:

- zalecane jest stosowanie systemów operacyjnych wyłącznie w wersjach wspieranych przez ich producentów,
- zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów.

- Usuwanie danych:
  - zaleca się konfigurację „kosza" systemowego, aby nie przechowywał usuniętych plików,
  - zaleca się do usuwania danych używać dedykowanego do tego celu oprogramowania.
- 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 zaleca się usunąć dysk i przechowywać w zabezpieczonej szafie,
  - zaleca się wdrożyć regulacje (w tym ewidencję nośników) zapewniające obsługę pamięci flash, oraz dysków przenośnych, podłączanych okresowo do stacji, zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywane w bezpieczny sposób,
  - 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.
- Rozmieszczenie sprzętu:
  - stacja robocza powinna być ustawiona w miejscu ograniczającym lub uniemożliwiającym do niej dostęp osobom nieupoważnionym,
  - zalecane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut. Wznowienie pracy powinno wymagać podania hasła. Zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska,
- Kopie bezpieczeństwa:
  - zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii nie rzadziej niż raz na 7 dni,
  - składowanie kopi zapasowych powinno odbywać się w innym budynku bądź pomieszczeniach w odpowiednio zabezpieczonej szafie.
- Zasilanie awaryjne:
  - stacje robocze powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) umożliwiające automatyczne bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.

5.2.3. Środowiska wirtualne (maszyny wirtualne)

- Konta użytkowników i hasła:
  - wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora,
  - każdemu użytkownikowi komputera powinno być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora,

- 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,
- zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni,
- zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.

- Ochrona przed atakami zewnętrznymi (zapora ogniowa):
  - zalecane jest zastosowanie zapory ogniowej (sprzętowe lub programowe rozwiązanie) oraz wdrożenie regulacji zapewniających jego bieżącą aktualizację.
- Sieci Wi-Fi:
  - do połączenia z sieciami Wi-Fi zaleca się 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).
- Ochrona antywirusowa:
  - zaleca się aby oprogramowanie antywirusowe miało włączoną ochronę w czasie rzeczywistym,
  - zaleca się konfigurację oprogramowania zapewniającą bieżącą aktualizację sygnatur antywirusowych,
  - zaleca się konfigurację oprogramowania zapewniającą pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu.
- Aktualizacja Systemu i oprogramowania:
  - zalecane jest stosowanie systemów operacyjnych wyłącznie w wersjach wspieranych przez ich producentów,
  - zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów.
- Usuwanie danych:
  - zaleca się konfigurację „kosza" systemowego, aby nie przechowywał usuniętych plików,
  - zaleca się do usuwania danych używać dedykowanego do tego celu oprogramowania.
- 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 zaleca się usunąć dysk i przechowywać w zabezpieczonej szafie,
  - zaleca się wdrożyć regulacje (w tym ewidencję nośników) zapewniające obsługę pamięci flash, oraz dysków przenośnych, podłączanych okresowo do stacji, zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywane w bezpieczny sposób,

    - 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.
- Rozmieszczenie sprzętu:
    - serwer lub stacja robocza powinny być ustawione w miejscu ograniczającym lub uniemożliwiającym do nich dostęp osobom nieupoważnionym,
    - zalecane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut. Wznowienie pracy powinno wymagać podania hasła. Zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska.
- Kopie bezpieczeństwa:
    - zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii nie rzadziej niż raz na 7 dni,
    - składowanie kopi zapasowych powinno odbywać się w innym budynku bądź pomieszczeniach w odpowiednio zabezpieczonej szafie.
- Zasilanie awaryjne:
    - serwery i stacje robocze powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) umożliwiające automatyczne bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny zostać ograniczone tylko do użytkowników maszyny wirtualnej.
- Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż Administrator.
- Stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash nie jest zalecane. W przypadku konieczności stosowania rozwiązania zaleca się, aby:
    - nośnik plików maszyny wirtualnej był w całości zaszyfrowany,
    - wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami oraz prowadzić ewidencję dysków przenośnych bądź pamięci flash,
    - nośniki wynoszone powinny być wyposażone w rozwiązanie 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.

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

- Konta użytkowników i hasła:
    - wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora,
    - każdemu użytkownikowi komputera powinno być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora,
    - 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,
- zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni,
- zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.

- Ochrona przed atakami zewnętrznymi (zapora ogniowa):
  - zalecane jest zastosowanie zapory ogniowej (sprzętowe lub programowe rozwiązanie) oraz wdrożenie regulacji zapewniających jego bieżącą aktualizację.
- Sieci Wi-Fi:
  - do połączenia z sieciami Wi-Fi zaleca się 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).
- Ochrona antywirusowa:
  - zaleca się aby oprogramowanie antywirusowe instalowane na stacjach miało włączoną ochronę w czasie rzeczywistym,
  - zaleca się konfigurację oprogramowania zapewniającą bieżącą aktualizację sygnatur antywirusowych,
  - zaleca się konfigurację oprogramowania zapewniającą pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu.
- Aktualizacja Systemu i oprogramowania:
  - zalecane jest stosowanie systemów operacyjnych wyłącznie w wersjach wspieranych przez ich producentów,
  - zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów.
- Usuwanie danych:
  - zaleca się konfigurację „kosza" systemowego, aby nie przechowywał usuniętych plików,
  - zaleca się do usuwania danych używać dedykowanego do tego celu oprogramowania.
- 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 zaleca się usunąć dysk i przechowywać w zabezpieczonej szafie,
  - zaleca się wdrożyć regulacje (w tym ewidencję nośników) zapewniające obsługę pamięci flash, oraz dysków przenośnych, podłączanych okresowo do stacji, zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywane w bezpieczny sposób,
  - 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,

    - dodatkowo partycja lub dysk stacji przenośnej na której są składowane dane zaleca się w całości zaszyfrować przy wykorzystaniu sprzętowego modułu szyfrowania lub programowo, przy użyciu algorytmu AES256.
- Rozmieszczenie sprzętu:
    - stacja robocza powinna być ustawiona w miejscu ograniczającym lub uniemożliwiającym do niej dostęp osobom nieupoważnionym,
    - zalecane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut. Wznowienie pracy powinno wymagać podania hasła. Zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska.
- Kopie bezpieczeństwa:
    - zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii nie rzadziej niż raz na 7 dni,
    - składowanie kopi zapasowych powinno odbywać się w innym budynku bądź pomieszczeniach w odpowiednio zabezpieczonej szafie.
- Zasilanie awaryjne:
    - stan baterii powinien umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego,
    - stacje robocze powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) umożliwiające automatyczne bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.
- Rozmieszczenie sprzętu:
    - stacja przenośna powinna być użytkowana w sposób ograniczający lub uniemożliwiający do niej dostęp osobom nieupoważnionym,
    - stację przenośną w miejscach korzystania powinno się zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe),
    - zaleca się ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnym poziomie 5 minut, wznowienie pracy wymaga podania hasła, blokowanie stacji przy każdorazowym opuszczeniu stanowiska.