ZATWIERDZAM

ZASTĘPCA
KOMENDANTA GŁÓWNEGO POLICJI
nadinsp. Wojciech OLBRYŚ

10 GRU. 2013

4 - 5582 / 13

ZALECENIA

DOTYCZĄCE STANDARDÓW TECHNICZNYCH,

UŻYTKOWYCH ORAZ BEZPIECZEŃSTWA, STOSOWANYCH W POLICJI,

W ZAKRESIE INFORMATYKI I ŁĄCZNOŚCI

(tekst jednolity po zmianach wprowadzonych aneksem nr Lj-2102/13 z 23 kwietnia 2013 r.)

SPIS TREŚCI

Rozdział 1 Postanowienia wstępne

1.1 Cele i zakres dokumentu

Niniejszy dokument przedstawia standardy i tzw. dobre praktyki w zakresie planowania, projektowania, wdrażania, użytkowania oraz bezpieczeństwa systemów łączności i informatyki. Standardy te winny być stosowane w jednostkach organizacyjnych Policji, w celu stworzenia warunków do zapewnienia interoperacyjności, spójności, poufności i integralności oraz efektywności rozwiązań w obszarach łączności i informatyki.

W przypadku, gdy obecnie użytkowane elementy systemów łączności i informatyki nie spełniają wymagań określonych w dokumencie, zaleca się podjęcie działań zmierzających do zapewnienia zgodności. Tempo wprowadzania zmian dostosowawczych zależy od możliwości finansowych jednostki. W przypadku podjęcia decyzji o nierealizowaniu działań dostosowawczych, kierownik jednostki organizacyjnej Policji przeprowadza analizę ryzyka skutków niezapewnienia interoperacyjności, spójności, poufności i integralności oraz efektywności rozwiązania, określając i akceptując ryzyka szczątkowe.

1.2 Akty prawne obowiązujące w zakresie przedmiotowym objętym dokumentem

Wszelkie działania w zakresie objętym niniejszym dokumentem, muszą być zgodne z obowiązującymi regulacjami prawnymi, zawartymi w ustawach i aktach wykonawczych.

1.3 Terminologia przyjęta w dokumencie

1)	**4FSK** *(Four-level Frequency Shift Keying)*	czterowartościowe kluczowanie częstotliwości
2)	**AAA** (*Authentication, Authorization and Accounting*)	uwierzytelnianie, autoryzacja, rozliczalność.
3)	**Administrator**	Policjant albo pracownik Policji, któremu powierzono obowiązki w zakresie eksploatacji systemu teleinformatycznego, sieci lub ich wyodrębnionych komponentów. Administratorów wyznaczają właściwi przełożeni. Osobom wyznaczanym do pełnienia roli administratora można uzupełnić nazwę funkcji o określenie wskazujące na specyfikę wykonywanych zadań, przez te osoby lub o ograniczoną właściwość terytorialną, np. administrator urządzeń sieciowych, administrator materiałów kryptograficznych, administrator baz danych, administrator lokalny, administrator kopii zapasowych itp. W systemach teleinformatycznych, w których przetwarzane są informacje niejawne, sposób powoływania oraz zadania administratorów systemu określa dokumentacja bezpieczeństwa tworzona na podstawie

		przepisów o ochronie informacji niejawnych.
4)	**Administrator Lokalny**	Policjant albo pracownik Policji wyznaczony przez właściwego przełożonego, który odpowiada za prawidłowe funkcjonowanie, eksploatację i zabezpieczenie, użytkowanych w tej jednostce lub komórce organizacyjnej Policji, komponentów systemów łączności oraz informatyki, wymagających działań administracyjnych i eksploatacyjnych.
5)	**Akredytacja**	formalne potwierdzenie przez uprawniony podmiot spełnienia ustalonych wymagań i kryteriów jakości.
6)	**Algorytm Szyfrowania Danych**	sposób szyfrowania informacji przetwarzanych w systemach teleinformatycznych. Przykładami takich algorytmów są DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard) i inne.
7)	**APN** *(Access Point Name)*	dedykowany punkt dostępu do sieci operatora GSM, umożliwiający transmisję danych.
8)	**Atak typu DoS** (*Denial of Service*)	atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich lub części wolnych zasobów, przeprowadzany równocześnie z wielu komputerów.
9)	**Autoryzacja**	proces, w którym sprawdzane jest czy dany podmiot (o ustalonej właśnie tożsamości) ma prawo dostępu do żądanych zasobów.
10)	**BER** - *(Bit Error Ratio)*	bitowa stopa błędu
11)	**Bezpieczeństwo danych**	zbiór zagadnień z dziedziny informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów i sieci teleinformatycznych, rozpatrywany z perspektywy poufności, integralności, rozliczalności i dostępności danych.
12)	**Bezpieczeństwo TI** *(teleinformatyczne)*	wykorzystanie sprzętowych i programowych środków w celu ochrony przetwarzanych, przechowywanych oraz przekazywanych danych w Systemach TI w sposób zapewniający poufność, rozliczalność, integralność i dostępność.
13)	**BŁiI KGP**	Biuro Łączności i Informatyki Komendy Głównej Policji.
14)	**BTUU**	Bezpieczny Tryb Uwierzytelniania Użytkownika -

		centralny policyjny system autoryzacji i uwierzytelniania, specjalizowane oprogramowanie uprawniające zidentyfikowanych użytkowników do dostępu do zasobów informacyjnych Systemów BŁiI.
15)	**CDO**	Centrum Dystrybucji Oprogramowania, usługa dostępna w sieci PSTD zawierająca produkty: instrukcje, oprogramowanie, zarządzenia, formularze i informacje wykorzystywane do pracy z systemami teleinformatycznymi Policji.
16)	**CSD**	Centralny System Dostępowy - system dla potrzeb platformy lokalizacyjno-informacyjnej z Centralną Bazą Danych oraz dostępu do innych systemów oraz zasobów zewnętrznych.
17)	**CTCSS** *(Continuous Tone-Coded Squelch System)*	system wyłączania blokady szumów odbiornika ciągłym, niesłyszalnym tonem podakustycznym
18)	**CWI**	Centralny Węzeł Internetowy - wydzielony w BŁiI KGP technicznie i organizacyjnie punkt dostarczania usług internetowych dla KGP z możliwością dostarczania takich usług dla innych jednostek organizacyjnych Policji.
19)	**DMR** *(Digital Mobile Radio)*	otwarty standard cyfrowej łączności radiowej opracowany przez Europejski Instytut Norm Telekomunikacyjnych (ETSI)
20)	**Dostępność**	właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot upoważniony do pracy w systemie teleinformatycznym.
21)	**duosimpleks**	sposób pracy radiowej prowadzony przemiennie na dwóch różnych częstotliwościach, przy którym nadawanie i odbiór odbywa się na przemian
22)	**dupleks**	sposób pracy radiowej, przy którym nadawanie i odbiór prowadzone jest jednocześnie na dwóch różnych częstotliwościach
23)	**EDACS** *(Enhanced Digital Access Communication System)*	stworzony przez firmę Ericsson standard radiotelefonicznej łączności dyspozytorskiej (trankingowej)
24)	**ESD** *(Electrostatic Discharge)*	wyładowanie elektrostatyczne

25)	**FM** *(Frequency Modulation)*	modulacja częstotliwościowa
26)	**GDOI** *(Group Domain Of Interpretation)*	protokół zarządzania kluczami, odpowiedzialny za ustanawianie wspólnej polityki bezpieczeństwa (IPsec SA) pomiędzy routerami będącymi członkami tej samej "zaufanej" grupy.
27)	**GET VPN** *(Group Encrypted Transport)*	zbiór protokołów służących implementacji bezpiecznych, szyfrowanych połączeń typu tunel-less VPN.
28)	**GPS** - *(Global Positioning System)*	satelitarny system lokalizacji
29)	**Integralność**	właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.
30)	**IPsec** (*Internet Protocol Security*)	zbiór protokołów służących implementacji bezpiecznych, szyfrowanych połączeń typu punkt-punkt VPN oraz wymiany kluczy kodowych pomiędzy komputerami. Protokoły wchodzące w skład architektury IPsec służą do bezpiecznego przesyłania przez sieć pakietów IP.
31)	**kanał radiowy**	tor transmisyjny wykorzystywany do bezprzewodowego przesyłania informacji za pomocą fal elektromagnetycznych
32)	**Karta mikroSD krypto**	Karta mikroprocesorowa, umożliwiająca identyfikację i uwierzytelenienie użytkownika terminala MTN
33)	**KGP**	Komenda Główna Policji.
34)	**klasa ochrony IP** - *(Internal Protection code)*	kod IP, stopień ochrony obudowy wg normy EN 60529
35)	**KSP**	Komenda Stołeczna Policji.
36)	**KWP**	Komenda Wojewódzka Policji.
37)	**łączność radiowa**	łączność między stacjami radiowymi realizowana w oparciu o przydzielony kanał radiowy
38)	**maskowanie**	sposób przekazywania informacji jawnych drogą radiową, utrudniający osobom nieuprawnionym ich zrozumienie

39)	**MOS** (*Mean Opinion Score*)	subiektywny współczynnik jakości dźwięku używany w telefonii, zwłaszcza w telefonii VoIP. MOS podawany jest w skali od 1 do 5 (1 – zła, 5 – znakomita).
40)	**MPLS**	technologia w sieci operatorskiej OST 112 z zaimplementowanymi mechanizmami technologii Multi-Protocol Label Switching.
41)	**MTN**	Mobilny Terminal Noszony – komputer przenośny komunikujący się z systemami teleinformatycznymi dostępnymi poprzez sieć PSTD z wykorzystaniem bezprzewodowej transmisji danych.
42)	**MTP**	Mobilny Terminal Przewoźny – komputer zainstalowany w pojeździe, komunikujący się z systemami teleinformatycznymi dostępnymi poprzez sieć PSTD z wykorzystaniem bezprzewodowej transmisji danych.
43)	**NAC** (*Network Access Control*)	kontrola dostępu do sieci.
44)	**Napięcie gwarantowane**	napięcie zasilające gwarantujące parametry zgodnie z normami/zaleceniami dla sprzętu teleinformatycznego.
45)	**OST 112**	Ogólnopolska platforma komunikacyjna służąca do obsługi wywołań na numer alarmowy 112 i inne numery alarmowe oraz komunikacji pomiędzy służbami odpowiedzialnymi za ratownictwo i bezpieczeństwo publiczne.
46)	**pasmo częstotliwości**	określony zakres częstotliwości radiowych przydzielony do pracy radiowej służbom Policji
47)	**Poczta Elektroniczna**	ogólnopolski system poczty elektronicznej Policji pracującej na platformie Lotus Notes.
48)	**Polifax–A i Polifax–Z**	podsieci przeznaczone do transmisji telekopiowej jawnej.
49)	**Poufność**	właściwość określająca, że informacja nie jest ujawniania podmiotom do tego nieuprawnionym.
50)	**PPE** *(Kryptomail)*	Policyjna Poczta Elektroniczna – system poczty elektronicznej pracującej wewnątrz sieci PSTD.
51)	**PSTD** *(Policyjna Sieć Transmisji Danych)*	wirtualna sieć prywatna VPN, działająca na bazie wydzielonej sieci szkieletowej OST 112 w technologii

		IP MPLS z zaimplementowaną kryptografią, umożliwiająca łączenie sieci LAN na obszarze całego kraju w jedną sieć korporacyjną i zapewniająca użytkownikom policyjnym bezpieczny dostęp do centralnych systemów informatycznych Policji.
52)	**PSTN** *(Public Switched Telephone Network)*	publiczna komutowana sieć telefoniczna.
53)	**radiotelefon**	urządzenie elektroniczne składające się z nadajnika i odbiornika przeznaczone do transmisji dwustronnej sygnałów (w szczególności akustycznych) drogą radiową
54)	**RADIUS** *(Remote Authentication Dial In User Service)*	protokół opisany w RFC2865 dotyczący uwierzytelniania, autoryzacji oraz informacji o jego konfiguracji.
55)	**RFC** (*Request For Comments*)	dokumenty opisujące protokoły (standardy) internetowe stanowiące propozycję rozwiązań przedstawione przez projektantów i naukowców do akceptacji przez odpowiednie organizacje opiniujące i zatwierdzające standardy telekomunikacyjne (np. ANSI, ITU itp.).
56)	**Router CE** *(Customer Edge)*	router kliencki sieci operatorskiej MPLS.
57)	**Router PE** *(Provider Edge)*	router brzegowy w sieci operatorskiej MPLS.
58)	**Rozliczalność**	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
59)	**Sieć TI** *(teleinformatyczna)*	element składowy Systemu TI Policji zapewniający transport danych w sposób automatyczny.
60)	**simpleks**	sposób pracy radiowej polegający na wykorzystaniu jednej częstotliwości, przy którym nadawanie i odbiór odbywają się na przemian
61)	**SINAD**	parametr określający stosunek (sygnał + szum + zniekształcenia) / (szum + zniekształcenia)
62)	**SSR**	Samodzielne Stanowisko Robocze – stanowisko komputerowe niebędące Stanowiskiem Dostępowym.
63)	**stacja retransmisyjna**	zespół urządzeń nadawczo-odbiorczych, umożliwiający dwustronną retransmisję korespondencji radiowej z automatycznym

		wykorzystaniem osobnych częstotliwości radiowych, pozwalający na zwiększanie zasięgów łączności radiowej lub zwiększanie pojemności sieci radiowych wykorzystujących kanały dwuczęstotliwościowe
64)	**Stanowisko Dostępowe**	stanowisko komputerowe, podłączone do sieci TI w celu dostępu do centralnych zasobów informatycznych Systemów TI BŁiI.
65)	**SUŁTelP**	System Utajnionej Łączności Telekopiowej Policji funkcjonujący w oparciu o podsieć komutowaną przeznaczony do szyfrowanej transmisji telekopiowej.
66)	**SWWN**	System Wykrywania Włamań i Napadów.
67)	**system konwencjonalny**	podstawowy system łączności radiowej stosowany w Policji wykorzystujący kanały częstotliwościowe o szerokości 12,5 kHz z pasma 148 - 174 MHz oraz modulację sygnału F3E
68)	**System TI** *(teleinformatyczny)*	w myśl ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144 poz. 1204, z późn. zm.) jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 16 września 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).
69)	**system trankingowy**	system łączności radiowej typu dyspozytorskiego, zbudowany w oparciu o sieć stacji bazowych, wykorzystujący konfigurowalne grupy rozmówne, charakteryzujący się dynamicznym dostępem do kanałów częstotliwościowych
70)	**TACACS** (*Terminal Access Controller Access Control System*)	protokół opisany w RFC1492. Jest to protokół uwierzytelnienia, autoryzacji i rozliczenia [AAA - Autentication, Authorization and Accounting], który realizuje kontrolę dostępu dla routerów, przełączników, punktów dostępowych, czy sieciowych serwerów dostępu.
71)	**TDM** (*Time Division Multiplexing*)	multipleksowanie sygnału z podziałem czasu transmisji.

72)	**TDMA** *(Time Division Multiple Access)*	technika pozwalająca na wielodostęp do medium transmisyjnego z podziałem czasu
73)	**TETRA** *(Terrestrial Trunked Radio)*	otwarty standard cyfrowej radiotelefonicznej łączności dyspozytorskiej (trankingowej) stworzony przez Europejski Instytut Norm Telekomunikacyjnych (ETSI)
74)	**TI**	teleinformatyczny
75)	**Urządzenie wielofunkcyjne**	urządzenie z funkcjami skanowania, kopiowania, faksowania oraz drukowania, wyposażone w kartę sieciową, wysyłające i odbierające dane za pośrednictwem sieci telekomunikacyjnej
76)	**Uwierzytelnianie**	proces polegający na weryfikacji zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych.
77)	**VHF** *(Very High Frequency)*	częstotliwość z zakresu 30-300 MHz, Policja użytkuje częstotliwości z zakresu 148 -174 MHz
78)	**VLAN** *(Virtual Local Area Network)*	Wirtualna Sieć Lokalna – lokalna sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.
79)	**VLSM** (*Variable Length Subnet Mask*)	maski podsieci o zmiennej długości umożliwiają podział adresu (np.: klasy A, B, C) na kilka mniejszych podsieci zawierających różne liczby hostów.
80)	**VPN** *(Virtual Private Network)*	Wirtualna Sieć Prywatna – odseparowana sieć, w ramach której zapewniona jest komunikacja między grupą lokalizacji lub urządzeń. Granice VPN określone są poprzez politykę bezpieczeństwa i administracyjną, ustaloną przez użytkownika VPN.
81)	**Zalecenia (rekomendacje) ITU-T**	zalecenia (rekomendacje) dla sektora rynku telekomunikacyjnego wydawane przez Sektor Normalizacji Telekomunikacji Międzynarodowego Związku Telekomunikacyjnego.
82)	**Zasilanie bezprzerwowe**	zasilanie pozwalające osiągnąć parametry napięcia gwarantowanego bez względu na zaniki zasilania podstawowego.
83)	**Zasilanie podstawowe**	zasilanie z publicznej sieci elektroenergetycznej.
84)	**Zasilanie rezerwowe**	zasilanie z baterii akumulatorów i/lub zespołu

		spalinowo-elektrycznego.
85)	**Zasób systemu TI**	informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy, które mają wpływ na bezpieczeństwo tych informacji
86)	**ZSODE**	Zintegrowany System Obiegu Dokumentów Elektronicznych umożliwiający tworzenie obiegu dokumentów elektronicznych oraz przesyłanie korespondencji elektronicznej wewnątrz PSTD oraz poza tę podsieć.

Rozdział 2 Ogólne standardy łączności i informatyki policyjnej

Prowadzenie przedsięwzięć teleinformatycznych w Policji regulują odrębne przepisy. Za generalną zasadę przyjmuje się uzgadnianie wszelkich inicjowanych projektów z zakresu TI, z Biurem Łączności i Informatyki KGP, celem zapewnienia kompletności przyjętych rozwiązań i kompatybilności z funkcjonującymi rozwiązaniami.

W Systemach TI niezbędnym wymogiem jest zapewnienie właściwej ochrony i bezpieczeństwa informacji w nich przetwarzanych poprzez spełnienie następujących wymagań:

1) Jednostki organizacyjne Policji powinny ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i stale doskonalić udokumentowany System Zarządzania Bezpieczeństwem Informacji (SZBI) w kontekście prowadzonej działalności i występującego ryzyka. W celu realizacji powyższego zaleca się wykorzystanie Polskich Norm, w tym normy ISO serii 27001.
2) SZBI obejmować musi normy, zasady i wszystkie przedsięwzięcia realizowane przez użytkowników systemów TI, zmierzające do utrzymania odpowiedniego poziomu bezpieczeństwa informacji, zapewniającego ich poufność, dostępność i integralność. Założenia SZBI muszą być zatwierdzone przez kierownika jednostki organizacyjnej Policji.
3) Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej, podlegają procesowi akredytacji w Departamencie Bezpieczeństwa Teleinformatycznego ABW. Komendant Główny Policji udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.
4) Zbiory danych osobowych muszą być przetwarzane w systemach informatycznych, zgodnie z obowiązującymi w tym zakresie regulacjami prawnymi, tj. dla systemów informatycznych musi być opracowana polityka bezpieczeństwa oraz instrukcja zarządzania systemem, a także winni być wyznaczeni administratorzy ponoszący odpowiedzialność za eksploatację tego systemu.

2.1 Normy i międzynarodowe standardy

Jednolite kryteria oceny bezpieczeństwa Systemów TI zapewnia stosowanie międzynarodowych standardów. Do najważniejszych dokumentów o znaczeniu międzynarodowym należą[1]:

2.1.1 w zakresie technologii informatycznych:

1) **ISO/IEC 15408** Common Criteria for Information Technology Security Evaluation (Common Criteria - CC) - Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych:
   Część 1 - Wprowadzenie i model ogólny,
   Część 3 - Wymagania uzasadnienia zaufania do zabezpieczeń.
   Obie części 1 i 3 jeszcze w wersji 2.1 zostały wydane przez Polski Komitet Normalizacyjny jako Polskie Normy 15408:2002 (część 1 - Wprowadzenie i model ogólny).
2) **ISO/IEC 15408-1** – Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych:
   Część 1 - Wprowadzenie i model ogólny – Norma definiuje podstawowe pojęcia, zasady oceny systemów informatycznych oraz ogólny model przeprowadzania takiej oceny.
   Część 2 - Wymagania bezpieczeństwa funkcjonalnego – Norma definiuje katalog komponentów funkcjonalnych pogrupowanych w grupy i klasy, za pomocą których można tworzyć szablony wymagań bezpieczeństwa dla środków teleinformatycznych.
   Część 3 - Wymagania uzasadnienia zaufania do zabezpieczeń – Norma definiuje wymagania w celu osiągnięcia wskazanych poziomów zaufania, przedstawiono w niej kryteria oceny profilu zabezpieczeń i zadania zabezpieczeń, jak również wprowadzono poziomy zaufania (*EAL – Evaluation Assurance Levels*).
3) **dyrektywa Parlamentu Europejskiego i Rady** z dnia 15 grudnia 2004 r. w sprawie zbliżenia ustawodawstwa Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej oraz uchylająca dyrektywę 89/336/EWG *(Dz. Urz. UE L 390 z 31.12.2004 r., str. 24).*
4) **dyrektywa Parlamentu Europejskiego i Rady nr 1999/5/WE** z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności (Dz. Urz. UE, Polskie wydanie specjalne: rozdział 13, tom 23, str. 254 - 272).
5) **komunikat Komisji** w sprawie wdrożenia dyrektywy 1999/5/WE Parlamentu Europejskiego i Rady z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności (Dz. Urz. UE C 303 z 15.12.2009 r., str. 35) [komunikat zawiera wykaz norm zharmonizowanych z dyrektywą nr 1999/5/WE].

[1] W dokumencie przywołano normy i standardy oraz ich wersje, dostępne w dniu wprowadzenia niniejszych wytycznych w życie. W dłuższej perspektywie czasowej należy uwzględniać aktualne wersje norm i standardów oraz pojawiające się nowe normy i standardy, w obszarach objętych wytycznymi.

6) **rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 106/2008** z dnia 15 stycznia 2008 r. w sprawie wspólnotowego programu znakowania efektywności energetycznej urządzeń biurowych (*Dz. Urz. UE L 39 z 13.2.2008, str. 1—7).*

2.1.2 w zakresie technologii telekomunikacyjnych przepisy międzynarodowe wyszczególnione w Prawie telekomunikacyjnym, a w szczególności:

1) Rekomendacje Sektora Standaryzacji Międzynarodowej Unii Telekomunikacyjnej (ITU-T).
2) Standardy/normy Europejskiego Instytutu Standardów Telekomunikacyjnych (ETSI), w tym:
   - **PN-ETSI EN 300 247 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącze dzierżawione o przepływności 2.048 kbit/s pracujące w trybie nieramkowym (D2048U) - Parametry połączenia;
   - **PN-ETSI EN 300 452 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Analogowe czteroprzewodowe łącze dzierżawione specjalnej jakości, wykorzystujące pasmo mowy (A2S) - Parametry połączenia i prezentacja interfejsu sieciowego;
   - **PN-ETSI EN 300 289 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącza dzierżawione o przepływności 64 kbit/s bez ograniczeń z integralnością oktetową (D64U) - Parametry połączenia;
   - **PN-ETSI EN 300 418 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącza dzierżawione o przepływności 2.048 kbit/s pracujące w trybie nieramkowym i ramkowym (D2048U i D2048S) - Prezentacja interfejsu sieciowego;
   - **PN-ETSI EN 300 419 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącze dzierżawione o przepływności 2.048 kbit/s pracujące w trybie ramkowym (D2048S) - Parametry połączenia;
   - **PN-ETSI EN 300 448 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Analogowe dwuprzewodowe łącze dzierżawione zwykłej jakości, wykorzystujące pasmo mowy (A2O) - Parametry połączenia i prezentacja interfejsu sieciowego;
   - **PN-ETSI EN 300 449 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Analogowe dwuprzewodowe łącze dzierżawione specjalnej jakości, wykorzystujące pasmo mowy (A2S) - Parametry połączenia i prezentacja interfejsu sieciowego;
   - **PN-ETSI EN 300 451 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Analogowe czteroprzewodowe łącze dzierżawione zwykłej jakości, wykorzystujące pasmo mowy (A4O) - Parametry połączenia i prezentacja interfejsu sieciowego;
   - **PN-ETSI EN 300 288 V1.2.1:2002U** Dostęp i urządzenia końcowe (AT) - Cyfrowe łącze dzierżawione o przepływności 64 kbit/s bez ograniczeń z integralnością oktetową (D64U) - Prezentacja interfejsu sieciowego.

2.2 Polskie Normy

Normalizację krajową w zgodności z zasadami normalizacji europejskiej i międzynarodowej prowadzi się między innymi na podstawie przepisów ustawy z dnia 12 września 2002 r. o normalizacji (*Dz.U. Nr 169, poz. 1386, z późn. zm.*).

2.2.1 Do najważniejszych polskich wersji standardów ISO/IEC, z zakresu bezpieczeństwa, należą ustanowione normy:

1) **PN-I-02000:2002** - Technika informatyczna - zabezpieczenia w systemach informatycznych - Terminologia.
2) **PN-ISO/IEC 2382-8:2001** - Technika informatyczna - Terminologia - Bezpieczeństwo.
3) **PN-I-13335-1:1999** - Technika informatyczna - wytyczne do zarządzania bezpieczeństwem systemów informatycznych - pojęcia i modele systemów informatycznych.
4) **PN-ISO/IEC 17799:2007** - Technika informatyczna - Praktyczne zasady zarządzania bezpieczeństwem informacji.
5) **PN-ISO/IEC 15408-1:2002** - Technika informatyczna - Techniki zabezpieczeń - Kryteria oceny zabezpieczeń informatycznych - Część 1: Wprowadzenie i model ogólny.
6) **PN-ISO/IEC 15408-3:2002** - Technika informatyczna - Techniki zabezpieczeń - Kryteria oceny zabezpieczeń informatycznych - Część 3: Wymagania uzasadnienia zaufania do zabezpieczeń.
7) **PN-EN 60950-23:2007/AC:2009** - Urządzenia techniki informatycznej - Bezpieczeństwo użytkowania - Część 23:Wielkogabarytowe urządzenia do magazynowania danych.
8) **PN-EN-1047-2:2009** - Pomieszczenia i urządzenia do przechowywania wartości-Klasyfikacja i metody badań odporności ogniowej - Część 2: Pomieszczenia oraz pojemniki do przechowywania nośników informacji.
9) **PN-EN 60950-22:2007/A11:2009** - Urządzenia techniki informatycznej - Bezpieczeństwo użytkowania - Część 22: Urządzenia instalowane na zewnątrz.
10) **PN-EN 60950:2002** - Bezpieczeństwo urządzeń techniki informatycznej.
11) **PN-EN 60950-1:2004** - Urządzenia techniki informatycznej. Bezpieczeństwo. Część 1: Wymagania podstawowe.
12) **PN-ISO/IEC 27001:2007** - Technika informatyczna-Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji-Wymagania.
13) **PN**-ISO/IEC 27005:2010 - Technika informatyczna-Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

2.2.2 Do najważniejszych dokumentów standaryzacyjnych z zakresu telekomunikacji należy zaliczyć następujące normy:

1) **PN-T-05112:1996** – Systemy sygnalizacji komutacyjnej międzycentralowej w telekomunikacyjnej sieci krajowej użytku publicznego.
2) **PN-T-83101:1996** – Urządzenia zasilające w telekomunikacji – określenia, wymagania i badania.
3) **PN-T-83102:1996** – Urządzenia zasilające w telekomunikacji – siłownie telekomunikacyjne prądu stałego. Wymagania i badania.
4) **PN-T-83103:1996** – Urządzenia zasilające w telekomunikacji – zespoły prostownikowe. Wymagania i badania.

5) **PN-T-83104:1996** – Urządzenia zasilające w telekomunikacji – przetwornice półprzewodnikowe. Wymagania i badania.
6) **PN-EN 55022:2006** – Kompatybilność elektromagnetyczna (EMC) – Urządzenia informatyczne, Charakterystyki zaburzeń radioelektrycznych, poziomy dopuszczalne i metody pomiaru, Kompatybilność elektromagnetyczna (EMC), Urządzenia informatyczne, Charakterystyki zaburzeń radioelektrycznych, Poziomy dopuszczalne i metody pomiaru.
7) **PN-S-76020:1997** - Pojazdy drogowe - Urządzenia elektroniczne pojazdów samochodowych - Ogólne wymagania i metody badań.
8) **PN-ETS 300 683:2000** - Systemy i urządzenia radiowe (RES) - Kompatybilność elektromagnetyczna (EMC) urządzeń małego zasięgu (SRD) pracujących na częstotliwościach pomiędzy 9 kHz i 25 GHz.
9) **PN-ETSI EN 301 489-1 V1.8.1:2008** - Kompatybilność elektromagnetyczna i zagadnienia widma radiowego (ERM) - Norma kompatybilności elektromagnetycznej (EMC) dotycząca urządzeń i systemów radiowych - Część 1: Ogólne wymagania techniczne.
10) **PN-ETSI EN 301 489-5 V1.3.1:2003** - Kompatybilność elektromagnetyczna i zagadnienia widma radiowego (ERM) - Norma kompatybilności elektromagnetycznej (EMC) dotycząca urządzeń i systemów radiowych - Część 5: Wymagania szczegółowe dla urządzeń lądowej radiokomunikacji ruchomej typu dyspozytorskiego (PMR) i wyposażenia pomocniczego (do transmisji sygnałów mowy i innych).

Rozdział 3 Wymagania dotyczące bezpieczeństwa

Wymagania bezpieczeństwa stanowią zbiór zasad, celów i regulacji opracowanych dla zapewnienia skutecznej oraz bezpiecznej realizacji zadań z wykorzystaniem Systemów TI.

3.1 Zalecenia w zakresie wyposażenia Centrów Przetwarzania Danych (PCPD – Podstawowego Centrum Przetwarzania Danych, ZCPD – Zapasowego Centrum Przetwarzania Danych oraz RCPD – Regionalnych Centrów Przetwarzania Danych)

a) Współczynnik niezawodności na poziomie 99,99%;
b) System monitoringu, kontroli dostępu, SWWN;
c) Zasilanie podstawowe i rezerwowe (rozwiązania w zakresie zasilania powinny umożliwiać osiągnięcie parametrów napięcia gwarantowanego bez względu na jakiekolwiek problemy z zasilaniem podstawowym – tzw. zasilanie bezprzerwowe);
d) System PPOŻ – zgodnie z obowiązującymi przepisami i normami;
e) System klimatyzacji precyzyjnej;
f) Instalacje teletechniczne (okablowanie strukturalne) kable światłowodowe (FO - fiber optic) i miedziane min. kat. 6;
g) Zaleca się stosowanie rozwiązań, ograniczających zjawisko tzw. ulotu elektromagnetycznego (emisji ujawniającej).

3.2 Elementy bezpieczeństwa sieci teleinformatycznej

3.2.1 Podstawowym zadaniem systemu bezpieczeństwa jest uniemożliwienie nieuprawnionego dostępu do systemów TI. W jego rozwiązaniu muszą zostać zaimplementowane:

a) środki i metody zabezpieczeń, które muszą zapewnić utrzymanie głównych atrybutów bezpieczeństwa informacji tj.: poufność, integralność, dostępność oraz dodatkowych, takich jak: rozliczalność, autentyczność, niezawodność.
b) mechanizmy kontroli dostępu do systemów teleinformatycznych Policji, muszą zapewnić, że z tych systemów będą mogły korzystać w ramach autoryzowanych uprawnień jedynie osoby zidentyfikowane i pozytywnie uwierzytelnione. Zastosowane mechanizmy i środki kontroli dostępu (np.: AAA, NAC itp.) do systemów TI muszą być adekwatne do indywidualnej specyfiki i zawartości informacyjnej systemu (systemy jawne, systemy w których przetwarzane są dane osobowe, systemy niejawne).
c) wszystkie centralne systemy teleinformatyczne dołączone do sieci PSTD muszą korzystać z systemu BTUU jako podstawowego mechanizmu kontroli dostępu użytkowników. W uzasadnionych przypadkach Dyrektor BŁiI KGP może wyrazić zgodę na odstępstwo od tej zasady. W przypadku systemów funkcjonujących lokalnie, a dołączonych do sieci PSTD, w KWP/KSP oraz komórkach organizacyjnych KGP, dopuszcza się inne mechanizmy kontroli dostępu, np. autoryzacja użytkowników z wykorzystaniem loginu i hasła.
d) co najmniej dwa podstawowe typy systemów zaporowych: działające w warstwie aplikacji oraz w warstwie sieciowej modelu ISO OSI RM np.: „proxy" i filtry pakietów.

3.2.2 Cele systemu bezpieczeństwa:

a) zapewnienie identyfikacji - weryfikacja użytkownika,
b) zapewnienie integralności danych,
c) możliwość aktywnej i pasywnej inspekcji transmitowanych pakietów, urządzeń oraz usług systemowych (FTP, HTTP, itp.) zarówno z poziomu BŁiI KGP jak i Administratora Lokalnego,
d) zarządzanie regułami bezpieczeństwa – możliwość definiowania globalnych reguł obowiązujących w całej sieci.

3.2.3 Proces zabezpieczania sieci przez administratora sieci musi obejmować działania polegające na cyklicznym wykonywaniu czynności:

a) krok pierwszy: Zdefiniowanie silnych reguł bezpieczeństwa w sieci na podstawie szczegółowej mapy sieci,
b) krok drugi: Zabezpieczenie sieci przy użyciu produktów takich jak: firewalle, systemy AAA, systemy szyfrujące dla sieci LAN przetwarzających informacje niejawne itp.,
e) krok trzeci: Nieustanne monitorowanie sieci i reagowanie na wszelkie niebezpieczeństwa zarówno z poziomu BŁiI KGP jak i Administratora Lokalnego,

c) krok czwarty: Testowanie urządzeń bezpieczeństwa sieciowego (pasywnie - przegląd konfiguracji i rodzaju urządzeń, aktywnie – sprawdzanie reakcji sieci na ataki symulowane),
d) krok piąty: Analiza pracy systemu bezpieczeństwa, śledzenie wykrytych luk w stosowanych produktach oraz wprowadzanie niezbędnych udoskonaleń i łat.

3.2.4 Zachowanie poufności danych przesyłanych w sieci – protokół IPsec, GDOI, SSL/TLS, SSH, GET VPN, SNMP v3 (auth, prix), najnowsze wersje.

3.2.5 Wykorzystanie certyfikowanego systemu szyfrowania dla zachowania poufności, integralności i autentyczności informacji niejawnych.

3.2.6 Udostępnianie zasobów poprzez podsieć PSTD dla odbiorców zewnętrznych powinno następować w jednym punkcie, którego ochronę stanowi system typu firewall.

3.2.7 Firewall, o którym mowa w punkcie poprzednim, występuje jako punkt ochrony, zadaniem którego jest chronić urządzenia i systemy w PSTD przed atakami pochodzącymi z sieci zewnętrznej oraz przed nieuprawnioną transmisją danych pochodzącą z wewnątrz sieci.

3.2.8 System Firewall musi zapewniać:

a) dynamiczną filtrację pakietów,
b) najwyższe aktualnie dostępne współczynniki wydajności,
c) filtrację danych w warstwie aplikacji (np. SMTP, FTP, Oracle SQL, itp.),
d) wydajną translację adresów (NAT, PAT),
e) chronić przed atakiem fragmentacji pakietów IP,
f) współpracę z serwerami autentykacji, filtrowania adresów URL itp.,
g) możliwość blokowania apletów Javy oraz ActiveX,
h) gromadzenie informacji o dokonanych połączeniach,
i) implementację transmisji z użyciem standardu IPsec lub SSL,
j) terminowanie tuneli VPN.

3.2.9 Architektura systemu firewall musi być redundantna i implementowana w oparciu o wielopoziomowe (co najmniej trójpoziomowe) systemy zabezpieczeń, w których muszą być szeregowo połączone urządzenia różnych producentów.

3.2.10 W celu uwierzytelniania i autoryzacji zdalnych użytkowników w sieci zaleca się, tam gdzie jest to możliwe, stosowanie standardowego protokołu HTTPS.

3.2.11 W celu monitorowania zagrożeń i zdarzeń w ruchu sieciowym, należy stosować systemy wykrywania i ochrony przed włamaniami typu IPS (Intrusion Prevention System)/IDS (Intrusion Detection System), które muszą zapewnić w czasie rzeczywistym:

a) bezzwłoczne wykrywanie błędów w wynikach przetwarzania strumienia danych,
b) wykrywanie incydentów i anomalii w ruchu sieciowym,
c) natychmiastowego identyfikowania naruszeń bezpieczeństwa i incydentów,
d) poufność uzyskanych informacji.

3.2.12 Metody zabezpieczenia infrastruktury sieci:

a) zabezpieczenie fizycznego dostępu do urządzeń sieciowych – polityka bezpieczeństwa musi jasno określać, kto, kiedy, w jakim celu i na jakich zasadach ma prawo dostępu do pomieszczeń serwerowni, punktów dystrybucyjnych,
b) zabezpieczenie dostępu administracyjnego do urządzeń obejmuje:
   - Stosowanie bezpiecznych alternatyw dla standardowych protokołów komunikacji administracyjnej: SSH, SSL, OTP (One Time Password), SNMP,
   - Stosowanie dedykowanych portów do zarządzania urządzeniami, typu out-of-band, z wykorzystaniem dedykowanej infrastruktury połączeń do realizacji administracji urządzeniami,
   - W przypadku niedostępności w urządzeniach portów typu out-of-band, należy stosować:
     - listy dostępu, definiowane na zarządzanych urządzeniach, wskazujące dokładny adres stacji zarządzania jako jedynej, z której możliwy jest dostęp administracyjny
     - oraz wydzielone VLAN`y do zarządzania urządzeniami, niezależne od pozostałych VLAN-ów. Zaleca się uwierzytelnianie sesji administracyjnej poprzez zewnętrzny serwer Tacacs+/Radius, który dodatkowo może współpracować z serwerem obsługującym hasła jednokrotne (one-time-passwords).

3.3 Środki ochrony kryptograficznej

PSTD jest wirtualną siecią prywatną VPN, działającą na bazie wydzielonej sieci szkieletowej IP MPLS OST 112, w której przetwarzane są głównie informacje jawne niebędące jednak informacją publiczną oraz podlegające przepisom ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.). W ramach istniejącej sieci policyjnej wydzielono i zabezpieczono kryptograficznie pojedyncze podsieci z systemami służącymi do przetwarzania informacji niejawnych, urządzeniami certyfikowanymi przez ABW.

3.3.1 Zalecanym standardem w zapewnieniu poufności i bezpieczeństwa przesyłanych danych pomiędzy sieciami WAN jest technologia GET VPN. Ponadto:

a) wykorzystuje się certyfikowane rozwiązania sprzętowe dla przesyłania informacji niejawnych - szyfratory kryptograficzne z Certyfikatem Ochrony Kryptograficznej wydanym przez jednostkę certyfikującą Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego. Certyfikat taki stwierdza, że szyfratory spełniają wymagania dla urządzeń przetwarzających i przesyłających informacje o klauzuli "poufne".
   Certyfikowane szyfratory muszą być stosowane dla tych podsieci, w których przetwarzane są informacje niejawne, a na użytkowanie takich podsieci wymagana jest akredytacja Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.
b) wykorzystuje się protokół GET VPN na wszystkich routerach CE (Customer Edge) sieci MPLS OST 112 lub SSL dla przesyłania informacji jawnych.

3.3.2 Jako standard dla zarządzania certyfikatami kluczy publicznych przyjmuje się infrastrukturę PKI (Public Key Infrastructure).

Infrastruktura klucza publicznego musi być oparta na standardzie ITU-X.509 oraz zaimplementowana zgodnie z normą PN-I-02000:2002, a centrum autoryzacji musi wykorzystywać funkcję haszującą min. SHA-2 o rozmiarze skrótu co najmniej 224 bitów.

3.3.3 Aplikacje korzystające z infrastruktury PKI, muszą wykorzystywać przy transmisji danych:

a) szyfrowanie danych dla zapewnienia ich poufności,
b) podpisy cyfrowe dla zapewnienia niezaprzeczalności i weryfikacji integralności danych,
c) certyfikaty dla uwierzytelnienia osób, aplikacji, urządzeń i serwisów oraz dla zapewnienia kontroli dostępu (uwierzytelnienia).

3.4 Mechanizmy ochrony korespondencji głosowej

3.4.1 Łączność konwencjonalna

W wybranych konwencjonalnych sieciach radiowych użytkowane są moduły maskujące korespondencję głosową, stanowiące wyposażenie opcjonalne radiotelefonów analogowych. Eksploatacja lub wycofanie z eksploatacji modułów maskujących TRANSCRYPT i DAXON leży w gestii właściwej KWP/KSP lub KGP.

Zastosowanie modułów maskujących innych typów niż obecnie eksploatowane wymaga zgody Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji.

3.4.2 Łączność trankingowa (cyfrowa)

a) TETRA
W użytkowanych lokalnych systemach TETRA opartych o infrastrukturę produkcji Motorola stosowane jest maskowanie korespondencji SCK TEA 1.

b) DMR
Przy rozbudowie istniejących sieci DMR należy zapewniać zachowanie kompatybilności w zakresie dotychczas stosowanego algorytmu maskowania korespondencji.
W zakresie uruchamiania nowych sieci radiowych DMR wybór algorytmu maskowania korespondencji należy uzgadniać z BŁiI KGP.

3.4.3 Telefonia IP

Wymagania techniczno-użytkowe w systemach łączności IP:

a) CallProcesor – system sterujący połączeniami telefonicznymi;
b) Brama głosowa – styk sieci VoIP z innymi systemami (np. PSTN, telefonia stacjonarna, inna sieć VoIP lub inna sieć TI);
c) Gatekeeper – urządzenie sterujące połączeniami telefonicznymi, zapewniające m. innymi call admission controll, translację adresów itp.
d) Urządzenia końcowe – aparaty telefoniczne, aparaty video, aplikacje

e) Sieć IP – transport dla pakietów rozmównych,

f) Protokoły sygnalizacyjne:
   - H.323
   - MGCP,
   - SIP,
   - SCCP

g) Protokoły transmisji danych:
   - RTP (Real-Time Transport Protocol),
   - RTCP (Real-Time Transport Control Protocol)
   - cRTP, Compresses IP/UDP/RTP,
   - SRTP.

h) Kodeki i pasmo:
   - G.711 (bandwidth 64 kb/s, sample size 240, packets 33),
   - G.729 ((bandwidth 8kb/s, sample size 40, packets 25),

i) W zakresie sieci lokalnej – kodek VOIP G.722.

3.5 Organizacja dostępu do Internetu

3.5.1 Zaleca się, aby dostęp do sieci INTERNET w jednostkach organizacyjnych Policji, realizowany był z wykorzystaniem separowanych IP VPN w sieci OST 112, za pośrednictwem CWI KGP/CSD sieci OST 112.

3.5.2 Jeżeli dostęp do sieci Internet nie jest realizowany w sposób opisany w pkt. 3.5.1, to lokalny węzeł dostępu do sieci INTERNET, zwany dalej węzłem dostępowym, musi składać się z: routera brzegowego, wielofunkcyjnej zapory sieciowej klasy UTM (Unified Threat Management), serwera pocztowego (Lotus Notes), serwera DNS, serwera WWW lub specjalizowanych urządzeń zawierających wszystkie te funkcjonalności. Taki węzeł dostępowy powinien również zostać wyposażony w rozwiązania wykrywające ataki i zapobiegające włamaniom typu IDS/IPS, a także blokujące aktywność typu botnet oraz ataki typu DoS i DDoS. Poniżej zamieszczono krótką charakterystykę urządzeń wchodzących w skład węzła dostępowego:

a) router brzegowy – konfiguracja sprzętowa i programowa powinna pozwalać na wstępną kontrolę i odrzucanie ruchu niepożądanego (funkcja screening router),
b) wielofunkcyjna zapora sieciowa klasy UTM (Unified Threat Management) powinna zapewniać co najmniej:
   - mechanizmy zabezpieczeń: kontrole poprawności transmisji na poziomie wszystkich warstw modelu OSI, z funkcjami blokowania ataków typu DoS (Denial of Service/DDoS (Distributed Denial of Service), ochrony przed kodem złośliwym oraz wykrywania włamań do sieci.
   - filtrowanie treści: (JAVA/ActiveX), URL,

- funkcję NAT,
- współpracę z systemami uwierzytelniania typu RADIUS/TACACS+, RSA SecurID,
- możliwość współpracy z systemami antywirusowymi dla protokołów http, ftp, smtp, pop3,
- współpracę z systemami ochrony przed włamaniami typu IPS/IDS,
- tworzenie sieci VPN (tunele IPsec VPN z szyfrowaniem 3DES lub AES-256 lub SSL VPN).

c) serwer pocztowy – postfix (stabilna wersja, wspierana przez producenta) lub inne stabilne serwery. Serwer pocztowy może być włączony do ZSODE,
d) serwer DNS – BIND (stabilna wersja, wspierana przez producenta),
e) serwer WWW – np. Apache HTTP Serwer (najnowsza, stabilna wersja).

3.5.3 Zaleca się, aby węzeł dostępowy znakował wiadomości typu SPAM i posiadał oprogramowanie antywirusowe skanujące ruch przychodzący i wychodzący przynajmniej dla wiadomości pocztowych.

3.5.4 W newralgicznych punktach węzła dostępowego zaleca się stosowanie sond typu IPS.

3.5.5 Węzeł dostępowy powinien umożliwiać identyfikację urządzeń podłączonych do sieci LAN poprzez system adresów prywatnych protokołu IP oraz identyfikację użytkowników.

3.5.6 Podstawowe usługi udostępniane przez węzeł dostępowy, to: poczta elektroniczna, www, ftp (pod warunkiem zabezpieczenia tej usługi oraz wykorzystania klienta ftp wyłącznie w trybie pobierania), połączenia VPN, itp.

3.5.7 System operacyjny dla serwerów w węzłach dostępowych to: system operacyjny z rodziny Windows Server – minimum Windows 2008 R2 Server, SUN SOLARIS, FreeBSD oraz inne systemy OPEN SOURCE, w najnowszych, stabilnych wersjach bądź wspieranych przez producenta.

3.5.8 Zalecane oprogramowanie użytkowe (stabilne wersje, wspierane przez producentów) stanowisk komputerowych:

a) przeglądarka internetowa: Internet Explorer, Firefox,
b) klienci poczty: Thunderbird, Outlook Express, Microsoft Outlook, Lotus Notes, Poczta Systemu Windows (Windows Vista),
c) bezpieczni klienci FTP, z obsługą połączeń SSL: FileZilla lub inny posiadający wsparcie dla połączeń szyfrowanych,
d) oprogramowanie antywirusowe z możliwością centralnego zarządzania,
e) centralnie zarządzane oprogramowanie typu „Firewall", przy czym konfiguracja takiego oprogramowania musi umożliwiać administratorom systemu, wykonanie diagnostyki połączeń sieciowych (ping) i aktualizowanie oprogramowania antywirusowego.

3.5.9 Zabrania się w szczególności:

a) podłączania stanowisk komputerowych jednocześnie do dwóch sieci, np. z sieci PSTD do sieci Internet i odwrotnie lub jednocześnie do obu sieci,

b) wyłączania zainstalowanego oprogramowania antywirusowego oraz poszczególnych jego usług (komponentów), zatrzymywania systemowych zadań tj. aktualizacji oprogramowania antywirusowego oraz skanowania systemu w poszukiwaniu wirusów,
c) instalowania oprogramowania nasłuchującego i skanującego sieć (tzw. sniffery i analizatory sieci), bez zgody Dyrektora Biura Łączności i Informatyki KGP bądź Naczelnika wydziału właściwego ds. łączności/informatyki,
d) podłączania stanowisk komputerowych bez zgody administratora sieci,
e) używania oprogramowania służącego do omijania zabezpieczeń CWI bądź węzłów dostępowych, tj. rozwiązań zapobiegających analizie ruchu sieciowego czy umożliwiających anonimizację użytkowników, np. TOR (The Onion Router), proxy itp.
f) podłączania urządzeń sieciowych typu router, przełącznik, modem oraz tworzenia podsieci, nie autoryzowanych przez administratorów CWI bądź administratorów węzłów dostępowych.

3.5.10 Przenośne SSR, które wykorzystują niechroniony dostęp do sieci INTERNET, muszą być wyposażone w oprogramowanie zapewniające kontrolę polityki bezpieczeństwa SSR, zintegrowane z centralnym systemem bezpieczeństwa. Oprogramowanie to powinno posiadać budowę modułową z funkcjonalnością zapory Firewall, skanera antywirusowego, szyfratora dysków twardych, klienta IPsec VPN lub SSL VPN oraz NAC (Network Access Control).

3.5.11 Należy zapewnić okresową aktualizację tzw. krytycznych poprawek systemu operacyjnego (nie rzadziej niż raz w miesiącu) oraz skanowanie antywirusowe stanowisk komputerowych i serwerów (zgodnie z przyjętymi politykami).

3.6 Zasilanie elektroenergetyczne

3.6.1 Bezpieczeństwo zasilania

Przez bezpieczeństwo zasilania należy rozumieć zapewnienie najwyższych wymagań niezawodnościowych systemu zasilania, polegających na eliminowaniu przerw w dostawie energii elektrycznej oraz zakłóceń pochodzących z sieci zasilającej.

3.6.1.1 Urządzenia zapewniające obsługę aplikacji centralnych, dostęp do tych aplikacji oraz sprzęt łączności zapewniający mobilność dla służb dyżurnych Policji muszą być objęte zasilaniem:

- bezprzerwowym na poziomie KGP, komend wojewódzkich (Stołecznej), miejskich, powiatowych Policji, komisariatów Policji o stanie etatowym powyżej 60 etatów oraz szkół policji,
- podstawowym na poziomie pozostałych komisariatów Policji,
- zaleca się by, fizyczne okablowanie budynków Policji zapewniało wydzieloną, dedykowaną sieć elektroenergetyczną dla sieci LAN,
- bezprzerwowe zasilanie i napięcie gwarantowane powinno być dostępne w Centralnych Punktach Dystrybucyjnych.

3.6.1.2 Zasilaniem bezprzerwowym na poziomie KGP, komend wojewódzkich (Stołecznej), miejskich, powiatowych, rejonowych, komisariatów Policji o stanie etatowym powyżej 60 etatów, oraz szkół policji obejmuje się urządzenia wchodzące w skład:

- węzłów teleinformatycznych (WWT, PWT, WT),
- centralnych oraz lokalnych punktów dystrybucyjnych,
- sieci energetycznej dedykowanej dla sieci LAN (okablowania strukturalnego),
- systemów telewizji przemysłowej CCTV,
- kontroli dostępu,
- systemów rozgłoszeniowych.

3.6.1.3 Zasilaniem rezerwowym na poziomie komend wojewódzkich (Stołecznej), miejskich, powiatowych, rejonowych, komisariatów Policji o stanie etatowym powyżej 60 etatów, oraz szkół policji obejmuje się urządzenia wchodzące w skład:

- systemów klimatyzacyjnych w węzłach teleinformatycznych.

3.6.1.4 Zasilanie podstawowe stosuje się do zasilania urządzeń teleinformatycznych w pozostałych komisariatach Policji i komórkach niższego szczebla. W celu ochrony instalowanych urządzeń przed zanikami napięcia zasilającego, zaleca się stosowanie zasilaczy UPS lub siłowni telekomunikacyjnych małej mocy.

3.6.2 Zasilanie węzłów TI

Przy projektowaniu podstawowych wymagań siłowni telekomunikacyjnych zaleca się odpowiednie stosowanie postanowień zawartych w rozporządzeniu Ministra Łączności z dnia 21 kwietnia 1995 r. w sprawie warunków technicznych zasilania energią elektryczną obiektów budowlanych łączności (Dz. U. Nr 50, poz. 271).

Przy projektowaniu siłowni telekomunikacyjnych należy dążyć do rezerwowania prostowników i inwertorów zgodnie z zasadą redundancji n + 1.

3.6.2.1 Podstawowe wymagania w zakresie zasilania energią elektryczną węzłów TI:

a) konstrukcja modułowa siłowni telekomunikacyjnych,
b) zdalne monitorowanie oraz możliwość zdalnej zmiany parametrów poprzez sieć Ethernet wykorzystując protokół TCP/IP z możliwością kontroli pracy systemów zasilania zainstalowanych w podległych jednostkach,
c) stacjonarny agregat prądotwórczy w jednostkach Policji szczebla KGP, komendy wojewódzkiej Policji i komendy miejskiej Policji oraz szkoły Policji, posiadający funkcję automatycznego uruchamiania się,
d) zapas paliwa dla stacjonarnego agregatu prądotwórczego musi zapewnić ciągłość jego pracy przez okres, co najmniej 72 godzin,
e) zalecane baterie bezobsługowe, o żywotności zgodnie z normą EUROBAT 12,
f) czas rezerwy bateryjnej na szczeblu KGP, komendy wojewódzkiej (Stołecznej) Policji i komendy miejskiej Policji oraz szkoły Policji musi wynosić min. 3 godziny przy znamionowym obciążeniu siłowni. W przypadku zastosowania agregatu prądotwórczego, czas ten może być krótszy, jednak musi wystarczyć do wystartowania i zsynchronizowania agregatu,
g) Do zasilania urządzeń w węzłach TI na szczeblu komendy powiatowej Policji, komendy rejonowej Policji, komisariatów Policji o stanie etatowym powyżej 60 etatów, stosuje się:

- centralne zasilacze UPS o min. 15 minutowej autonomii pracy, przy obciążeniu znamionowym,
- ogólno-budynkowe samo startujące spalinowe agregaty prądotwórcze z zapasem paliwa na min. 24 godziny pracy przy obciążeniu znamionowym,
- siłownie telekomunikacyjne.

3.6.2.2 Zasilacze UPS

Do zasilania urządzeń teleinformatycznych w pozostałych jednostkach organizacyjnych podległych komendom miejskim, powiatowym i rejonowym należy stosować:

a) siłownie inwertorowe lub zasilacze UPS typu kompakt (tzn. zintegrowane z szafą teleinformatyczną) o min. 15 minutowej autonomii pracy przy obciążeniu znamionowym,
b) zasilacze UPS w zakresie mocy 1-120kVA należy projektować zgodnie z zasadą redundancji n+1, stosując konstrukcję modułową, z zachowaniem możliwości rozbudowy o kolejne moduły. W zakresie mocy 100-500kVA stosować należy konstrukcję monoblokową z możliwością pracy równoległej szaf,
c) zasilacze UPS w technologii VFI - SS 111, posiadające certyfikat zgodności z zasadniczymi wymaganiami wydany przez notyfikowaną jednostkę certyfikującą lub deklarację zgodności z wymaganiami szczegółowymi wydany przez producenta lub importera,
d) zasilacze UPS spełniające normy:
   - PN-EN-62040-1-1:2006 (Systemy bezprzerwowego zasilania (UPS) - Część 1-1: Wymagania ogólne i wymagania dotyczące bezpieczeństwa UPS stosowanych w miejscach dostępnych dla operatorów),
   - PN-EN 50091-2:2002 (U) (Systemy bezprzerwowego zasilania (UPS) - Część 2: Wymagania dotyczące kompatybilności elektromagnetycznej (EMC)) [norma o takim samym numerze, ale bez indeksu "U" - dotyczy ogólnych wymagań technicznych dla domowych i budynkowych systemów elektronicznych (HBES)],
   - PN-EN 62040-3:2005 (Systemy bezprzerwowego zasilania (UPS) - Część 3: Metody określania właściwości i wymagania dotyczące badań).
e) zasilacze UPS zapewniające instalację kolejnych modułów bez konieczności montażu dodatkowego okablowania na obiekcie, z możliwością komunikacji z zasilaczem UPS poprzez adapter SNMP,
f) dodatkowe wyłączniki p-poż. w pomieszczeniach całodobowej służby dyżurnej,
g) akumulatory do zasilaczy UPS:
   - zaleca się stosowanie akumulatorów w technologii VRLA:
     - o żywotności min. 10 lat (UPSy >20kVA),
     - o żywotności min. 6 lat (UPSy <20kVA),
     - spełniające wymagania określone w decyzji Rady nr 87/95/EWG z dnia 22 grudnia 1986 r. w sprawie normalizacji w dziedzinie technologii informatycznych i telekomunikacji (Dz. Urz. UE, Polskie wydanie specjalne: rozdział 13, tom 08, str. 236) oraz w dyrektywie 2006/66/WE Parlamentu Europejskiego i Rady z dnia 6 września 2006 r. w sprawie baterii i akumulatorów oraz zużytych baterii i akumulatorów oraz uchylająca dyrektywę 91/157/EWG (Dz. Urz. UE L 266 z 26.09.2006 r. , str.1).

- należy stosować baterie akumulatorów składającą się z ogniw tego samego typu (w miarę możliwości pochodzących z tej samej serii produkcyjnej),
- należy stosować minimum dwie równoległe gałęzie akumulatorów, odpowiednio zabezpieczonych na obu biegunach,

h) zaleca się wykonywanie zabezpieczeń i instalację zasilania z UPS-ów w sposób umożliwiający wymianę elementów i rozbudowę sieci elektroenergetycznej, bez konieczności rozłączania jakiegokolwiek obwodu podłączonego do tej sieci.

3.6.2.3 Siłownie telekomunikacyjne:

a) siłownie telekomunikacyjne 48V DC oraz 230V AC należy projektować zgodnie z zasadą redundancji n+1, stosując konstrukcję modułową, z zachowaniem możliwości rozbudowy o kolejne moduły,
b) należy stosować siłownie posiadające deklarację zgodności z dyrektywami Wspólnoty Europejskiej CE oraz EMC (kompatybilności elektromagnetycznej),
c) należy stosować siłownie spełniające normy: PN-T-83102, PN-T-83103, PN-T-83104,
d) w pomieszczeniach całodobowej służby dyżurnej należy instalować wyłączniki p.poż.,
e) <u>wymagania dot. siłowni telekomunikacyjnych 48V DC:</u>
   - zasilanie wejściowe trójfazowe, jednofazowe moduły prostownikowe pracują na różnych fazach (w siłowniach pow. 35kW stosować prostowniki trójfazowe),
   - równoległa praca modułów prostownikowych,
   - praca w układzie buforowym z dwoma bateriami,
   - charakterystyka wyjściowa modułów - UPI,
   - aktywny podział prądu obciążenia zespołów prostownikowych,
   - zarządzanie energią pobieraną przez zespoły prostownikowe,
   - układ pomiaru prądu zbiorczego baterii 1, baterii 2 i odbiorów,
   - układ ładowania dozorowego baterii,
   - czujnik temperatury baterii do kompensacji napięcia buforowania,
   - czujnik temperatury w pomieszczeniu technicznym,
   - pole dystrybucji DC: zabezpieczenia typu „S" i (lub) NHOO,
   - możliwość wymiany zabezpieczeń od przodu w sposób gwarantujący bezpieczeństwo,
   - programowalny rozłącznik głębokiego rozładowania baterii,
   - sprawność siłowni $\geq$ 91%,
   - możliwość rozbudowy o dodatkowe moduły zwiększające obciążalność siłowni o min 50% (przy uwzględnieniu nadmiarowości n+1).
f) <u>wymagania dot. siłowni inwertorowych 230V AC:</u>
   - znamionowe napięcie wejściowe DC 48 V,
   - znamionowe napięcie wyjściowe AC 230V,
   - równoległa praca modułów inwertorowych,
   - elektroniczny i ręczny przełącznik obejściowy,
   - pole dystrybucji AC: wyłączniki typu „S",
   - sprawność siłowni dla mocy do 10kVA $\geq$ 91%, dla mocy powyżej 10kVA – w trybie podstawowym (np. EPC) $\geq$ 95%, w trybie bateryjnym $\geq$ 91%,
   - stabilizacja napięcia wyjściowego dla trybu podstawowego < 5%,
   - przeciążalność ciągła 110%,

- możliwość rozbudowy o dodatkowe moduły zwiększające obciążalność siłowni o min. 50% (przy uwzględnieniu nadmiarowości n+1).

g) wymagania dot. sterownika mikroprocesorowego siłowni:
   - sterowanie pracą i konfigurowanie parametrów siłowni lokalne i zdalne kontrolowanie stanów alarmowych systemu zasilania,
   - zarządzanie mocą zespołów prostownikowych,
   - ograniczanie prądu ładowania baterii akumulatorów,
   - test dyspozycyjności baterii,
   - automatyczne przekazywanie informacji o parametrach i stanach alarmowych siłowni do istniejących systemów nadzoru bez dodatkowych, pośrednich modułów sterownikowych,
   - automatyczny odczyt stanu obiektu o zadanej porze,
   - komunikacja ze stanowiskiem zarządzania i administracji poprzez sieć LAN wykorzystując protokół TCP/IP w standardzie Ethernet,
   - min. 5 styków cyfrowych do monitorowania innych urządzeń w obiekcie możliwych do podłączenia przez obsługę,
   - min. 5 styków analogowych do monitorowania innych urządzeń w obiekcie możliwych do podłączenia przez obsługę,
   - pomiar temperatury baterii oraz w pomieszczeniu technicznym,
   - lokalny zapis i odczyt zdarzeń z własnej pamięci,
   - wszystkie komunikaty wyświetlane lokalnie w języku polskim.

h) wymagania dot. baterii akumulatorów:
   - napięcie znamionowe DC 48 V,
   - napięcie znamionowe pojedynczego ogniwa 2 V,
   - typ baterii: OPzV, wykonane w technologii żelowej z zaworami regulującymi ciśnienie,
   - trwałość baterii min. 15 lat,
   - praca przy napięciu buforu regulowanym w zależności od temperatury w pomieszczeniu baterii,
   - montaż na stojaku.

3.6.2.4 Agregaty prądotwórcze:

a) do zasilania urządzeń o zwiększonych jakościowo wymaganiach w zakresie dostarczania energii elektrycznej (zasilacze UPS, systemy telekomunikacyjne, sprzęt komputerowy) należy stosować agregaty samostartujące, spełniające klasę wymagań G3, zgodnie z normą PN-ISO-8528-1, posiadające deklarację producenta, że wyrób wprowadzany do obrotu spełnia wymagania zasadnicze określone w przepisach o systemie oceny zgodności CE (Conformability European - Zgodność Europejska),

b) główne parametry
   - silnik wyposażony w automatyczny, elektroniczny regulator prędkości obrotowej silnika zapewniający stabilność częstotliwości ±0.25 % w całym zakresie obciążeń,
   - prądnica synchroniczna, samowzbudna, bezszczotkowa, posiadająca automatyczny, elektroniczny regulator napięcia prądnicy, zapewniający stabilność napięcia ±0,5 % w całym zakresie obciążeń,
   - zakłócenia radioelektryczne zgodne ze standardami VDE 0875 stopień G i MIL 461 AB,

- współczynnik THD (bez obciążenia) < 2,0 %,
- stopień ochrony IP23,
- klasa izolacji stojana i wirnika: H,
- sprawność prądnicy przy 100% obciążenia należy określać dla konkretnej mocy agregatu (np. 85 kVA ≥ 91,5%, 150 kVA ≥ 92,2%, 250 kVA ≥ 92,4%, 400kVA≥ 94,1%).

c) wymagania w przypadku zabudowy kontenerowej:
- wielkość kontenera powinna być zależna od wielkości agregatu i zastosowanego wyciszenia,
- powierzchnia podłogi antypoślizgowa, odporna na rdzę: np. blacha ryflowana aluminiowa,
- oświetlenie podstawowe (230 V) i awaryjne (12 lub 24 V) wnętrza kontenera,
- wyłącznik „STOP" awaryjny przy każdych drzwiach wejściowych do kontenera,
- poziom hałasu: max. 69 dB, mierzony w odległości 7 m od agregatu.

d) dobierając moc agregatu należy uwzględnić:
- oczekiwaną moc zapotrzebowaną przez odbiorniki, które mają zostać objęte zasilaniem z agregatu,
- pokrycie potrzeb częściowo rozładowanych akumulatorów współpracującego z agregatem zasilacza UPS lub siłowni,
- zapas mocy ze względu na urządzenia klimatyzacyjne.

3.6.3 Monitoring urządzeń:

a) w pomieszczeniach całodobowej służby dyżurnej jednostek Policji należy montować wizualno-akustyczne panele sygnalizacyjne informujące o aktualnym stanie urządzeń zasilających (UPS, agregat) oraz sygnalizujące ich ewentualne awarie,
b) całodobowej służbie dyżurnej Wojewódzkiego Węzła Teleinformatycznego należy zapewnić zdalne monitorowanie systemów zasilania zainstalowanych w podległych jednostkach Policji z możliwością kontroli ich parametrów w oparciu o protokół SNMP,
c) należy stosować układy monitorujące stan akumulatorów oraz systemów zarządzających ładowaniem akumulatorów,
d) obiekty komisariatów Policji zaleca się wyposażać w przyłącze dla agregatu przewoźnego,
e) zaleca się przeprowadzanie okresowych testów potwierdzających sprawność urządzeń zasilających.

3.6.4 Zasilanie urządzeń radiotelefonicznych

3.6.4.1 Łączność konwencjonalna i trankingowa

3.6.4.1.1 Radiotelefon bazowy, stacja retransmisyjna:

a) zasilanie sieciowe 230V ±10%, 50 Hz,
b) zasilanie rezerwowe zespołu nadawczo-odbiorczego z akumulatora 12V lub 24V zapewniające czas pracy nie mniej niż 8 godzin przy proporcjach nadawanie/odbiór/nasłuch równych 10%/10%/80% i mocy nadajnika dla stacji bazowej i retransmisyjnej 25W,

c) wymagane jest także zasilanie rezerwowe dla wydzielonego manipulatora operatorskiego z akumulatora 12V zapewniającego czas pracy nie mniejszy niż 8 godzin przy proporcjach nasłuch/odbiór równych 90%/10% i mocy m.cz. 3W.

3.6.4.1.2 Radiotelefony przewoźne:

Zasilane z sieci pokładowej pojazdu – wymagane jest zasilanie prądem stałym o napięciu 13,2V (±20%) z minusem na masie pojazdu.

3.6.4.1.3 Radiotelefony noszone:

Podstawowym źródłem zasilania są akumulatory o parametrach zapewniających pracę radiotelefonu przez co najmniej 8 godzin, przy proporcjach nadawania/odbioru/stanu gotowości do pracy wynoszących odpowiednio 5%/5%/90% i mocy nadajnika 5W (2W dla radiotelefonu kamuflowanego).

Urządzenia ładujące akumulatory muszą spełniać wymienione poniżej wymagania:

- ładowarka jedno- i wielopozycyjna zasilana z sieci 230V ±10% 50 Hz ma zapewnić:
  - ładowanie akumulatorów z sygnalizacją cyklu pracy,
- ładowarka wielopozycyjna z funkcją regeneracji zasilana z sieci 230V ±10% 50 Hz ma zapewnić:
  - ładowanie akumulatorów z sygnalizacją cyklu pracy oraz funkcję wstępnego rozładowania,
  - regenerację akumulatorów,
  - określenie pojemności akumulatorów,
  - każda z ww. funkcji ma być realizowana przez wszystkie stanowiska ładowarki.

3.6.4.2 Łączność satelitarna

Telefony satelitarne muszą posiadać możliwość:

a) zasilania z sieci energetycznej 230V±10% 50 Hz,
b) zasilania prądem stałym o napięciu 13,2V (±20%) z minusem na masie pojazdu - w przypadku telefonów zasilanych z sieci pokładowej pojazdu,
c) zasilania bateryjnego przy pracy: nadawanie min. 3 godziny, a w stanie czuwania min. 50 godzin.

Rozdział 4 Wymagania dotyczące projektowania, implementacji i wdrażania

4.1 Sieci teleinformatyczne

a) Biuro Łączności i Informatyki KGP do identyfikacji urządzeń w sieci LAN Policji (sieć wewnętrzna) przyjęło systemem adresów protokołu IPv4. Ponadto z puli adresów dostępnych dla klasy A wybrano prywatną (specjalną) przestrzeń adresową zaczynająca się od 10.X.X.X.. W celu efektywnego przydziału jednostkom i komórkom Policji adresów IP dostępnych w puli prywatnej przestrzeni adresowej zaleca się tworzenie podsieci o różnych rozmiarach (VLSM) na bazie masek klasy C,
b) nowo kupowany sprzęt musi umożliwiać obsługę protokołu IPv6,

c) obowiązującym protokołem współdziałania międzysieciowego w każdej sieci LAN jest TCP/IP,
d) lokalne połączenia do sieci LAN istniejące obecnie, eksploatowane za zgodą Dyrektora Biura Łączności i Informatyki KGP, mogą być utrzymywane,
e) nowe, tworzone lokalnie, połączenia do sieci LAN pozapolicyjnych Systemów TI wymagają zgłoszenia do Dyrektora Biura Łączności i Informatyki KGP w celu uzyskania oceny i akceptacji rozwiązania systemu zabezpieczeń,
f) w sieci LAN włączonej do sieci PSTD mogą być eksploatowane urządzenia i systemy zapewniające pracę z centralnie dystrybuowanymi aplikacjami Komendy Głównej Policji oraz lokalne systemy, które otrzymały akceptację Dyrektora Biura Łączności i Informatyki KGP,
g) włączenie lokalnych systemów (nie dot. pkt. 4.1 f) do sieci PSTD może nastąpić na wniosek Naczelnika wydziału właściwego ds. łączności/informatyki, który opisuje budowę i warunki bezpieczeństwa lokalnego systemu TI, po uzyskaniu zgody Dyrektora Biura Łączności i Informatyki KGP i zatwierdzeniu przez gestora systemu,
h) podstawowym interfejsem sieciowym w sieci PSTD jest standard ETHERNET: 10/100/1000 Mb full-duplex oraz 10 Gb full-duplex z wykorzystaniem kabli miedzianych lub światłowodowych,
i) skanowania sieci zarządzanych przez służby Policji w obrębie kraju lub BŁiI KGP może dokonywać tylko osoba upoważniona przez Dyrektora Biura Łączności i Informatyki KGP. Skanowania w obrębie województwa, może dokonywać tylko osoba upoważniona przez Naczelnika wydziału właściwego ds. łączności/informatyki za zgodą Dyrektora Biura Łączności i Informatyki KGP. Każde działanie tego typu przeprowadzone przez inną osobę traktowane będzie, jako atak na zasoby skanowanej sieci. W uzasadnionych przypadkach Naczelnik wydziału właściwego ds. łączności/informatyki może upoważnić osobę bez występowania o zgodę na skanowanie sieci, jednakże po wykonaniu czynności musi o zaistniałym fakcie zostać przesłana informacja do Dyrektora BŁiI KGP.
j) realizacja połączeń sieciowych odbywa się poprzez łącza stałe lub radioliniowe,
k) połączenia typu Wi-Fi (łączność bezprzewodowa) powinna być implementowana w oparciu o międzynarodową specyfikację IEEE 802.11 wg standardu 802.11 a/b/g/n zabezpieczoną dodatkowo przez urządzenia szyfrujące wykorzystujące min. klucz WPA2/tryb Enterprise o długości co najmniej 12 znaków. Sieć Wi-Fi musi dawać gwarancję dostępności tylko i wyłącznie uprawnionym podmiotom. Rozwiązanie dopuszcza się jedynie dla sieci z dostępem do Internetu,
l) dopuszcza się możliwość korzystania z technologii bezprzewodowych, np.: Bluetooth w telefonach komórkowych i komputerach za wyjątkiem stacji włączonych do PSTD,
m) w oparciu o technologię GSM realizacja połączeń związanych z dostępem do policyjnych systemów teleinformatycznych możliwa jest pod warunkiem zastosowania szyfrowania transmisji danych oraz połączenia przez dedykowany APN z sygnałem przechodzącym przez CSD (Centralny System Dostępowy) administrowany przez BŁiI KGP.

4.2 Okablowanie strukturalne

a) okablowanie strukturalne sieci LAN jednostek Policji musi być budowane w oparciu o aktualne normy ISO/IEC 11801:2002 (wersja ostateczna), ANSI EIA/TIA 568 B.2 (wersja ostateczna), EN 50173 oraz PN-EN 70153:2004. Budowę okablowania należy opierać o kable UTP kategorii min. 6 lub wyższej oraz o kable światłowodowe,
b) nowo budowane okablowanie strukturalne należy wykonywać w standardzie kategorii min. 6 channel, poświadczone certyfikatem producenta,
c) Centralne i Lokalne Punkty Dystrybucyjne zaleca się wykonywać w pomieszczeniach technicznych, przeznaczonych na potrzeby urządzeń łączności i informatyki, w postaci szafy dystrybucyjnej z panelami krosowniczymi kat. min. 6 z gniazdami RJ-45 oraz dwoma listwami zasilającymi po minimum 8 gniazd każda, z sygnalizacją optyczną napięcia z wyłącznikiem listwy i opcjonalnym systemem wentylacji,
d) w przypadku konieczności połączenia dwóch punktów dystrybucyjnych (w dwóch budynkach) połączenie należy wykonywać kablem światłowodowym minimum 8 włóknowym zewnętrznym. Każde włókno należy zakończyć odpowiednim złączem na panelu w szafie dystrybucyjnej,
e) zaleca się, aby w przypadku zastosowania więcej niż jednego punktu dystrybucyjnego (w jednym budynku) okablowanie pionowe wykonać kablem światłowodowym minimum 8 włóknowym wewnętrznym. Każde włókno należy zakończyć złączem na panelu w szafie dystrybucyjnej,
f) zaleca się, aby system okablowania w szafie dystrybucyjnej składał się z 24 lub 48 portowych paneli, z gniazdami RJ45,
g) zaleca się stosowanie szaf dystrybucyjnych z uwzględnieniem zastosowanego systemu klimatyzacji,
h) zaleca się, aby całość oferowanej instalacji okablowania strukturalnego dla wskazanych lokalizacji miała możliwość dalszej rozbudowy w części logicznej: posiadać przekroje tras kablowych oraz wielkość szafy dystrybucyjnej dostosowane do zwiększenia struktury o 25%,
i) zaleca się, aby w Centralnych i Lokalnych Punktach Dystrybucyjnych w pomieszczeniach technicznych stosować odpowiednie urządzenia klimatyzacyjne zapewniające poprawną pracę urządzeń aktywnych sieci,
j) zaleca się, aby w trakcie budowy lub modernizacji systemów okablowań strukturalnych dokonywać integracji z istniejącą siecią telefoniczną.

4.3 Systemy operacyjne, protokoły i systemy zarządzania bazami danych

a) w serwerach przeznaczonych dla obsługi aplikacji bazodanowych stosować należy systemy operacyjne zapewniające poziom ochrony nie niższy niż EAL3 (według *Common Criteria*),
b) standardami systemów operacyjnych dla serwerów baz danych oraz serwerów aplikacji są:
   - HP-UX,
   - IBM-AIX,
   - SUN-Solaris,

- system operacyjny z rodziny Windows Server – minimum Windows 2003 Server,
- zaleca się stosowanie komercyjnych wersji systemów LINUX i UNIX, tym niemniej dopuszcza się wykorzystanie innych dystrybucji, spośród których zalecany jest Debian i FreeBSD.

c) wszystkie nowotworzone bazy danych muszą być relacyjne (jednak, gdy jest to konieczne i uzasadnione dopuszcza się, za zgodą Dyrektora Biura Łączności i Informatyki KGP, implementowanie innych baz danych), obsługujące polską stronę kodową ISO 8859-2 lub UTF-8,
d) interfejs użytkownika w aplikacjach policyjnych (wszystkie systemy) musi być w języku polskim,
e) wymianę informacji o routingu pomiędzy routerami w sieci PSTD należy opierać o protokoły dynamiczne IGP,
f) zarządzanie serwisami, systemami operacyjnymi centralnych systemów odbywa się tylko i wyłącznie z poziomu Biura Łączności i Informatyki KGP,
g) zaleca się stosowanie formatu XML jako standardu wymiany danych pomiędzy systemami w strukturze organizacyjnej Policji,
h) zaleca się, aby bezpieczeństwo logowania na serwerach z systemem UNIX obsługiwał protokół KERBEROS,
i) zgodę na wykorzystywanie innych systemów lub sprzętu niezgodnego z przyjętym standardem i ich eksploatację w sieci LAN (PSTD) każdorazowo wydaje Dyrektor Biura Łączności i Informatyki KGP,
j) do przechowywania informacji o użytkownikach i ich uprawnieniach, wykorzystywany jest protokół oparty o usługi katalogowe zgodne z otwartymi standardami (np.: LDAP, AD),
k) do identyfikacji użytkowników i zasobów stosowane są metody oparte o PKI.

4.4 Systemy teletransmisyjne

Sieć WAN to sieć szkieletowa IP MPLS obejmującej swym zasięgiem obszar całej Polski, w której zdefiniowane są routery P i PE z zaimplementowanymi mechanizmami MPLS. W dokumencie przedstawione zostały podstawowe wymagania dla urządzeń i mechanizmów zaimplementowanych na urządzeniach.

Odnośnie sieci MAN zawarte zostały wymagania dotyczące miejskich sieci teleinformatycznych MAN, obejmujące swoim zasięgiem jednostki Policji zlokalizowane na terenie miast wojewódzkich.

4.4.1 Urządzenia teletransmisyjne, routery CE (Customer Edge) umiejscowione w obiektach Komendy Głównej Policji, komend wojewódzkich Policji, Komendy Stołecznej Policji, komend miejskich Policji, komend powiatowych Policji, szkołach Policji

a) współpraca z międzycentralowymi łączami Ethernet, E&M, ISDN BRA, ISDN PRI oraz E1 (nx64kb/s),
b) obsługa protokołów sygnalizacji: SIP, H.323, ETSI oraz Q.sig,
c) obsługa faksów grupy G3, G4 z protokołem T.38,
d) parametry styków do transmisji danych:
   - styk interfejsu V.36, V.35, Ethernet, G.703/G.704,
   - routing pakietów IP,

e) możliwość tworzenia oddzielnych kanałów wirtualnych dla tworzenia podsieci na bazie infrastruktury urządzeń,
f) obsługa kanałów Frame Relay (PVC i SVC),
g) port LAN Ethernet 10 Mb/s lub 10/100 Mb/s lub 10/100/1000/10000 Mb/s,
h) obsługa standardu VLAN 802.1p oraz 802.1q na portach Ethernet,
i) styk do operatorów telekomunikacyjnych: Ethernet, E1, ułamkowy E1 na styku G.703/G.704/G.706; możliwość tworzenia na interfejsach ułamkowych E1, co najmniej trzech grup kanałów, Ethernet, V.36, V.35,
j) efektywne wykorzystanie pasma:
   - kompresja głosu, tylko w miejscach wejścia-wyjścia z sieci, bez pośrednich stopni dekompresji-kompresji,
   - możliwość kompresji połączeń głosowych do wartości poniżej 8 kb/s, przy czym musi istnieć możliwość wybierania przez użytkownika dowolnej wartości współczynnika kompresji, głos w kanałach TDM po skompresowaniu ma być przenoszony przez sieć wraz z sygnalizacją międzycentralową,
   - dynamiczny przydział pasma,
   - dynamiczna aktywacja usługi fragmentacji pakietów w sytuacji, kiedy w sieci pojawiają się pakiety głosowe (automatyczne włączanie fragmentacji pakietów równocześnie z rozpoczęciem transmisji głosu),
   - w celu zapewnienia odpowiedniej jakości skompresowanego głosu dla połączeń VoFR lub VoIP parametr MOS (Mean Opinion Score) nie może być gorszy niż 3,7 według pomiaru określonego w normie ITU-P.800,
k) możliwość automatycznego wyłączania kompresji głosu dla konkretnych numerów abonentów,
l) możliwość stworzenia systemu łączności dyspozytorskiej,
m) skalowalność,
n) akceptowanie numeracji o zmiennej liczbie cyfr; możliwość wykonywania operacji na numeracjach telefonicznych (np. dodawanie prefixów, postfixów, podmiana),
o) automatyczna rekonfiguracja sieci w stanach awaryjnych,
p) nadzór, konfigurowanie, zarządzanie, testowanie urządzeń i sieci ze stanowiska zarządzania z poziomu węzła w Komendzie Głównej Policji / komendzie wojewódzkiej Policji / Komendzie Stołecznej Policji,
q) zasilanie urządzeń sieci napięciem przemiennym 230V lub napięciem stałym 48V.

4.4.2 Urządzenia teletransmisyjne, routery CE (Customer Edge) umiejscowione w obiektach komisariatach Policji, posterunkach Policji, referatach dzielnicowych

a) współpraca z łączami Ethernet, E&M, FXO, FXS, ISDN PRI, ISDN BRI oraz E1 (nx64kb/s),
b) obsługa protokołów sygnalizacji: SIP, H.323, ETSI oraz Q.sig,
c) obsługa faksów grupy G3 i G4,
d) możliwość tworzenia oddzielnych kanałów wirtualnych dla tworzenia podsieci na bazie infrastruktury urządzeń,
e) obsługa kanałów Frame Relay (PVC i SVC),
f) port LAN Ethernet 10Mb/s lub 10/100/1000 Mb/s,
g) obsługa standardu VLAN 802.1p oraz 802.1q na portach Ethernet,
h) konfiguracja styków do transmisji danych:
   - styk interfejsu V.36, V.35, Ethernet,

- routing protokołów IP.

i) styk do operatorów telekomunikacyjnych: E1, ułamkowy E1 na styku G.703/G.704/G.706; możliwość tworzenia na interfejsach ułamkowych E1, co najmniej trzech grup kanałów, Ethernet, V.36, V.35,
j) efektywne wykorzystanie pasma:
   - kompresja głosu, tylko w miejscach wejścia-wyjścia z sieci, bez pośrednich stopni dekompresji-kompresji,
   - możliwość kompresji połączeń głosowych do wartości poniżej 8 kb/s, przy czym musi istnieć możliwość wybierania przez użytkownika dowolnej wartości współczynnika kompresji, głos w kanałach TDM po skompresowaniu ma być przenoszony przez sieć wraz z sygnalizacją międzycentralową,
   - dynamiczny przydział pasma,
   - dynamiczna aktywacja usługi fragmentacji pakietów w sytuacji, kiedy w sieci pojawiają się pakiety głosowe,
   - w celu zapewnienia odpowiedniej jakości skompresowanego głosu dla połączeń VoFR lub VoIP parametr MOS (Mean Opinion Score) nie może być gorszy niż 3,7 według pomiaru określonego w normie ITU-P.800,
k) możliwość tworzenia połączeń dyspozytorskich,
l) możliwość automatycznego wyłączania kompresji głosu dla konkretnych numerów abonentów,
m) akceptowanie numeracji o zmiennej liczbie cyfr,
n) nadzór, konfigurowanie, zarządzanie, testowanie urządzeń i sieci ze stanowiska zarządzania z poziomu węzła w komendzie wojewódzkiej (Stołecznej) Policji,
o) automatyczna rekonfiguracja sieci w stanach awaryjnych,
p) zasilanie urządzeń sieci napięciem przemiennym 230V lub napięciem stałym 48V.

4.4.3 Urządzenia teletransmisyjne, routery PE (Provider Edge) WAN/MAN

Zaleca się, aby nowobudowane sieci miejskie wykorzystywały technologię MPLS *(Multi Protocol Label Switching)* i MetroEthernet.

4.4.3.1 Wymagania dla urządzeń WAN/MAN w technologii MPLS:

a) budowa modularna,
b) możliwość przełączania w oparciu o standard MPLS i IP v4, IP v6,
c) architektura elementu przełączającego oparta o w pełni nieblokowalną matrycę przełączającą,
d) zaleca się redundancję wszystkich krytycznych elementów urządzenia: zasilacze, karty kontroli (procesorowe), matryce przełączające,
e) możliwość rozbudowy bez ponoszenia kosztów zmian w oprogramowaniu,
f) wymiana karty w urządzeniu musi odbywać się bez konieczności wyłączania całego urządzenia („wymiana na gorąco"),
g) zapewnienie wsparcia dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
   - protokół Fast Reroute,
   - protokół VRRP albo analogiczne rozwiązanie,
h) zasilanie ze źródeł prądu zmiennego 230V lub stałego 48V,
i) zapewnienie jednoczesnej obsługi protokołów:
   - Label Distribution Protocol (LDP),

- MPLS VPN L2 i L3,
- MPLS-RSVP-TE,
- Mechanizmy QoS z użyciem tzw. bitów eksperymentalnych (EXP),
- MPLS Differentiated Services (DiffServ)-Aware Traffic Engineering (MPLS-DS-TE),
- IP v6 edge over MPLS,
- EoMPLS,
- EloMPLS
- AToM
- VPLS,

j) możliwość pracy w trybie LER i LSR,
k) zapewnienie instalacji następujących typów portów:
   - Ethernet 10/100/1000 BASE-T, Gigabit Ethernet,
   - 10 GB Ethernet,
l) zapewnienie wsparcia dla transmisji video poprzez Ethernet z obsługą tzw. ramek „jumbo" o wielkości nie mniejszej niż 9 tysięcy bajtów oraz możliwość obsługi ruchu multicast z wykorzystaniem IGMP v1, v2, PIM, DVMRP,
m) możliwość przełączania w warstwie trzeciej oraz definiowania routingu w oparciu o routing statyczny lub dynamiczny dla protokołu IP v4 i v6,
n) zapewnienie wsparcia dla następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:
   - obsługa co najmniej czterech kolejek sprzętowych dla różnego rodzaju ruchu,
   - obsługa co najmniej jednej kolejki ze statusem priorytetowym (bezwzględne pierwszeństwo obsługi),
   - dynamiczna alokacja pamięci dla kolejki,
   - zapewnienie możliwości zmiany pola 802.1p (CoS) oraz IP DSCP i MPLS EXP pakietu przychodzącego do urządzenia przed jego przesłaniem na port wyjściowy (re-kolorowanie pakietów przez urządzenie),
o) zalecane zarządzanie poprzez protokoły SSH v2 i SNMP v3,
p) możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS lub TACACS+ dla kont administratorów urządzenia,
q) możliwość montażu w szafie 19".

4.4.3.2 W celu przenoszenia kanałów TDM przez sieć MPL/IPS dopuszcza się stosowanie urządzeń agregujących ruch z central telefonicznych/TDM spełniających następujące wymagania:

a) zapewnienie transmisji strumieni TDM w ramkach "Ethernet" i "MPLS" (TDM over IP, TDM over MPLS),
b) zapewnienie obsługi usług bazujących na TDM, a w szczególności synchronizację poprzez sieć Ethernet, IP, MPLS,
c) możliwość wyposażenia w moduły interfejsów Ethernet 10/100/1000 BaseT dla podłączenia do sieci IP,
d) wyposażenie w interfejs zarządzający Ethernet 10 BaseT oraz port szeregowy,
e) obsługa znakowania pakietów IP (modyfikacja pól ToS),
f) obsługa:
   - protokołów 802.1q, 802.1p,

- protokołu ICMP,
- agregacji strumieni E1,
- strumieni E1 zgodnie ze standardami ITU-T Rec. G.703, G.704,
- strumieni E1 z ramkowaniem CRC-4 MF, CAS MF i kodowaniem HDB3,
- strumieni E1 przy impedancji 120 Ω (ballanced),
- detekcji i modyfikacji alarmów wraz ze statystykami błędów,
- alarmów LOS/AIS/LOF/LCV oraz testowania remote/local loopback,
- transmisji alarmów E1 w trybie end-to-end,

g) wnoszenie opóźnień nie większych niż 2 ms,
h) zapewnienie monitorowania i nadzoru usług TDMoIP,
i) buforowanie strumieni IP/TDM,
j) synchronizacja czasu usług TDM:
   - Internal – zegarowanie z wewnętrznego generatora,
   - Loopback – zegarowanie z wybranego portu,
   - Adaptive – zegarowanie z portu Ethernet,
   - External – zegarowanie z zewnętrznego urządzenia.

4.5 Systemy Łączności Telefonicznej

4.5.1 Sieci łączności telefonicznej

Policyjna Sieć Łączności Telefonicznej (PSŁT) stanowi strukturę obejmującą wszystkie lokalne sieci łączności telefonicznej jednostek organizacyjnych Policji (Komenda Główna Policji, komenda wojewódzka (Stołeczna) Policji, komenda miejska Policji, komenda powiatowa Policji, komenda rejonowa Policji i komisariat Policji) połączone ze sobą poprzez sieć szkieletową OST 112 oraz sieci MAN, utrzymywane i zarządzane przez właściwe terytorialnie jednostki Policji.

Policyjna Sieć Łączności Telefonicznej (PSŁT) jest połączona z sieciami publicznymi PSTN oraz sieciami resortów, służb i instytucji, do których ma odniesienie art. 4 ustawy z dnia 16 września 2004 r. - Prawo telekomunikacyjne, zgodnie z odrębnymi umowami i ustaleniami. Identyfikacja urządzeń końcowych w sieci następuje zgodnie z obowiązującym planem numeracji resortowej.

Policyjna Sieć Łączności Telefonicznej (PSŁT) jest siecią pracującą synchronicznie, a źródłem synchronizacji są urządzenia sieci szkieletowej OST 112 oraz sieci publiczne lub inne źródło synchronizacji klasy zgodnej z zaleceniem ITU - T G.812.

4.5.2 Serwery telefoniczne (centrale telefoniczne, switche IP, softswitche)

W ramach województwa zaleca się budowę systemów telekomunikacyjnych telefonii IP i VoIP typu single-site lub multisite, umożliwiającą realizację wszystkich usług systemowych przy wykorzystaniu sygnalizacji systemowej.

System telekomunikacyjny powinien składać się z następujących elementów: systemu sterującego połączeniami telefonicznymi, bramy głosowej realizującej punkt styku z innymi systemami PSTN, urządzeń zapewniających między innymi call admission controll, translację adresów, urządzeń końcowych. Brama głosowa systemu musi być wyposażona w wystarczającą ilość interfejsów głosowych i dostosowana do potrzeb w danym węźle łączności, stosownie do szczebla organizacyjnego i zadań jednostki Policji

a) wymagania dotyczące łączy i sygnalizacji:

- cyfrowe łącza pierwotno grupowe ISDN PRI (sygn. CCS, CAS) w warstwie fizycznej zgodnie z zaleceniami ITU-T I.431,
- analogowe łącza FXO, E&M, cyfrowe łącza abonenckie EuroISDN (styk So i U; sygn. EDSS1),
- cyfrowe łącza abonenckie do podłączenia cyfrowych aparatów systemowych,
- analogowe łącza abonenckie FXS do współpracy ze standardowymi aparatami telefonicznymi z wybieraniem dekadowym i DTMF oraz sygnalizacją FSK,
- cyfrowe łącza wykorzystujące port Ethernet 10/100/1000 Mb/s, obsługujące protokoły sygnalizacyjne: H.323, MGCP, SIP, SCCP.

Wykorzystywane protokoły sygnalizacji muszą odpowiadać Polskiej Normie PN-T-05112 oraz spełniać specyficzne wymagania dla sygnalizacji w sieci policyjnej. Protokoły muszą zapewnić pełny dostęp do wszystkich istniejących zasobów oraz zachować jednakową funkcjonalność dostępną we wszystkich serwerach połączonych w sieć.

b) Dopuszcza się czasowe stosowanie następujących rodzajów łączy:
   - łącza cyfrowe PCM 2 Mb/s (sygn. R2 DLB i DLM),
   - analogowe łącza miejskie typu abonenckiego końcowe a/b,
   - analogowe łącza międzycentralowe jedno- i dwukierunkowe do współpracy z centralami publicznymi (sygnalizacja jak dla central publicznych),
   - łącza MB,
   - analogowe łącza dwukierunkowe jedno- i dwutorowe E&M (sygnalizacja liniowa prądem stałym, R2 i impulsowa) o napięciu międzyżyłowym na żyłach sygnalizacyjnych RON TRON min. 20V.
c) wymagania dla łączy cyfrowych ISDN 30B+D:
   - parametry elektryczne zgodne z zaleceniami ITU-T G.703, impedancja falowa 120 Ω, przepływność 2 Mb/s,
   - parametry jakościowe zgodne z zaleceniami ITU-T M.2100, M.2101 oraz G.821, G.826,
   - dopuszczalne fluktuacje fazy i przepływności zgodne z zaleceniami ITU-T G.823 i G.921,
   - struktura ramki zgodna z G.704 (bity E wykorzystane do kontroli parzystości CRC4) i G.705,
   - wartość maksymalna bitowej stopy błędów BER wynosi 10-6.
d) protokół (sygnalizacja) w sieci policyjnej oraz współpraca z innymi sieciami niepublicznymi:
   - Q.sig zgodnie z zaleceniami ITU Q.931 BC/GF,
   - IETF Session Initiation Protocol (SIP),
   - ITU H.323.
e) protokół (sygnalizacja) do współpracy z sieciami publicznymi:
   - EuroISDN DSS-1 zgodnie ETS 300 102-1.
f) kodowanie głosu:
   - kodek audio: G.711 A-law, G.729A, G.723.1, G.718, G.719, G.722, G.722.1, G.722.2, G.726, G. 728, G. 279.

4.5.3 Wytyczne dotyczące wyposażenia i konfiguracji serwerów telefonicznych, realizujących sterowanie połączeniami telefonicznymi:

a) wyposażenie podstawowe:

- stanowisko administratora,
- stanowisko pośredniczące (awizo, call center) wraz z elektroniczną książką telefoniczną,
- pulpity dyspozytorskie,
- aparaty IP, umożliwiające połączenia telefoniczne i video,
- możliwość użycia lokalnych aplikacji, typu poczta głosowa, itp.,
- system rejestracji i taryfikacji połączeń, rejestrujący cały ruch telefoniczny i przechowujący dane przez okres co najmniej 24 miesięcy, posiadający możliwość zdalnego dostępu do danych taryfikacyjnych, zbierania informacji o wszystkich połączeniach, również w sieci resortowej, generowania zestawień statystycznych, rachunków zbiorczych oraz umożliwiający pełną archiwizację danych na standardowych nośnikach,
- system zapowiedzi słownych.

b) podstawowe wymagania techniczno-użytkowe serwera telefonicznego:
   - zgodność z zasadniczymi bądź szczegółowymi wymaganiami lub specyfikacjami technicznymi,
   - zgodność ze szczególnymi wymaganiami bezpieczeństwa dotyczącymi urządzeń przeznaczonych do podłączenia do sieci telekomunikacyjnych w europejskiej normie zharmonizowanej EN 41003:1998 (lub w PN-EN 41003:2001),
   - architektura wspierająca otwarte standardy współpracy z systemami innych producentów oraz zapewniająca elastyczność konfiguracji interfejsów i sieciowanie w oparciu o pakietową sieć IP,
   - możliwość tworzenia podsystemów dyspozytorskich,
   - możliwość zestawiania, co najmniej 3 jednoczesnych telekonferencji do min. 8 abonentów w grupie,
   - możliwość rozbudowy o zintegrowany sprzętowo i/lub funkcjonalnie system telefonii bezprzewodowej DECT lub DECT IP,
   - system poczty głosowej,
   - możliwość zdalnego wykonania podstawowych zmian konfiguracyjnych oraz nadzoru,
   - skalowalność rozwiązań umożliwiająca prostą rozbudowę systemu,
   - zasilanie napięciem stałym 48V lub ~230V).

c) podstawowe wymagania techniczno-użytkowe serwera przetwarzania połączeń:
   - architektura wspierająca otwarte standardy współpracy z systemami innych producentów (IETF H.323, SIP, MGCP) oraz zapewniająca elastyczność konfiguracji interfejsów i sieciowanie w oparciu o sieć IP,
   - przesyłanie pakietów głosowych w sieci LAN musi być realizowane przy zastosowaniu mechanizmów jakości usług QoS oraz mechanizmów separacji podsieci (np. VLAN L2, L3, VPLS – bez konieczności budowy oddzielnego okablowania sieci LAN), natomiast przenoszenie telefonii IP poprzez sieć WAN musi być realizowane przy użyciu sieci pakietowej IP,
   - dedykowane rozwiązanie sprzętowe i programowe posiadające możliwość rozbudowy pojemności oraz zwiększenia jego niezawodności poprzez zastosowanie klastra serwerów przetwarzających połączenia telefoniczne,

- co najmniej dwa interfejsy Ethernet w celu realizacji redundantnego podłączenia do sieci LAN,
- skalowalność systemu umożliwiająca prostą rozbudowę,
- serwer musi realizować następujące funkcje telefoniczne,
  - identyfikację numeru dla połączeń przychodzących,
  - przenoszenie wywołań warunkowe oraz bezwarunkowe,
  - parkowanie połączeń (możliwość „zawieszenia" połączenia przychodzącego, a następnie odebranie tego samego połączenia z innego aparatu w systemie),
  - obsługę połączeń oczekujących – możliwość obsługi przez abonenta kilku połączeń jednocześnie (jedno aktywne, pozostałe zawieszone),
  - obsługę klawiszy szybkiego wybierania,
  - transferowanie połączeń,
  - funkcję zamawiania połączeń,
  - zestawianie telekonferencji,
  - automatyczny wybór standardu kompresji głosu dla obsługiwanych połączeń,
  - automatyczne zestawianie najtańszej drogi połączenia wychodzącego,
  - automatyczne uaktualnianie oprogramowania telefonów IP z serwera przetwarzania połączeń,
  - obsługa zestawów sekretarsko – dyrektorskich.
- możliwość współpracy z bramami głosowymi do sieci PSTN,
- możliwość centralnego wykonania zmian konfiguracyjnych oraz nadzoru przez przeglądarkę internetową,
- książka telefoniczna dostępna z aparatów IP,
- możliwość generowania raportów na temat wszystkich zrealizowanych połączeń,
- integracja z dodatkowymi aplikacjami za pomocą interfejsów programowych CTI,
- funkcja kontroli pasma dla połączeń głosowych,
- możliwość rozbudowy o dodatkowe funkcjonalności typu: zapowiedzi słowne, poczta głosowa, systemy pracy grupowej, call center itp..

d) podstawowe wymagania techniczno-użytkowe bramy głosowej:

- wspieranie technologii GET-VPN,
- wspieranie funkcjonalności realizacji translacji sygnalizacji IP-to-IP,
- możliwość wyposażenia w interfejsy ISDN PRA (30B+D), ISDN BRA (2B+D) i analogowe z możliwością prostej rozbudowy o kolejne interfejsy (analogowe bądź cyfrowe) jedynie poprzez włożenie dodatkowych wyposażeń,
- posiadanie odpowiedniej ilość licencji umożliwiającą jednoczesną obsługę wszystkich wyspecyfikowanych połączeń głosowych,
- współpraca z serwerem zestawiającym połączenia głosowe z wykorzystaniem standardów kodowania: G.711, G.729A lub G.723.1 (automatyczny wybór standardu kompresji głosu) oraz wideo z wykorzystaniem standardów kodowania H.261/263/264,
- możliwość pełnienia funkcji zapasowego serwera przetwarzania połączeń (na wypadek awarii lub braku łączności z serwerami sterującymi) i zapewnienie realizacji podstawowych funkcji systemu telefonicznego,

- możliwość konfiguracji, jako mostek konferencyjny lub transkoder pomiędzy dwoma strumieniami z różnymi standardami kompresji głosu,
- możliwość transmisji faksów poprzez sieć IP z wykorzystaniem protokołu T.38.

4.5.4 Przełączniki LAN

Wszystkie instalowane przełączniki Ethernet w sieci LAN powinny umożliwiać przesyłanie energii elektrycznej z pomocą skrętki UTP do urządzeń końcowych będących elementami sieci Ethernet, zgodnie z obowiązującymi wersjami standardu PoE (Power over Ethernet):

	802.3af	**802.3at**
– maksymalna moc:	15,40 W	34,20 W
– zakres napięcia:	44 – 57 V	50 – 57 V
– maksymalny prąd:	350 mA	600 mA
– maksymalna rezystancja okablowania UTP:	20 Ω	12,5 Ω

Każdy przełącznik musi zawierać układ zabezpieczający przed dostarczaniem napięcia do urządzenia końcowego, które nie spełnia wymogów standardu PoE.

4.5.5 Urządzenia końcowe (terminale)

Zaleca się stosowanie następujących urządzeń końcowych (terminali) w Policyjnej Sieci Łączności Telefonicznej:

- aparaty cyfrowe systemowe z prezentacją numeru wywołującego,
- aparaty cyfrowe ISDN z prezentacją numeru wywołującego,
- aparaty cyfrowe ISDN z prezentacją numeru wywołującego oraz sekretarką automatyczną,
- aparaty analogowe z prezentacją numeru wywołującego oraz daty i godziny połączenia w sygnalizacji FSK lub DTMF,
- aparaty analogowe z prezentacją numeru wywołującego oraz daty i godziny połączenia w sygnalizacji FSK lub DTMF, z wbudowaną sekretarką automatyczną,
- urządzenia telekopiowe (faksowe),
- urządzenia wielofunkcyjne,
- aparaty DECT z prezentacją numeru wywołującego,
- aparaty DECT z prezentacją numeru wywołującego oraz sekretarką automatyczną,
- modemy analogowe,
- modemy ISDN,
- abonenckie centrale telefoniczne ISDN,
- abonenckie analogowe centrale telefoniczne,
- aparaty telefoniczne IP z możliwością zasilania PoE lub za pomocą adaptera sieci zasilającej ~230V oraz rozbudowy/zwiększenia ilości przycisków poprzez zastosowanie przystawek rozszerzających,
- wideotelefony ISDN i IP,
- zestawy wideokonferencyjne ISDN i IP.

Dopuszcza się użytkowanie aparatów telefonicznych cyfrowych oraz analogowych bez identyfikacji numerów, w przypadku braku możliwości zastosowania innych rozwiązań.

4.5.6 System Polifax

a) standard sprzętowy:
   - sieć Polifax–A i Polifax–Z abonenckie urządzenia telekopiowe o wydruku laserowym z prędkością transmisji ITU-T Super G3 z korekcją ECM lub ISDN G4,
   - sieć rozsiewcza Polifax–Z zbudowana na bazie sprzętu tego samego producenta, posiadającego parametry umożliwiające adresowanie i zabezpieczanie dostępu poprzez zestaw haseł,
   - sieć SUŁTelP - wykorzystuje szyfratory transmisji telekopiowej (faksowej) Omnisec 520.

b) standard transmisyjny:
   - sieć Polifax-A – sieć otwarta, co oznacza, że każdy abonent może dokonywać indywidualnych połączeń telekopiowych z dowolnym abonentem sieci Polifax-A lub z dowolną stacją telekopiową pracującą w sieci operatora publicznego,
   - sieć Polifax-Z – sieć zamknięta, co oznacza, że dokonywanie połączeń telekopiowych jest możliwe wyłącznie w ramach zamkniętej grupy abonentów telekopiowych.

4.6 Systemy radiokomunikacyjne

4.6.1 Łączność radiotelefoniczna konwencjonalna

W celu zapewnienia kompatybilności w funkcjonowaniu systemów łączności radiotelefonicznej, zdefiniowano podstawowe parametry, które muszą spełniać radiotelefony i stacje retransmisyjne.

Montaż radiotelefonów w pojazdach Policji, musi być zgodny z przepisami Regulaminu EKG ONZ nr 21, ogłoszonego przez Ministra Infrastruktury w Dz. Urz. MI Nr 6, poz. 27 z dnia 18 kwietnia 2002 r.

4.6.1.1 Podstawowe parametry dotyczące wszystkich typów radiotelefonów i stacji retransmisyjnych:

a) **parametry techniczne ogólne**
   - modulacja F3E (11K0F3E),
   - szerokość pasma pracy od 148 do 174 MHz; od 164 do 174 MHz dla stacji retransmisyjnych i radiotelefonów noszonych kamuflowanych,
   - dopuszczalna odchyłka od częstotliwości środkowej kanału ± 0,5 kHz,
   - odstęp międzykanałowy: 12,5 kHz.

b) **parametry techniczne nadajnika (dla odstępu 12,5 kHz)**
   - moc wyjściowa nadajnika w.cz. programowana w trybie serwisowym, w całym zakresie częstotliwości,
   - stabilność mocy nadajnika ± 1,5 dB wartości znamionowej w wymaganym paśmie pracy,
   - maksymalna dopuszczalna dewiacja częstotliwości ± 2,5 kHz,
   - dewiacja sygnału CTCSS (250 ± 50 Hz),
   - charakterystyka pasma akustycznego (+1,-3 dB) przy nachyleniu (preemfaza) 6 dB/okt. 300 ÷ 2550 Hz,

- łączne zniekształcenia modulacji mniejsze od 5% (1 kHz, dewiacja 60% wartości maksymalnej),
- całkowity przydźwięk i szumy własne ≤ -40dB,
- moc w kanale sąsiednim nie przekraczająca wartości mniejszej od maksymalnej mocy wyjściowej o 60 dB,
- moc dowolnej składowej emisji niepożądanej nie przekraczająca wartości 0,25 μW w zakresie od 9 kHz do 1 GHz przy maksymalnej mocy wyjściowej.

c) **parametry techniczne odbiornika (dla odstępu 12,5 kHz)**
- czułość odbiornika lepsza niż 0,5 μV przy SINAD równym 20 dB i 0,35 μV przy SINAD równym 12 dB,
- selektywność sąsiedniokanałowa nie mniejsza niż 60 dB,
- selektywność wspólnokanałowa pomiędzy –12 dB i 0 dB,
- selektywność w stosunku do sygnałów o częstotliwościach niepożądanych nie mniejsza niż 70 dB,
- odporność na zakłócenia powodowane przez zjawisko blokowania ≥ 84 dB,
- histereza blokady szumów ≤ 4,5 dB,
- charakterystyka pasma akustycznego (+1÷-3dB) przy nachyleniu (deemfaza) 6 dB/okt. w zakresie 300 ÷ 2550 Hz,
- współczynnik zawartości harmonicznych ≤ 5% (1 kHz, dewiacja 60% wartości maksymalnej i mocy maksymalnej akustycznej wymaganej dla danego typu radiotelefonu).

d) **ogólne cechy użytkowe**
- praca w trybie: simpleks, duosimpleks; dupleks – dotyczy tylko stacji retransmisyjnych,
- programowanie wyświetlanej nazwy kanału (min. 12 znaków alfanumerycznych) – nie dotyczy stacji retransmisyjnych, dopuszcza się min. 6 znaków dla radiotelefonów noszonych kamuflowanych,
- praca z dużą lub małą mocą (ustawiana programowo dla danego kanału),
- programowe ograniczanie czasu nadawania (dla wszystkich kanałów),
- w przypadku stosowania selektywnego wywołania w danej sieci radiowej wyposażenie radiotelefonu w selektywne wywołanie 5-tonowe zgodnie z CCIR 100 ms, CCIR 70 ms, EEA 40 ms i możliwością ustawiania cyfry „0" jako pierwszej cyfry selektywnego wywołania (nie dotyczy radiotelefonów noszonych kamuflowanych), wskazana (nieobligatoryjna) możliwość obsługi co najmniej dwóch sekwencji tonów, rodzaj systemu selektywnego wywołania wybierany programowo na dowolnym kanale,
- regulacja poziomu blokady szumów (tylko w trybie serwisowym, możliwość ustawienia progu na poziomie 0,5 μV dla radiotelefonów bazowych i stacji retransmisyjnych oraz 0,35 μV dla radiotelefonów przewoźnych, noszonych i noszonych kamuflowanych),
- kodowa blokada szumów CTCSS,
- jednoczesna praca z kodową blokadą szumów i selektywnym wywołaniem (nie dotyczy radiotelefonów noszonych kamuflowanych),
- ustawiana programowo możliwość włączenia/wyłączenia kodowej blokady szumów przez użytkownika.

e) **środowisko i klimatyczne warunki pracy**
   - zakres temperatury pracy od -30°C do +60°C (dla manipulatora stacji bazowej od 5°C do 40°C),
   - radiotelefon bazowy i stacja retransmisyjna spełnia wymagania normy ETSI EN 300 019-1-3 w zakresie promieniowania słonecznego klasa 3.1,wilgotności, zapylenia i piasku klasa 3.1, wibracji i udarów klasa 3.3, radiotelefon przewoźny spełnia wymagania normy ETSI EN 300 019-1-5: w zakresie promieniowania słonecznego klasa 5.1, wilgotności, zapylenia i piasku klasa 5.2, deszczu klasa 5.2, wibracji i udarów Typ II klasa 5M3, zderzeń z ciałami obcymi, kamieniami klasa 5M2, radiotelefon noszony spełnia wymagania normy ETSI EN 300 019 – 1-7. w zakresie promieniowania słonecznego klasa 7.2,wilgotności zapylenia i piasku klasa 7.2, deszczu klasa 7.3E wibracji i udarów Typ II klasa 5M3, zderzeń z ciałami obcymi, kamieniami klasa 5M3.

f) **wymagania uzupełniające**
   - zgodność parametrów urządzeń z wymaganiami w zakresie kompatybilności elektromagnetycznej określonymi w normach ETSI 301 489-1 i ETSI 300 019-5,
   - zgodność z wymaganiami w zakresie bezpieczeństwa określonymi w normie EN 60950-1.

4.6.1.2 Parametry dodatkowe dotyczące poszczególnych rodzajów urządzeń:

4.6.1.2.1 Stacje retransmisyjne

a) **parametry techniczne ogólne**
   - odstęp dupleksowy w zakresie od 4,5 do 9,5 MHz włącznie,
   - filtr dupleksowy w paśmie od 164,5 do 167,5 MHz włącznie dla odbiornika i w paśmie od 172 do 174 MHz włącznie dla nadajnika,
   - izolacja wzajemna pasm filtru dupleksowego nie mniejsza niż 60 dB,
   - tłumienność wtrąceniowa filtru dupleksowego nie większa niż 2 dB,
   - pobór mocy nie większy niż 250 W.

b) **parametry techniczne nadajnika**
   - moc wyjściowa nadajnika w.cz. regulowana w zakresie nie mniejszym niż od 5 W do 25 W (tylko w trybie serwisowym),
   - możliwość ustawienia poziomu mocy z krokiem nie większym niż 1 W (tylko w trybie serwisowym),
   - tłumienność intermodulacji nie mniejsza niż 70 dB.

c) **parametry techniczne odbiornika**
   - pogorszenie czułości nie może przekraczać 3 dB w przypadku równoczesnego nadawania i odbioru,
   - odporność na zakłócenia o częstotliwościach niepożądanych w przypadku równoczesnego nadawania i odbioru nie może być mniejsza niż 67 dB,
   - odporność na zakłócenia intermodulacyjne nie mniejsza od 70 dB.

d) **ogólne cechy użytkowe**
   - programowe ustawienie czasu podtrzymania transmisji po zaniku sygnału aktywacji retransmisji,
   - możliwość wysyłania tonów CTCSS w czasie podtrzymania retransmisji,
   - możliwość retransmisji sygnałów selektywnego wywołania w standardach: CCIR 100 ms, CCIR 70 ms, EEA 40 ms,

- przeźroczystość dla retransmisji maskowanej korespondencji głosowej,
- retransmisja jednej z co najmniej 5 sieci radiowych pracujących na tym samym kanale z różnymi kodami blokady szumów CTCSS.

e) dodatkowe cechy użytkowe

- praca na dowolnym z co najmniej 16 kanałów możliwych do zaprogramowania,
- zabezpieczenie przepięciowe i przed odwrotnym podłączeniem biegunów zasilania,
- praca ze źródłem zasilania rezerwowego (akumulatorem lub baterią akumulatorów) o napięciu znamionowym 12V lub 24V,
- automatyczne, bezzwłoczne przełączanie z zasilania sieciowego na rezerwowe i odwrotnie,
- automatyczne ładowanie „*on – line*" akumulatora zasilania rezerwowego,
- automatyczne zabezpieczenie akumulatora przed nadmiernym rozładowaniem,
- możliwość zdefiniowania obniżonego poziomu mocy wyjściowej nadajnika dla pracy ze źródła zasilania rezerwowego,
- możliwość pracy stacji z odłączonym akumulatorem zasilania rezerwowego,
- wskazana (nieobligatoryjna) sygnalizacja pracy ze źródła zasilania rezerwowego za pomocą sygnału akustycznego transmitowanego w trakcie nadawania,
- wskazana (nieobligatoryjna) sygnalizacja przekroczenia dopuszczalnego WFS toru antenowego za pomocą sygnału akustycznego transmitowanego podczas nadawania,
- lokalna manipulacja z panelu sterującego umożliwiająca:
  - zmianę kanału pracy, ze wskazaniem wybranego kanału,
  - odbiór i nadawanie korespondencji głosowej na wybranym kanale,
  - regulację głośności (w przypadku możliwości odsłuchu za pomocą wbudowanego głośnika).

f) parametry techniczne anteny

- pasmo częstotliwości pracy 164 ÷174 MHz,
- WFS ≤ 1,6 w paśmie częstotliwości pracy,
- zysk ≥ 0 dB_d,
- dopuszczalna moc min. 50 W,
- impedancja 50 Ω,
- polaryzacja pionowa,
- w zależności od potrzeb dookólna lub kierunkowa (sektorowa) charakterystyka promieniowania w płaszczyźnie poziomej,
- zakres temperatury pracy od -40°C do +70°C,
- wymiary: długość do 5 m (nie dotyczy anten kierunkowych)
- wytrzymałość na złamanie przy wiatrach o prędkości min. 150 km/h,

g) parametry przewodu antenowego

- impedancja falowa 50 Ω,
- tłumienność falowa ≤ 5 dB/100m dla częstotliwości 174 MHz, przy czym całkowita tłumienność toru antenowego dla danego radiotelefonu nie powinna przekraczać 3 dB.

h) parametry techniczne zabezpieczenia odgromowego anteny

- prąd w impulsie 50 kA,
- WFS ≤ 1,1 w całym paśmie,
- pasmo pracy min. 100 ÷ 200 MHz,

- tłumienność ≤ 0,15 dB.

4.6.1.2.2 Radiotelefony bazowe lub biurkowe

a) **parametry techniczne nadajnika**
   - moc wyjściowa nadajnika w.cz. regulowana w zakresie co najmniej od 5 W do 25 W (tylko w trybie serwisowym),
   - możliwość ustawienia poziomu mocy z krokiem nie większym niż 1 W (tylko w trybie serwisowym),
   - tłumienność intermodulacji nie mniejsza niż 70 dB.

b) **parametry techniczne odbiornika**
   - odporność na zakłócenia intermodulacyjne nie mniejsza od 70 dB.

c) **sterowanie zespołu nadawczo-odbiorczego (NO) z manipulatorów operatorskich (w przypadku radiotelefonów z takim sterowaniem)**
   - sterowanie radiotelefonu (zespołu nadawczo-odbiorczego) z manipulatora operatorskiego (konsoli) przez niekomutowaną jednoparową linię telefoniczną, na odległość nie mniejszą niż 10 km (o tłumienności falowej linii do 15 dB dla 1 kHz) z uwzględnieniem możliwości sterowania poprzez linię wykonaną częściowo w technice światłowodowej,
     albo
     sterowanie radiotelefonu (zespołu nadawczo odbiorczego) z manipulatora operatorskiego (konsoli) z wykorzystaniem protokołu TCP/IP, z wykorzystaniem styku Ethernet 10/100/1000 Mbps (złącze RJ 45), z możliwością adresowana urządzeń z wykorzystaniem adresu MAC,
   - dopuszcza się stosowanie automatycznego protokołu negocjacji parametrów połączenia (nie wymagających indywidualnej regulacji obwodów urządzenia w zależności od długości linii, jej parametrów, parametrów sieci IP)

d) **ogólne cechy użytkowe**
   - programowe ustawienie dowolnego kanału do pracy w skaningu (z możliwością nadawania priorytetu i co najmniej 5 skanowanych kanałów),
   - przystosowanie do zainstalowania (w manipulatorze operatorskim) i pracy z urządzeniem maskującym korespondencję głosową, na zasadzie „Plug-in" (bez lutowania i przecinania ścieżek),
   - wybór kanałów przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
   - regulacja głośności,
   - minimalny poziom głośności ustawiany programowo,
   - manipulator operatorski musi zapewniać:
     - włączanie i wyłączanie manipulatora,
     - zmianę kanału pracy radiotelefonu,
     - wyświetlanie nazwy wybranego kanału,
     - możliwość załączania i wyłączania blokady szumów,
     - możliwość załączania i wyłączania kodowanej blokady szumów CTCSS,
     - możliwość aktywowania nadajnika przyciskiem ręcznym i nożnym (wyposażenie opcjonalne),
     - regulację głośności (poziomu sygnału akustycznego z odbiornika),

- sygnalizację stanów awaryjnych zespołu N/O: zanik napięcia sieciowego (praca z zasilania rezerwowego), z zewnętrznych czujników alarmowych (m.in. czujnik pożaru, włamania),
- włączanie i wyłączanie pracy z maskowaniem mowy oraz możliwość wyboru przez operatora jednego z co najmniej trzech dostępnych kluczy kodowych,
- współpracę z rejestratorami rozmów,
- możliwość dołączenia do manipulatora operatorskiego, manipulatora dodatkowego za pomocą niekomutowanej linii telefonicznej o długości minimum 300 m lub sieci z wykorzystaniem protokołu IP,
- manipulator dodatkowy musi zapewniać minimum: nadawanie i odbiór korespondencji na kanale wybranym w manipulatorze operatorskim (korespondencja radiowa prowadzona z użyciem manipulatora głównego musi być słyszalna w manipulatorze dodatkowym i na odwrót).

e) dodatkowe cechy użytkowe stacji bazowych

- praca na dowolnym z co najmniej 100 zaprogramowanych kanałów,
- wyposażenie manipulatora operatorskiego w złącze akcesoryjne umożliwiające podłączenie dodatkowego głośnika i mikrotelefonu z przyciskiem nadawania,
- zabezpieczenie przepięciowe i przed odwrotnym podłączeniem biegunów zasilania,
- jako dodatkowe rozwiązanie dopuszcza się możliwość wyposażenia w zestaw nagłowny (słuchawki i mikrofon) dla dyspozytora obsługującego stację bazową (manipulator operatorski),
- automatyczne, bezzwłoczne przełączanie z zasilania sieciowego na rezerwowe i odwrotnie,
- automatyczne ładowanie „*on – line*" akumulatora zasilania rezerwowego,
- automatyczne zabezpieczenie akumulatora przed nadmiernym rozładowaniem,
- możliwość pracy stacji z odłączonym akumulatorem zasilania rezerwowego,
- lokalna manipulacja z panelu sterującego zespołu N/O, umożliwiająca:
  - zmianę kanału pracy, ze wskazaniem wybranego kanału,
  - odbiór i nadawanie na wybranym kanale,
  - regulację głośności (w przypadku odsłuchu za pomocą wbudowanego głośnika),

i) parametry techniczne anteny

- pasmo częstotliwości pracy 164 ÷174 MHz,
- WFS ≤ 1,6 w paśmie częstotliwości pracy,
- zysk ≥ 0 dB_d,
- dopuszczalna moc min. 50 W,
- impedancja 50 Ω,
- polaryzacja pionowa,
- w zależności od potrzeb dookólna lub kierunkowa (sektorowa) charakterystyka promieniowania w płaszczyźnie poziomej,
- zakres temperatury pracy od -40°C do +70°C,
- wymiary: długość do 5 m (nie dotyczy anten kierunkowych)
- wytrzymałość na złamanie przy wiatrach o prędkości min. 150 km/h,

j) parametry przewodu antenowego

- impedancja falowa 50 Ω,

– tłumienność falowa ≤ 5 dB/100m dla częstotliwości 174 MHz, przy czym całkowita tłumienność toru antenowego dla danego radiotelefonu nie powinna przekraczać 3 dB.

k) parametry techniczne zabezpieczenia odgromowego anteny

- prąd w impulsie 50 kA,
- WFS ≤ 1,1 w całym paśmie,
- pasmo pracy min. 100 ÷ 200 MHz,
- tłumienność ≤ 0,15 dB.

4.6.1.2.3 Radiotelefony przewoźne

a) parametry techniczne nadajnika

- moc wyjściowa nadajnika w.cz. regulowana w zakresie co najmniej od 2 W do 25 W (tylko w trybie serwisowym),
- możliwość ustawienia poziomu mocy z krokiem nie większym niż 1 W (tylko w trybie serwisowym).

b) parametry techniczne odbiornika

- maksymalna moc wyjściowa akustyczna dostarczana do głośnika minimum 3 W,
- odporność na zakłócenia intermodulacyjne nie mniejsza niż 65 dB.

c) ogólne cechy użytkowe

- praca na dowolnym z co najmniej 250 zaprogramowanych kanałów,
- programowe ustawienie dowolnego kanału do pracy w skaningu (z możliwością nadawania priorytetu i co najmniej 5 skanowanych kanałów),
- włączanie/wyłączanie przez użytkownika blokady szumów dedykowanym lub ustawianym programowo do tego celu przyciskiem łatwo dostępnym na obudowie radiotelefonu,
- włączanie/wyłączanie przez użytkownika kodowej blokady szumów dedykowanym do tego celu przyciskiem łatwo dostępnym na obudowie radiotelefonu (lub ustawionym programowo),
- przystosowanie do zainstalowania i pracy z urządzeniem maskującym korespondencję głosową na zasadzie „Plug-in" (bez lutowania i przecinania ścieżek),
- łatwo dostępne przyciski funkcyjne umożliwiające po instalacji urządzenia maskującego korespondencję głosową: wł./wył. maskowania korespondencji, wybór do pracy dowolnego zaprogramowanego klucza kodowego,
- wybór kanałów przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- regulacja głośności potencjometrem, przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- ustawiany programowo minimalny poziom głośności,
- blokowanie/odblokowanie radiotelefonu drogą radiową,
- łatwo dostępne na obudowie przyciski funkcyjne umożliwiające włączenie/wyłączenie skanowania, włączenie trybu alarmowego,
- zabezpieczenie przepięciowe i przed odwrotnym podłączeniem biegunów zasilania,
- wyposażenie w złącze akcesoryjne (znajdujące się na obudowie radiotelefonu) umożliwiające sterowanie zewnętrznymi urządzeniami (syreny, światła)

uruchamiane sygnałem selektywnego wywołania, możliwość podłączenia dodatkowego głośnika, mikrofonu, przycisku nadawania, włącznika alarmu,
- wysyłanie sygnału alarmu w oparciu o system selektywnego wywołania z wbudowaną funkcją monitorowania (podsłuchu) wnętrza kabiny,
- możliwość instalacji rozdzielnej zespołu N/O i manipulatora w pojeździe (zapewniające zachowanie wszystkich funkcji radiotelefonu).

d) akcesoria wymagane w zestawie
- mikrofon zewnętrzny z zaczepem i przyciskiem nadawania,
- głośnik zewnętrzny o mocy min. 5 W z przewodem o długości min. 5 m (jeżeli radiotelefon nie posiada wbudowanego głośnika lub w razie potrzeby),
- mikrofon kamuflowany, z przewodem o długości min. 5 m (w przypadku radiotelefonu w wersji kamuflowanej lub w przypadku montażu rozdzielnego),
- kamuflowany włącznik nadawania, z przewodem o długości min. 5 m (w przypadku radiotelefonu w wersji kamuflowanej lub w przypadku montażu rozdzielnego),
- przewód instalacji rozłącznej o długości min. 5 m oraz inne elementy umożliwiające wykonanie montażu rozdzielnego radiotelefonu (tylko dla radiotelefonu w wersji kamuflowanej lub montażu rozłącznego),
- dedykowany zewnętrzny nożny włącznik alarmu, z przewodem o długości min. 5 m (opcjonalnie),
- niezbędne przewody, złącza i elementy umożliwiające bezpieczne zamontowanie w pojeździe (przewód zasilający o długości 7 m z zabezpieczeniem od strony akumulatora i możliwością rozłączenia gniazda bezpiecznikowego na przewodzie).

e) antena samochodowa
- pasmo częstotliwości pracy 164 ÷174 MHz,
- WFS ≤ 2 (w pełnym paśmie),
- zysk ≥ 0 dB_d,
- dopuszczalna moc min. 30 W,
- impedancja 50 Ω,
- polaryzacja pionowa,
- zakres temperatury pracy -30°C ÷ +60°C,
- kabel antenowy o długości minimum 5 m powinien być wyprowadzony z grzybka antenowego, złącze antenowe dedykowane do zainstalowania na przewodzie antenowym (luzem).

4.6.1.2.4 Radiotelefony noszone

a) parametry techniczne nadajnika
- moc wyjściowa nadajnika w.cz. regulowana w zakresie od 0,5 W do 5 W (tylko w trybie serwisowym),
- możliwość ustawienia poziomu mocy z krokiem nie większym niż 0,7 W (tylko w trybie serwisowym).

b) parametry techniczne odbiornika
- maksymalna moc wyjściowa akustyczna dostarczana do głośnika min. 0,5 W.

c) ogólne cechy użytkowe
- praca na dowolnym z co najmniej 250 zaprogramowanych kanałów,

- programowe ustawienie dowolnego kanału do pracy w skaningu (z możliwością nadawania priorytetu i co najmniej 5 skanowanych kanałów),
- jednoczesna praca z kodową blokadą szumów i selektywnym wywołaniem,
- przystosowanie do zainstalowania i pracy z urządzeniem maskującym korespondencję głosową na zasadzie „Plug-in" (bez lutowania i przecinania ścieżek),
- dedykowany lub ustawiany programowo, łatwo dostępny przycisk sygnału alarmowego (np. odróżniający się od innych przycisków kolorem),
- wybór kanałów przełącznikiem obrotowym,
- regulacja głośności potencjometrem lub przełącznikiem obrotowym,
- ustawiany programowo minimalny poziom głośności,
- sygnalizacja wizualna stopnia naładowania akumulatora oraz sygnalizacja akustyczna rozładowania (z możliwością programowego wyłączenia),
- złącze umożliwiające podłączenie dodatkowych akcesoriów, np.:
  - mikrofonogłośnik,
  - kamuflowany przewodowy i bezprzewodowy zestaw mikrofonosłuchawkowy,
  - przystosowanie do podłączenia adaptera z trwale osadzonym złączem (np.: 12–pinowym typu „Hirose") - przeznaczonym do podłączenia osprzętu obecnie eksploatowanych w Policji.
- możliwość włączania/wyłączania przez użytkownika blokady szumów dedykowanym lub ustawionym programowo do tego celu przyciskiem łatwo dostępnym na obudowie radiotelefonu,
- włączanie/wyłączanie przez użytkownika kodowej blokady szumów dedykowanym do tego celu przyciskiem łatwo dostępnym na obudowie radiotelefonu.

d) akcesoria wymagane w zestawie
- antena na pasmo 164÷174 MHz, o długości maksimum 200 mm,
- akumulator zapewniający pracę przez min. 8 godz. przy proporcjach nadawanie/odbiór/stan gotowości wynoszących odpowiednio 5%/5%/90% i mocy nadajnika 5 W,
- klips do pasa.

e) akcesoria opcjonalne
- przejście na gniazdo antenowe BNC (jeżeli radiotelefon wyposażony jest w złącze antenowe innego standardu),
- mikrofonogłośnik,
- futerał z zaczepem obrotowym do pasa,
- dodatkowe akumulatory.

4.6.1.2.5 Radiotelefony noszone kamuflowane

a) parametry techniczne nadajnika
- moc wyjściowa nadajnika w.cz. regulowana w zakresie od 0,5 W do 2 W (tylko w trybie serwisowym),
- możliwość ustawienia poziomu mocy z krokiem nie większym niż 0,7 W.

b) ogólne cechy użytkowe

- radiotelefon o małych gabarytach przeznaczony do pracy kamuflowanej, łatwy do ukrycia,
- praca na dowolnym z co najmniej 32 zaprogramowanych kanałów,
- przystosowanie do zainstalowania i pracy z urządzeniem maskującym korespondencję głosową na zasadzie „Plug-in" (bez lutowania i przecinania ścieżek),
- sygnalizacja wizualna stopnia naładowania akumulatora oraz sygnalizacja akustyczna rozładowania (z możliwością programowego wyłączenia),
- wybór kanałów przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- regulacja głośności potencjometrem, przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- ustawiany programowo minimalny poziom głośności,
- złącze umożliwiające podłączenie dodatkowych akcesoriów np.:
  - kamuflowany bezprzewodowy i przewodowy zestaw mikrofonosłuchawkowy,
  - kamuflowany zestaw wieloczęściowy.
- łatwo dostępne przyciski funkcyjne umożliwiające po instalacji urządzenia maskującego korespondencję głosową: wł/wył maskowania korespondencji, wybór do pracy dowolnego zaprogramowanego klucza kodowego,
- blokowanie/odblokowanie radiotelefonu drogą radiową,
- możliwość włączania/wyłączania przez użytkownika blokady szumów dedykowanym lub ustawionym programowo do tego celu przyciskiem łatwo dostępnym na obudowie radiotelefonu,
- możliwość włączania/wyłączania przez użytkownika kodowej blokady szumów dedykowanym lub ustawionym programowo do tego celu przyciskiem łatwo dostępnym na obudowie radiotelefonu.

4.6.2 Łączność radiotelefoniczna analogowo-cyfrowa

4.6.2.1 Stacja retransmisyjna standardu DMR (ang. Digital Mobile Radio)

a) ogólne cechy użytkowe:

- praca w systemie cyfrowym zgodnym ze specyfikacją ETSI TS 102 361 (tier II) oraz w systemie analogowym (z modulacją F3E) w trybach simpleks/duosimpleks, dupleks,
- złącze umożliwiające programowanie parametrów stacji oraz transmisję danych zgodną ze standardem USB,
- programowalny adres IP,
- możliwość podłączenia do sieci ETHERNET,
- przypisany adres sprzętowy (MAC adres),
- każdy sposób dostępu do danych konfiguracyjnych stacji, ich odczytu i/lub zmiany, zabezpieczony hasłem,
- obsługa transmisji maskowanych i jawnych,
- zasilanie podstawowe: sieć AC 230 V ± 10 %, 50 Hz,
- odporność obwodów zasilania AC na zapady i przerwy napięcia oraz udary według wymagań określonych w normie ETSI EN 301 489-1,

- automatyczne, bezzwłoczne przełączenie z zasilania sieciowego na rezerwowe i odwrotnie, zapewniające nieprzerwaną pracę,
- automatyczne ładowanie "on-line" baterii akumulatorów zasilania rezerwowego,
- automatyczne zabezpieczenie baterii zasilania rezerwowego przed nadmiernym rozładowaniem
- odporność przyłączy telekomunikacyjnych stacji na udary według wymagań określonych w normie ETSI EN 301 489-1
- zakres temperatury pracy od –30°C do +60°C

b) parametry techniczne

- minimalny zakres częstotliwości pracy 148 ÷ 174 MHz,
- odstęp dupleksowy (do pracy w trybach duosimpleks lub dupleks) ustalany indywidualnie dla lokalizacji posadowienia urządzenia,
- modulacja analogowa w kanale 12,5 kHz: częstotliwości (11K0F3E)
- protokół cyfrowy zgodny z ETSI TS102 361 (tier II)
- modulacja cyfrowa w kanale 12,5 kHz: 2 szczeliny TDMA (7K60FXD dane, 7K60FXE dane i głos),
- praca w dowolnym z co najmniej 16 zaprogramowanych kanałów (ewentualny wymóg zdalnej zmiany kanału uzależniony od lokalizacji posadowienia urządzenia),
- maksymalna dopuszczalna odchyłka częstotliwości fali nośnej ± 0,5 ppm,
- czułość analogowa odbiornika nie gorsza niż 0,4 μV dla SINAD 20 dB oraz 0,3 μV dla SINAD 12 dB
- czułość cyfrowa nie gorsza niż 0,3 μV przy 5% BER
- selektywność sąsiedniokanałowa ≥ 60 dB dla kanału 12,5 kHz
- odporność odbiornika na intermodulacje ≥ 70 dB
- tłumienie (selektywność dla) odbiorów niepożądanych ≥ 70 dB
- kodowa blokada szumów (CTCSS) wybierana programowo w dowolnym kanale analogowym z możliwością zaprogramowania dowolnego kodu z zakresu 67÷255 Hz (programowana ze skokiem 0,1 Hz)
- retransmisja tonów CTCSS
- moc fali nośnej nadajnika, programowana w zakresie 1-25 W,
- programowe ograniczenie czasu nadawania w granicach od 15 do 480 s ze skokiem 15 s

c) wymagania uzupełniające

- parametry radiowe, których nie wyszczególniono w niniejszych wymaganiach muszą być zgodne z odpowiednimi normami: odnośnie parametrów systemu analogowego z ETSI EN 300 086, odnośnie parametrów systemu cyfrowego z ETSI TS 102 361-1 oraz ETSI EN 300 113
- charakterystyki kompatybilności elektromagnetycznej stacji pod względem emisyjności i odporności na zaburzenia elektromagnetyczne muszą być zgodne z wymaganiami określonymi w normach ETSI EN 301 489-1 i ETSI EN 301 489-5
- pod względem bezpieczeństwa użytkowania stacje retransmisyjne oraz ich wyposażenie dodatkowe muszą być zgodne wymaganiami określonymi w normie EN 60950-1

4.6.2.2 Radiotelefon przewoźny standardu DMR

a) ogólne cechy użytkowe

- praca w systemie cyfrowym zgodnym ze specyfikacją ETSI TS 102 361 (tier II),
- oraz w systemie analogowym (modulacja F3E) w trybach simpleks/duosimpleks,
- wyświetlacz z podświetlaniem, umożliwiający jednoczesne wyświetlenie co najmniej 16 znaków, wizualizację odbieranych i wysyłanych wywołań oraz poziomu sygnału odbieranego w trybie cyfrowym,
- programowanie wyświetlanej nazwy kanału – co najmniej 14 znaków alfanumerycznych,
- programowe ograniczanie czasu nadawania,
- możliwość skanowania kanałów analogowych z kanału cyfrowego oraz grup i kanałów cyfrowych z kanału analogowego,
- możliwość wysyłania i odbierania wiadomości tekstowych, zdefiniowanych na etapie konfigurowania (programowania) sprzętu,
- wizualna sygnalizacja stanów pracy radiotelefonu, w tym: wywołań, skaningu i stanów monitorowania,
- wokoder cyfrowy zgodny z AMBE+2,
- wbudowany odbiornik GPS,
- wywołanie indywidualne, grupowe, alarmowe oraz okólnikowe (wszystkich) w trybie cyfrowym z identyfikacją na wyświetlaczu użytkownika wywołującego i sygnalizacją akustyczną (z możliwością wyłączenia sygnalizacji akustycznej)
- programowalny adres IP radiotelefonu
- wymagane są następujące funkcje:
  - zdalne sprawdzenie obecności radiotelefonu w sieci,
  - zdalne zablokowanie radiotelefonu,
  - zdalne odblokowanie radiotelefonu,
- kodowa blokada szumów CTCSS wybierana programowo w dowolnym kanale analogowym,
- możliwość pracy w systemie cyfrowym z wieloma urządzeniami retransmisyjnymi pracującymi na tej samej parze częstotliwości, z możliwością rozróżnienia urządzeń retransmisyjnych,
- wybór kanałów przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- regulacja głośności przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- złącze akcesoriów umożliwiające programowanie radiotelefonu i transmisję danych zgodną ze standardem USB, dołączenie dodatkowego głośnika i mikrofonu, przycisku nadawania,
- zasilanie DC 13,2 V ±20%, minus na masie,
- zabezpieczenie przed odwrotnym dołączeniem biegunów zasilania,
- odporność obwodów zasilania DC na zaburzenia występujące w sieci elektrycznej pojazdu (stany przejściowe i udary) według wymagań określonych w normie ETSI EN 301 489-1 (ISO 7637-2)
- złącze antenowe VHF typu BNC,
- złącze do anteny zewnętrznej GPS,
- wbudowany wewnętrzny głośnik,

- możliwość programowego tworzenia listy kontaktów (książki adresowej) - wywołań indywidualnych w trybie cyfrowym,
- menu radiotelefonu w języku polskim,
- wymagania dla zestawu rozłącznego określa użytkownik,
- wymagania dla zestawu biurkowego określa użytkownik.

b) parametry techniczne

- zakres częstotliwości pracy 148÷174 MHz,
- modulacja analogowa w kanale 12,5 kHz: częstotliwości (11K0F3E),
- protokół cyfrowy zgodny z ETSI TS102 361 (tier II),
- modulacja cyfrowa w kanale 12,5 kHz: 2 szczeliny TDMA (7K60FXD dane, 7K60FXE dane i głos),
- możliwość zaprogramowania co najmniej 250 kanałów z możliwością podziału na strefy,
- maksymalna dopuszczalna odchyłka częstotliwości fali nośnej ± 2 ppm,
- maksymalna dopuszczalna dewiacja częstotliwości dla FM: ±2,5 kHz,
- moc wyjściowa fali nośnej nadajnika programowana (tylko w trybie serwisowym) w całym zakresie częstotliwości w granicach od 1 W do 25 W,
- możliwość ustawienia przez użytkownika radiotelefonu jednego z dwóch poziomów mocy nadawania (moc niska, moc wysoka) (– predefiniowanych na etapie programowania sprzętu przez personel techniczny) w dowolnym kanale,
- moc na kanałach sąsiednich – system analogowy i cyfrowy: ≤ 60 dBc,
- charakterystyka pasma akustycznego (+1,–3 dB) – nadajnik system analogowy,
- łączne zniekształcenia modulacji ≤ 3%, przy 1 kHz, dewiacja 60% wartości maksymalnej,
- odstęp od zakłóceń –40 dB – nadajnik system analogowy,
- czułość analogowa odbiornika nie gorsza niż 0,3 μV dla SINAD 12 dB,
- czułość cyfrowa nie gorsza niż 0,3 μV przy 5% BER,
- selektywność sąsiedniokanałowa ≥ 60 dB dla kanału 12,5 kHz,
- tłumienie (selektywność dla) odbiorów niepożądanych ≥ 70 dB,
- współczynnik zawartości harmonicznych ≤ 5 %, przy 1 kHz, dewiacja 60% wartości maksymalnej i mocy akustycznej 0,5 W,
- charakterystyka pasma akustycznego (+1,–3 dB) – odbiornik system analogowy,
- odstęp od zakłóceń –40 dB – odbiornik system analogowy,
- moc wyjściowa akustyczna dla głośnika wewnętrznego minimum 3 W.

c) środowisko i klimatyczne warunki pracy

- zakres temperatury pracy od –20°C do +55°C,
- klasa ochrony obudowy przez wnikaniem pyłu i wody, wg normy EN 60529: IP 54.

d) wymagania uzupełniające

- parametry radiowe, których nie wyszczególniono w niniejszych wymaganiach muszą być zgodne z odpowiednimi normami: odnośnie parametrów systemu analogowego z ETSI EN 300 086, odnośnie parametrów systemu cyfrowego z ETSI TS 102 361-1 oraz ETSI EN 300 113
- charakterystyki kompatybilności elektromagnetycznej stacji pod względem emisyjności i odporności na zaburzenia elektromagnetyczne muszą być zgodne z wymaganiami określonymi w normach ETSI EN 301 489-1 i ETSI EN 301 489-5

- pod względem bezpieczeństwa użytkowania radiotelefony oraz ich wyposażenie dodatkowe muszą być zgodne wymaganiami określonymi w normie EN 60950-1

4.6.2.3 Radiotelefon noszony standardu DMR

a) ogólne cechy użytkowe

- praca w systemie cyfrowym zgodnym ze specyfikacją ETSI TS 102 361 (tier II) oraz w systemie analogowym (modulacja F3E) w trybach simpleks/duosimpleks,
- wyświetlacz z podświetlaniem, umożliwiający jednoczesne wyświetleniem co najmniej 16 znaków, wizualizację odbieranych i wysyłanych wywołań, poziomu sygnału odbieranego w trybie cyfrowym oraz stanu naładowania baterii,
- programowanie wyświetlanej nazwy kanału – co najmniej 14 znaków alfanumerycznych,
- standardowa klawiatura numeryczna (w zależności od wymagań użytkownika),
- wbudowane mikrofon i głośnik,
- programowe ograniczanie czasu nadawania,
- możliwość skanowania kanałów analogowych z kanału cyfrowego oraz grup i kanałów cyfrowych z kanału analogowego,
- możliwość wysyłania i odbierania wiadomości tekstowych, zdefiniowanych na etapie konfigurowania (programowania) sprzętu,
- wizualna sygnalizacja stanów pracy radiotelefonu, w tym: wywołań, skaningu i stanów monitorowania,
- wokoder cyfrowy zgodny z AMBE+2,
- wbudowany odbiornik GPS,
- wywołanie indywidualne, grupowe, alarmowe oraz okólnikowe (wszystkich) w trybie cyfrowym z identyfikacją na wyświetlaczu użytkownika wywołującego i sygnalizacją akustyczną (z możliwością wyłączenia sygnalizacji akustycznej),
- programowalny adres IP radiotelefonu,
- dedykowany łatwo dostępny przycisk wywołania alarmowego,
- wymagane są następujące funkcje:
  - zdalne sprawdzenie obecności radiotelefonu w sieci,
  - zdalne zablokowanie radiotelefonu,
  - zdalne odblokowanie radiotelefonu,
- kodowa blokada szumów CTCSS wybierana programowo w dowolnym kanale analogowym,
- wybór kanałów – przełącznikiem obrotowym,
- regulacja głośności przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- złącze akcesoriów umożliwiające programowanie radiotelefonu i transmisję danych zgodną ze standardem USB, dołączenie dodatkowego mikrofonogłośnika z przyciskiem nadawania,
- możliwość programowego tworzenia listy kontaktów (książki adresowej) - wywołań indywidualnych w trybie cyfrowym,
- możliwość wyłączenia sygnalizacji akustycznej i optycznej, tzw. "cicha praca",
- możliwość pracy w systemie cyfrowym z wieloma urządzeniami retransmisyjnymi pracującymi na tej samej parze częstotliwości, z możliwością rozróżnienia urządzeń retransmisyjnych,
- menu radiotelefonu w języku polskim,

b) parametry techniczne

- zakres częstotliwości pracy 148÷174 MHz,
- modulacja analogowa w kanale 12,5 kHz: częstotliwości (11K0F3E),
- protokół cyfrowy zgodny z ETSI TS102 361 (tier II),
- modulacja cyfrowa w kanale 12,5 kHz: 2 szczeliny TDMA (7K60FXD dane, 7K60FXE dane i głos),
- możliwość zaprogramowania co najmniej 250 kanałów z możliwością podziału na strefy,
- maksymalna dopuszczalna odchyłka częstotliwości fali nośnej ± 2 ppm,
- maksymalna dopuszczalna dewiacja częstotliwości dla FM: ±2,5 kHz,
- maksymalna moc nadajnika 5 W, programowana (tylko w trybie serwisowym) w całym zakresie częstotliwości w granicach od 1 W do 5 W,
- możliwość ustawienia przez użytkownika radiotelefonu jednego z dwóch poziomów mocy nadawania (moc niska, moc wysoka) – predefiniowanych a na etapie programowania sprzętu przez personel techniczny) w dowolnym kanale,
- moc na kanałach sąsiednich – system analogowy i cyfrowy: ≤ 60 dBc,
- charakterystyka pasma akustycznego (+1,–3 dB) – nadajnik system analogowy,
- łączne zniekształcenia modulacji ≤ 3%, przy 1 kHz, dewiacja 60% wartości maksymalnej,
- odstęp od zakłóceń –40 dB – nadajnik system analogowy,
- czułość analogowa odbiornika nie gorsza niż 0,3 μV dla SINAD 12 dB,
- czułość cyfrowa nie gorsza niż 0,3 μV przy 5% BER,
- selektywność sąsiedniokanałowa ≥ 60 dB dla kanału 12,5 kHz,
- tłumienie (selektywność dla) odbiorów niepożądanych ≥ 70 dB,
- współczynnik zawartości harmonicznych ≤ 5 %, przy 1 kHz, dewiacja 60% wartości maksymalnej i mocy akustycznej 0,5 W,
- charakterystyka pasma akustycznego (+1,–3 dB) – odbiornik system analogowy,
- odstęp od zakłóceń –40 dB – odbiornik system analogowy,
- moc wyjściowa akustyczna dla głośnika wewnętrznego minimum 0,5 W,

c) środowisko i klimatyczne warunki pracy

- minimalny zakres temperatury pracy radiotelefonu –20°C do +55°C,
- klasa ochrony obudowy przez wnikaniem pyłu i wody, wg normy EN 60529: IP 57.

d) wymagania uzupełniające

- parametry radiowe, których nie wyszczególniono w niniejszych wymaganiach muszą być zgodne z odpowiednimi normami: odnośnie parametrów systemu analogowego z ETSI EN 300 086, odnośnie parametrów systemu cyfrowego z ETSI TS 102 361-1 oraz ETSI EN 300 113.
- charakterystyki kompatybilności elektromagnetycznej stacji pod względem emisyjności i odporności na zaburzenia elektromagnetyczne muszą być zgodne z wymaganiami określonymi w normach ETSI EN 301 489-1 i ETSI EN 301 489-5,
- pod względem bezpieczeństwa użytkowania radiotelefony oraz ich wyposażenie dodatkowe muszą być zgodne wymaganiami określonymi w normie EN 60950-1.

4.6.3 Inne systemy łączności radiotelefonicznej

Jednostki Policji mogą użytkować funkcjonujące lokalnie systemy TETRA i EDACS. Modernizacja i rozbudowa tych systemów oraz budowa nowych niewyspecyfikowanych w niniejszym dokumencie systemów wymaga uzyskania zgody Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji. Zgody takiej nie wymaga doposażenie istniejących systemów w sprzęt abonencki.

4.7 Terminale mobilne

4.7.1 Mobilny Terminal Noszony (MTN)

a) wymagania użytkowe

- procesor min. 600 MHz,
- pamięć RAM min. 128MB,
- pamięć Flash ROM min. 128MB,
- system operacyjny Microsoft Windows Mobile 6.0 (lub wyższej wersji), bądź równoważny, przystosowany do obsługi polskiej wersji językowej wraz z bezterminową licencją, dokumentacja w języku polskim,
- edytor tekstu dedykowany pod mobilny system operacyjny z bezterminową licencją w polskiej wersji językowej, dokumentacja w języku polskim,
- zasilacz sieciowy AC (230V 50Hz),
- dwa wymienne akumulatory ładowalne, każdy zapewniający minimum 8 godzin ciągłej pracy, z podświetleniem ekranu przez przynajmniej 4 godziny czasu pracy oraz dodatkowo osobny wbudowany akumulator w MTN podtrzymujący dane,
- wymiana baterii bez utraty danych,
- czas czuwania baterii nie mniej niż 96 godzin,
- ładowarka samochodowa do terminala umożliwiająca ładowanie akumulatora terminala przewodem elastycznym z gniazda zapalniczki (bez pośrednictwa stacji dokującej), ładowarka musi obsługiwać poziom napięcia 12V, 24V DC z gniazda zapalniczki i przetwarzać napięcie do napięcia znamionowego terminala, umożliwiającego ładowanie baterii zasilającej,
- stacja dokująca ze złączem USB i funkcjonalnością ładowania baterii MTN oraz synchronizowania go z komputerem typu desktop lub laptop wraz z oprogramowaniem i licencją,
- kabel połączeniowy USB min. 2 m,
- możliwość dokowania urządzenia w samochodzie z możliwością ładowania baterii,
- zaleca się, aby waga urządzenia nie przekraczała 460g,
- zaleca się, aby wymiary nie były większe niż 168 mm x 84 mm x 45 mm,
- specjalizowany pokrowiec z uchwytem, umożliwiający stabilne przymocowanie MTN do umundurowania funkcjonariusza w czasie, gdy urządzenie nie jest wykorzystywane, w sposób niekrępujący ruchów w trakcie przemieszczania się lub pościgu,
- kolorowy ekran dotykowy o rozdzielczości minimum 320x240 pixeli (QVGA), przekątna ekranu nie mniejsza, niż 3,5", ilość kolorów – co najmniej 65 tys., możliwość regulacji natężenia podświetlania ekranu, podświetlanie

równomierne na całej powierzchni ekranu. Czytelność ekranu gwarantowana w przypadku intensywnego nasłonecznienia,
- urządzenie dotykowe (rysik) chowane w obudowie MTN lub w pokrowcu,
- zewnętrzne porty we/wy: USB 1.1 (slave) lub wyższy,
- slot na kartę SD (dopuszczalny Mini, Micro) + karta pamięci min. 2 GB,
- klawiatura wirtualna (ekranowa), wbudowana fizyczna klawiatura QWERTY (podświetlana) nierozerwalnie zintegrowana z urządzeniem,
- slot standardowej karty SIM,
- wbudowany głośnik, wbudowany mikrofon,
- wbudowany optyczny czytnik kodów jedno i dwu wymiarowych oraz aplikacja umożliwiająca odczyt i dekodowanie kodów AZTEC (stosowanych w dowodach rejestracyjnych) oraz jedno i dwu wymiarowych kodów (jednowymiarowych: kod 128, RSS, UPC/EAN 128, Code 39, Code 93, I 2 Discrete 2 of 5, Coda bar oraz kodów dwuwymiarowych: MaxiCode PDF 417 DataMatrix) (tj. w dokumentach: dowód osobisty, prawo jazdy, paszport, dowód rejestracyjny) za pomocą fabrycznie wbudowanego optycznego czytnika kodów – aplikacja musi umożliwiać przekazanie odczytanych informacji do wskazanego pola innej aplikacji,
- wbudowany modem min. GPRS/EDGE/HSDPA bez blokady typu sim-lock, umożliwiający pracę w sieci każdego krajowego operatora telefonii komórkowej,
- przeglądarka internetowa Internet Explorer lub równoważna,
- wbudowany moduł GPS (Global Positioning System), który umożliwia jednoczesną bezkolizyjną pracę urządzeń radiowych,
- funkcjonalność określania pozycji GPS, oraz transmisji danych o położeniu z GPS poprzez łączność bezprzewodową GPRS/EDGE/HSDPA pod wskazany adres sieciowy APN, jak również udostępnienie informacji o położeniu terminala na potrzeby aplikacji pracujących pod kontrolą systemu operacyjnego zainstalowanego w MTN,
- narzędzie (aplikacja), która współpracując z modemem umożliwi przekazywanie informacji o położeniu funkcjonariusza posiadającego terminal,
- moduł GPS musi udostępniać dane o położeniu geograficznym „na żądanie",
- parametry pracy modułu GPS muszą być możliwe do wysterowania z aplikacji zewnętrznej zainstalowanej w jednostce Policji w tym wysterowania pracy modemu GPRS/EDGE/HSDPA w zakresie parametrów przesyłu danych,
- dane o lokalizacji muszą być przekazywane przez moduł GPS poprzez narzędzie (aplikacje) następnie do systemów centralnych Policji zgodnie z wykorzystywanym formatem. Terminal musi realizować powyższe funkcjonalności samodzielnie bez udziału operatora. Moduł GPS musi podać położenie również po otrzymaniu zapytania z systemu centralnego,
- moduł GPS musi podawać dane o położeniu po otrzymaniu zapytania z narzędzia (aplikacji narzędzia sprzętowego) zgodnie z interwałami czasowymi zdefiniowanymi w ustawieniach narzędzia,
- odporny na warunki środowiskowe panujące w trakcie normalnej eksploatacji: wstrząsy, zapylenie, wilgotność, temperaturę,
- odporny na swobodny upadek na twardą powierzchnię z wysokości minimum 1m,

- uruchomienie i praca od -15°C do 50°C, 5% do 95% względna wilgotność bez kondensacji,
- temperatura przechowywania od -40°C do 50°C,
- odporności na poziomie określonym normą PN-EN 60529:2003 IP54,
- zgodność z wymaganiami w zakresie kompatybilności elektromagnetycznej określonymi w normie PN-EN 55022:2006 lub nowszej,
- znak CE potwierdzający że spełnienie zasadniczych wymagań określonych w przepisach wykonawczych do ustawy o systemie oceny zgodności z dnia 24 sierpnia 2004 r. (Dz. U. z 2004 r. Nr 204, poz. 2087),
- oprogramowanie/biblioteka do autoryzacji i uwierzytelnienia użytkownika w oparciu o dane z szyfrowanej przestrzeni karty mikroSD krypto, zgodne z zainstalowanym systemem operacyjnym,

b) pozostałe wymagania

- zaleca się, aby oprogramowanie/biblioteka pozwalało na uwierzytelnianie 8 użytkowników uzyskujących do niego dostęp w oparciu o spersonalizowaną kartę mikroSD krypto z mikroprocesorem kryptograficznym, zawierającą dla każdego użytkownika klucz prywatny i certyfikat,
- użytkownik terminala może zalogować się do jego systemu operacyjnego wyłącznie przy użyciu właściwej spersonalizowanej karty mikroprocesorowej (karta mikroSD krypto), po podaniu właściwego kodu PIN do ww karty,
- użytkownik musi mieć możliwość zmiany swojego kodu PIN do karty mikroSD krypto,
- oprogramowanie/biblioteka musi wykorzystywać funkcje kryptograficzne właściwe dla karty mikroSD krypto z wykorzystaniem interfejsów PKCS#11 i MS CSP wersji zgodnej z dostarczonym systemem operacyjnym,
- oprogramowanie/biblioteka musi umożliwiać zdalną wymianę certyfikatu użytkownika udostępnionego na karcie mikroSD krypto we współpracy z przeglądarką w celu uzyskania dostępu do systemów teleinformatycznych Policji dla użytkownika,
- uwierzytelnienie użytkowników w zakresie zdalnej wymiany certyfikatu musi odbywać się poprzez wykorzystywany w Policji serwer uwierzytelniający BTUU,
- uwierzytelnienie użytkowników terminala opiera się o podpis cyfrowy z wykorzystaniem kluczy kryptograficznych i certyfikatów przechowywanych na karcie mikroSD krypto,
- w procesie uwierzytelniania użytkownika w BTUU musi być wykorzystywany podpis elektroniczny oparty o algorytm RSA realizowany przez kryptoprocesor karty mikroSD krypto oraz certyfikat użytkownika przechowywany na karcie mikroSD krypto,
- oprogramowanie/biblioteka musi umożliwiać przeprowadzenie uwierzytelnienia i autoryzacji użytkownika w BTUU na podstawie nr PIN użytkownika do certyfikatu i certyfikatu użytkownika oraz dostęp do jawnych systemów informatycznych w sieci PSTD poprzez przeglądarkę,

- mechanizm uwierzytelnienia i autoryzacji musi zapewniać jednoznaczną identyfikację użytkownika,
- certyfikaty użytkowników muszą znajdować się w obszarze pamięci chronionej; dostęp do certyfikatów możliwy jest tylko z wykorzystaniem procesora kryptograficznego,
- terminal musi umożliwiać nawiązanie bezpiecznej sesji SSL/TLS,
- proces uwierzytelnienia zgodny z BTUU z wykorzystaniem serwera Proxy,
- terminal musi umożliwiać zarządzanie użytkownikami, kluczami i certyfikatami,
- komunikacja między terminalem, a modułem obsługi żądań certyfikacyjnych realizowana jest przy pomocy Web Services,
- komunikacja między terminalem, a modułem obsługi żądań certyfikacyjnych jest chroniona protokołem TLS,
- oprogramowanie musi współpracować z dostarczonymi przez producenta kart mikroSD krypto bibliotekami CSP i PKCS#11 umożliwiającymi korzystanie z kart mikroSD krypto przez system operacyjny,
- czas logowania do systemu operacyjnego terminala z wykorzystaniem oprogramowania uwierzytelniającego nie może wynosić więcej niż 1,5 minuty (czas zawiera wpisania PIN-u do karty mikroSD krypto oraz PIN-u użytkownika do certyfikatu).

4.7.2 Mobilny Terminal Przewoźny (MTP)

Wymagania użytkowe:

- architektura, co najmniej 32 bitowa,
- procesor typu x86 taktowany z prędkością nie mniejszą, niż 933 MHz,
- pamięć operacyjna o pojemności, co najmniej 512 MB RAM z możliwością rozbudowy, do co najmniej 1 GB RAM,
- systemem operacyjny Microsoft Windows XP Professional (lub równoważny) z najnowszą obowiązującą stabilną wersją ServicePack deklarowaną przez producenta (licencja i nośnik CD) lub nowszy. System operacyjny z polską wersją językową oraz bezterminową, niezbywalną licencją,
- przeglądarka Internet Explorer w wersji co najmniej 5.5 (lub równoważna),
- dysk twardy o pojemności, co najmniej 30 GB,
- slot na kartę SIM operatora sieci komórkowej,
- dysk twardy wyposażony w system zabezpieczający przed skutkami gwałtownych ruchów urządzenia (np. upadku),
- zasilanie urządzenia ze standardowej instalacji samochodowej 12V/24V (zgodne z napięciem instalacji pojazdu, w którym będzie montowany MTP), w instalacji dostarczającej zasilanie do terminala ma być wmontowany włącznik umożliwiający odcięcie zasilania,
- edytor tekstu rozumiany jako oddzielna aplikacja (zainstalowana w MTP po instalacji systemu operacyjnego), edytor Word pakietu Microsoft Office 2007 Professional PL z polską wersją językową lub równoważny,
- ekran o rozdzielczości nie mniejszej niż 1024x768 pikseli (XVGA), przekątnej ekranu nie mniejszej niż 8" kolorowy, 32- bitowa głębia kolorów, z regulacją kontrastu i jasności. Czytelność ekranu musi być także zagwarantowana w przypadku intensywnego nasłonecznienia,

- klawiatura QWERTY z wbudowanym urządzeniem wskazującym (np. mysz optyczna, trackball) współpracujące z dostarczonym terminalem (MTP) za pomocą portu bluetooth.
- karta grafiki: minimum 64 MB RAM (pamięć karty może być wydzielana z pamięci operacyjnej RAM pod warunkiem zwiększenia jej ilości o wielkość pamięci wykorzystywanej przez kartę grafiki, dopuszcza się zastosowanie karty graficznej zintegrowanej z płytą główną,
- karta dźwiękowa + głośniki (głośniki jako integralne komponenty MTP), dopuszcza się zastosowanie karty dźwiękowej zintegrowanej z płytą główną,
- porty zewnętrzne: USB-2.0 – 2 szt., złącze równoległe - port LPT (dopuszcza się stosownie konwertera LPT/USB), interfejs sieciowy (RJ45),
- modem GPRS/EDGE/HSDPA bez blokady typu sim-lock, umożliwiający pracę w sieci każdego krajowego operatora telefonii komórkowej,
- urządzenie GPS współpracujące z terminalem,
- funkcjonalność określania pozycji GPS oraz transmisji danych o położeniu z GPS poprzez łączność bezprzewodową GPRS/EDGE/HSDPA pod wskazany adres sieciowy APN, jak również udostępnienie informacji o położeniu pojazdu na potrzeby aplikacji pracujących pod kontrolą systemu operacyjnego zainstalowanego w MTP,
- GPS musi być trwale i nierozłącznie połączony z elementami stałymi radiowozu,
- GPS musi udostępniać dane o położeniu geograficznym „na żądanie",
- parametry pracy modułu GPS muszą być możliwe do wysterowania z aplikacji zewnętrznej zainstalowanej w jednostce Policji w tym wysterowania pracy modemu GPRS/EDGE/HSDPA w zakresie parametru przesyłu danych,
- terminal musi posiadać możliwość (moduł) monitorowania systemów pokładowych,
- moduł ten musi umożliwiać monitorowanie stanu wybranych systemów pokładowych w radiowozie (np. uruchomienie silnika, włączenie sygnałów świetlnych i dźwiękowych, otwarcie drzwi, „przycisk antynapadowy"),
- w ramach pracy terminala muszą być wysterowane parametry pracy takie jak częstotliwości przesyłania danych o położeniu pojazdu w funkcji jego prędkości oraz wysterowania pracy modemu GPRS/EDGE/HSDPA w zakresie parametrów przesyłu danych,
- dane o położeniu radiowozu i stanie wybranych systemów pokładowych muszą być przekazywane przez MTP do centralnych systemów policyjnych w celu ich dalszego przetwarzania,
- przekazywanie z pojazdu sygnału alarmowego wywołanego przez kierowcę za pomocą ukrytego w kabinie przycisku antynapadowego musi odbywać się na zasadzie bezwzględnego priorytetu,
- terminal musi posiadać budowę modułową,
- terminal musi być odporny na warunki panujące w normalnej eksploatacji radiowozu policyjnego, czyli: wibrację, zapylenie, wilgotność, temperaturę,
- gwarantowana temperatura uruchomienia i pracy urządzenia musi znajdować się w przedziale od -25°C do +50°C, przy kondensacji pary wodnej (wilgotność względna od 0 do 95%),
- temperatura przechowywania od -40°C do 50°C,

- terminal powinien spełniać wymagania określone w normie PN-S 76020 (gwarantowana temperatura uruchomienia i pracy od -25°C do +55°C oraz kondensacja pary wodnej w zakresie wilgotności względnej od 5% do 95%),
- sprzęt powinien spełniać wymagania określone w dyrektywie Rady nr 72/245/EWG z dnia 20 czerwca 1972 r. odnoszącej się do zakłóceń radioelektrycznych (kompatybilności elektromagnetycznej) pojazdów (Dz. Urz. UE Polskie wydanie specjalne, rozdział 13, tom 001, str. 226, z późn. zm.),
- sposób montażu MTP w pojeździe powinien być zgodny z wytycznymi zawartymi w regulaminie nr 21 Europejskiej Komisji Gospodarczej Organizacji Narodów Zjednoczonych (EKG ONZ)-(EKG ONZ) - Jednolite przepisy dotyczące homologacji pojazdów w odniesieniu do wyposażenia wnętrza (Dz. Urz. UE L 188 z 16 lipca 2008 r., str. 32).

4.8 Inne systemy

4.8.1 System łączności satelitarnej

Usługi w zakresie łączności satelitarnej dla Policji realizowane są za pośrednictwem systemu **INMARSAT**, dla którego musi być:

a) **zapewniona możliwość, wykorzystania terminali końcowych (współpracujących z systemem INMARSAT), o następujących parametrach:**
   - transmisja mowy - 4,8 kb/s,
   - transmisja danych - 2,4 kb/s,
   - transmisja faksów grupy 3 - 2,4 kb/s.

b) **zapewniona zgodność sprzętowa i programowa z obecnie użytkowanymi urządzeniami w celu:**
   - pełnej wymienialności sprzętu pomiędzy użytkownikami telefonów satelitarnych w sytuacjach kryzysowych,
   - współpracy nowych urządzeń z eksploatowanymi obecnie samonaprowadzającymi antenami samochodowymi oraz antenami stacjonarnymi i przenośnymi.

4.8.2 System monitoringu wizyjnego

4.8.2.1 Moduł kamerowy

Punkty obserwacyjne, tam gdzie jest to niezbędne, należy wyposażać w zintegrowane kamery szybkoobrotowe lub kamery z głowicami uchylno-obrotowymi spełniające następujące, podstawowe parametry i funkcje:

- kamera kolorowa o wysokiej rozdzielczości i czułości z funkcją obserwacji nocnej (przełączenie na monochromatyczny tryb pracy),
- przetwornik CCD 1/4" lub lepszy,
- automatyczna przysłona i ogniskowanie,
- obiektyw ze zmienną ogniskową (zoom),
- szybka głowica (obrót w poziomie - 360°, w pionie – 0°÷90°),
- funkcja maskowania stref obserwacji,
- funkcja programowania tras śledzenia,

- wejścia alarmowe,
- obudowa kamery hermetyczna, odporna na uszkodzenia mechaniczne, zapewniająca optymalną jakość obrazu bez względu na pogodę.

4.8.2.2 Sieć transmisyjna dedykowana na potrzeby monitoringu

W celu zapewnienia właściwych parametrów transmisyjnych, odporności na zakłócenia i niezawodności systemu, transmisję sygnałów wizyjnych i telemetrycznych zaleca się realizować poprzez wykorzystanie okablowania światłowodowego, dopuszcza się też wykorzystanie kabli koncentrycznych. Podstawowym standardem dla wszystkich kart, urządzeń i okablowania jest specyfikacja 100BaseT/1Gb/10Gb. W przypadku braku na danym terenie infrastruktury telekomunikacyjnej lub budowy mobilnych systemów monitoringu wizyjnego, należy rozważyć możliwość zastosowania alternatywnego medium transmisyjnego np.: w postaci szerokopasmowego systemu dostępu radiowego typu punkt-wielopunkt. Zastosowanie szerokopasmowych łączy radiowych musi być poprzedzone uzyskaniem od właściwych merytorycznie instytucji wszelkich pozwoleń, zgodnie z obowiązującymi w tym zakresie przepisami dotyczącymi eksploatacji urządzeń i systemów radiowych. Sieć taka musi umożliwiać współpracę z sieciami podkładowymi WAN i MAN. Minimalna przepływność na jedną kamerę powinna wynosić min. 2 Mb/s.

4.8.2.3 Stanowisko nadzoru i rejestracji

Zaleca się, aby na stanowisku monitoringu wizyjnego realizowane były następujące podstawowe funkcje:

- podgląd obrazu z dowolnej kamery na monitorach kolorowych o wysokiej rozdzielczości i przekątnej ekranu min. 19",
- podgląd obrazów z wielu kamer na monitorze (dzielenie obrazu),
- rejestracja obrazów z zapisem daty i godziny - ciągła ze wszystkich kamer oraz z wybranej kamery na żądanie,
- rejestracja cyfrowa z jednoczesną archiwizacją (wielkość archiwum min. na 30 dni),
- sterowanie wszystkimi parametrami kamer,
- szybki dostęp do zarejestrowanych danych z możliwością przegrywania, obróbki i wydruku zarejestrowanych obrazów.

4.8.3 Rejestratory rozmów telefonicznych i radiowych

Rejestratory rozmów telefonicznych i radiowych muszą spełniać wymagania wynikające z zarządzenia nr 1173 Komendanta Głównego Policji z dnia 10 listopada 2004 roku w sprawie organizacji służby dyżurnej w jednostkach organizacyjnych Policji (Dz. Urz. KGP Nr 21, poz. 132). Ponadto rejestratory powinny spełniać następujące wymagania:

- zbudowane na bazie dedykowanej platformy sprzętowej - zalecana obudowa rack 19",
- możliwość zdalnego odsłuchu poprzez sieci TCP/IP,
- możliwość zbudowania sieciowego systemu rejestracji, odsłuchu i archiwizacji o strukturze rozproszonej,
- identyfikacja numeru CPA abonentów,
- synchronizacja czasu astronomicznego do wskazanego źródła,

- wymagany min. okres 12 miesięcy przechowywania nagrań w systemie, który umożliwi w trybie on-line zdalny odsłuch oraz 24 miesięczny okres przechowywania nagrań zarchiwizowanych na nośnikach zewnętrznych (dostęp w trybie off-line),
- możliwość rejestracji i przetwarzania faksów (w standardzie G3, G4 i T.38),
- możliwość rejestracji Select V w standardach jak dla radiotelefonów,
- identyfikacja i rejestracja połączeń,
- konfigurowalna automatyczna archiwizacja nagrań – w systemie bazodanowym,
- skalowalność umożliwiająca prostą rozbudowę,
- możliwość archiwizacji danych poprzez sieć TCP/IP,
- możliwość rejestracji treści prowadzonej rozmowy, numeru telefonu wybieranego i inicjującego połączenie, datę i czas trwania połączenia oraz dodatkowo zapis treści wyświetlacza z telefonów systemowych,
- możliwość sieciowej pracy rejestratorów oraz możliwość zrzutu danych do centralnego serwera archiwizacyjnego,
- dostęp do konfiguracji rejestratora – lokalnie i zdalnie,
- możliwość zapisu nagrań w postaci skompresowanej i nieskompresowanej,
- możliwość zdalnego nasłuchu nagrań aktualnie rejestrowanych,
- wielopoziomowy system zabezpieczeń i uprawnień,
- podgląd stanu aktywności i sprawności interfejsów na rejestratorach,
- raporty o stanie systemu w aplikacji zarządzającej,
- redundantne zasilacze hot-plug, minimum dwa w serwerze,
- możliwość przeprogramowania z poziomu użytkownika karty systemowej na inny system, w przypadku wymiany centrali,
- opcja mirror dysku.

Rozdział 5 Wymagania dotyczące użytkowania

W przypadku konieczności naprawy urządzeń, o których mowa w niniejszym rozdziale, poza siedzibą jednostki organizacyjnej Policji, dyski twarde i inne nośniki pamięci wchodzące w ukompletowanie tych urządzeń, muszą pozostać w miejscu ich użytkowania.

5.1 Stanowiska dostępowe sieci PSTD

Stanowiska dostępowe, które służą dostępowi do centralnych systemów Policji, muszą zawierać elementy pozwalające na niezaprzeczalną identyfikację użytkownika przez BTUU za pomocą mechanizmów PKI. Dla obecnie funkcjonujących rozwiązań dopuszcza się autoryzację opartą o CPSA.

5.1.1 Ogólne wymagania bezpieczeństwa stanowiska dostępowego:

a) dostęp do BIOS-u musi być zabezpieczony hasłem,
b) BIOS powinien uniemożliwić nieautoryzowane uruchomienie systemu operacyjnego z urządzenia innego, niż wskazano w jego ustawieniach,
c) należy zablokować możliwość uruchamiania stanowiska dostępowego za pomocą „bootowalnej" karty sieciowej,

d) sekwencję startową w BIOS-ie należy ustawić, tak aby system startował tylko i wyłącznie z dysku twardego, zawierającego główny sektor rozruchowy (MBR) w celu uniemożliwienia startu z innego napędu,
e) użytkownik stanowiska dostępowego powinien korzystać z konta z ograniczonymi uprawnieniami, założonego przez administratora lokalnego,
f) hasła użytkowników muszą składać się przynajmniej z 8 znaków i spełniać wymagania co do złożoności (angielskie duże znaki, małe znaki, niealfanumeryczne lub cyfry), maksymalnego okresu ważności - 180 dni, historii haseł – 5 pamiętanych haseł, próg blokady konta – 5 nieudanych prób zalogowania,
g) stanowisko dostępowe musi mieć uaktywniony, zabezpieczony hasłem wygaszacz ekranu, uruchamiany automatycznie po max. 10 minutach bezczynności,
h) wszystkie partycje dysku należy sformatować w systemie plików NTFS lub równoważnym zapewniającym podobne funkcjonalności,
i) podłączenie komputera do sieci PSTD bez czytnika kart mikroprocesorowych, a tym samym bez spersonalizowanej imiennej karty mikroprocesorowej spowoduje, że dany użytkownik PC nie będzie mógł korzystać z centralnych systemów informacyjnych Policji. Brak powyższych elementów konfiguracyjnych stanowiska dostępowego skutkuje nie spełnieniem wymogów w zakresie standardów uwierzytelniania użytkowników uzyskujących dostęp do centralnych zasobów informatycznych Policji,
j) zabrania się podłączania Stanowisk Dostępowych do sieci Internet. W przypadku zaistnienia konieczności przeklasyfikowania Stanowiska Dostępowego na SSR przed jego podłączeniem do sieci Internet należy usunąć bez możliwości odzyskania wszystkie dane zapisane na dyskach tego Stanowiska Dostępowego wraz z informacjami o strukturze nośnika danych,
k) zabrania się wykorzystywania Stanowisk Dostępowych z wymiennymi dyskami,
l) dla konfiguracji systemu operacyjnego zaleca się stosowanie zasad prowadzenia inspekcji oraz ustawień dzienników zdarzeń określonych w pkt. 9 *Ogólne zasady konfiguracji sprzętu komputerowego wykorzystywanego w jednostkach Policji (komputery stacjonarne, komputery przenośne).*

5.1.2 Rodzaje stanowisk dostępowych:

a) terminal znakowy dla aplikacji tekstowych:
   - AVT 200ID posiadający elektroniczny czytnik identyfikatora cyfrowego,
   - AVT 200.

b) standardowy komputer dostępowy:
   - oprogramowanie identyfikujące użytkownika,
   - elektroniczny czytnik kart mikroprocesorowych lub identyfikatora cyfrowego.

c) dedykowany i specjalizowany komputer dla dostępu do obszaru informacji niejawnych, zawierający:
   - oprogramowanie identyfikujące sprzęt i użytkownika,
   - elektroniczny czytnik kart mikroprocesorowych,
   - szyfrator transmisji.

d) komputer dla systemu WZI zawierający co najmniej:
   - oprogramowanie identyfikujące sprzęt i użytkownika,
   - elektroniczny czytnik kart mikroprocesorowych,

e) mobilny Terminal:
   - Przewoźny (MTP),
   - Noszony (MTN).

f) uproszczone stanowisko dostępowe:
   - komputer klasy PC wyposażony w system operacyjny Windows klasy Professional lub Linux.

Wymagania dla czytnika i kart mikroprocesorowych wynikają z możliwości obsługi tych urządzeń przez BTUU. Minimalną konfigurację stanowiska dostępowego do współpracy z czytnikiem kart mikroprocesorowych oraz wymagania dla czytnika i kart mikroprocesorowych przedstawione są w Centrum Dystrybucji Oprogramowania. Za przygotowanie aktualnych wersji minimalnych konfiguracji: Stanowiska Dostępowego, czytnika kart mikroprocesorowych oraz samych kart odpowiedzialny jest Naczelnik Wydziału właściwego do spraw projektowania systemów TI BŁiI KGP, a za ich publikację odpowiada Naczelnik Wydziału właściwego do spraw utrzymania systemów TI BŁiI KGP.

Dopuszcza się możliwość użytkowania stanowisk dostępowych (stacji roboczych) do systemów przetwarzających informacje niejawne bez wbudowanych szyfratorów pod warunkiem, że będą się one znajdować w certyfikowanej strefie ochronnej, na brzegu której zainstalowany będzie szyfrator zapewniający szyfrowaną transmisję poza strefą. Szczegółowe wymagania w tym zakresie muszą być opisane w dokumentacji bezpieczeństwa systemu, zgodnie z przepisami ochrony informacji niejawnych.

5.1.3 Oprogramowanie użytkowe i antywirusowe stanowisk dostępowych

a) na stanowiskach dostępowych może być zainstalowane oprogramowanie wymagane przez aplikacje policyjnych systemów centralnych zgodne z opisanym w rozdziale „Oprogramowanie", w tym dozwolone pakiety oprogramowania biurowego,
b) stanowiska dostępowe muszą być objęte systemem ochrony antywirusowej,
c) zgodę na instalację innego oprogramowania, niezbędnego dla realizacji zadań służbowych może wydać Dyrektor BŁiI KGP właściwy ds. informatyki Naczelnik wydziału komendy wojewódzkiej (Stołecznej) Policji lub właściwy ds. łączności/informatyki kierownik komórki organizacyjnej szkoły Policji.

5.2 Samodzielne Stanowisko Robocze

Samodzielne Stanowiska Robocze (SSR), będące komputerem stacjonarnym lub przenośnym, służące do lokalnych zastosowań związanych głównie z aplikacjami o zasięgu lokalnym i biurowym mogą być włączone do PSTD i używane, jako Stanowiska Dostępowe po doposażeniu w niezbędne elementy autoryzacyjne oraz gruntownym skanowaniu antywirusowym.

5.2.1 Wymagania techniczno-użytkowe dla SSR

5.2.1.1 Komputer stacjonarny

a) minimalna konfiguracja musi być zgodna z konfiguracją stanowisk dostępowych dopuszczonych do pracy w PSTD. Dopuszcza się stosowanie systemu operacyjnego z rodziny Windows dedykowanego do zastosowań komercyjnych lub równoważny oraz Linux,
b) na samodzielnych stanowiskach roboczych może być zainstalowane oprogramowanie zakupione przez BŁiI KGP, komendę wojewódzką (Stołeczną) Policji lub szkołę Policji oraz oprogramowanie dodatkowe na

nieodpłatnej licencji, pozwalającej na jego używanie przez podległe jednostki Policji.

5.2.1.2 Komputer przenośny

a) konfiguracja komputera musi odpowiadać wymaganiom użytkownika w zakresie realizacji zadań służbowych. Akceptację na daną konfigurację wydaje właściwy ds. informatyki Naczelnik Wydziału jednostki organizacyjnej Policji dysponującej środkami budżetowymi.
b) włączenie przenośnego SSR do sieci PSTD może nastąpić po uzyskaniu zgody Naczelnika Wydziału właściwego ds. łączności/informatyki,
c) na komputerach przenośnych z zastrzeżeniem wskazanym w rozdziale 5.1.3 może być zainstalowane oprogramowanie zakupione przez BŁiI KGP, komendę wojewódzką Policji / Komendę Stołeczną Policji lub szkołę Policji oraz oprogramowanie dodatkowe na nieodpłatnej licencji, pozwalającej na jego używanie przez podległe jednostki Policji.

Komputery klasy PC z wyjmowanymi dyskami (lub inne trwałe media pamięci) pracujące samodzielnie albo w konfiguracji sieciowej, jak również komputery przenośne (np. laptopy lub elektroniczne „notatniki") z zamontowanym twardym dyskiem, uważane będą za media przechowywania w pamięci informacji w takim samym sensie, jak dyskietki lub inne usuwalne media pamięci komputera.

5.3 Sprzęt peryferyjny, urządzenia wielofunkcyjne

5.3.1 Wszelkie pamięci masowe, z wyłączeniem nośników backupu serwerów centralnych i lokalnych oraz macierzy dyskowych, muszą być szyfrowane,

5.3.2 Urządzenia wielofunkcyjne winny być eksploatowane i skonfigurowane, zgodnie z następującymi zaleceniami:

- urządzenia należy instalować w miejscach, zapewniających dostęp wyłącznie osobom upoważnionym, bądź jeżeli nie jest to możliwe, należy zastosować inne środki organizacyjne, techniczne, ograniczające dostęp do urządzenia osobom nieuprawnionym;
- hasło administratora powinno odpowiadać zasadom określonym w rozdziale 8 niniejszego dokumentu, dot. polityki haseł;
- urządzeniom eksploatowanym w sieci, należy przypisywać statyczne adresy IP;
- należy dezaktywować niewykorzystywane porty i protokoły;
- dostęp do książki adresowej, skrzynek pocztowych i logów należy ograniczyć wyłącznie do uprawnionych użytkowników;
- ustawienia urządzenia winny wymuszać uwierzytelnianie użytkowników przy korzystaniu z funkcji skanowania, kopiowania, faksowania, drukowania, z konsoli urządzenia;
- należy zapewnić aktualizację poprawek oprogramowania, tzw. łat bezpieczeństwa, dostarczanych przez producentów urządzeń;
- w urządzeniach eksploatowanych w sieci PSTD funkcja faksowania może być udostępniona, w przypadku zaakceptowania występujących ryzyk;

- zabrania się podłączania urządzeń wielofunkcyjnych, pracujących w sieci PSTD do sieci lokalnych, posiadających punkt styku z siecią Internet i odwrotnie lub jednocześnie do obu sieci

5.4 Sprzęt pozapolicyjny

5.4.1 Użytkowanie sprzętu TI dzierżawionego na potrzeby jednostek organizacyjnych Policji

a) sprzęt TI użytkowany przez jednostki organizacyjne Policji przez czas określony, na podstawie umów najmu, zawieranych z podmiotami zewnętrznymi, musi spełniać wymagania przedstawione w niniejszych „Standardach ...", w zależności od rodzaju i przeznaczenia urządzeń,
b) po wygaśnięciu umowy, przed zwrotem przedmiotu najmu podmiotowi zewnętrznemu, najmowane urządzenia muszą zostać poddane procedurze zapewniającej, że w zależności od rodzaju urządzenia:
   - przywrócono konfigurację urządzenia do stanu fabrycznego,
   - dokonano usunięcia danych znajdujących się na dyskach twardych w sposób uniemożliwiający odzyskanie informacji,
   - dokonano usunięcia danych znajdujących się w pamięciach typu FLASH lub EEPROM w sposób uniemożliwiający odzyskanie informacji,
   - dokonano usunięcia informacji o konfiguracji tych urządzeń w sposób uniemożliwiający odzyskanie informacji.

5.4.2 Użytkowanie prywatnego sprzętu TI w celu wykonywania prac na rzecz Policji

a) używanie prywatnych, usuwalnych nośników danych komputerowych, oprogramowania oraz sprzętu TI (np. komputerów osobistych lub komputerów przenośnych) jest zabronione,
b) w wyjątkowych wypadkach, za wiedzą i pisemną zgodą kierownika jednostki organizacyjnej Policji dopuszcza się użytkowanie prywatnego, należącego do pracownika lub funkcjonariusza Policji, sprzętu komputerowego, przy czym sprzęt, oprogramowanie oraz nośniki danych wprowadzane do jednostek organizacyjnych Policji muszą podlegać kontroli od momentu wprowadzenia do momentu ich wycofania. Użytkowane oprogramowanie musi posiadać licencje zezwalające na wykorzystanie komercyjne lub w administracji publicznej a sprzęt musi spełniać wymagania bezpieczeństwa jak dla SSR. Sprzęt ten nie może być dopuszczony do użytkowania w PSTD,
c) zgodę na wykorzystanie prywatnego sprzętu komputerowego w jednostce organizacyjnej Policji wydaje kierownik jednostki organizacyjnej Policji na podstawie pisemnego wniosku uzasadniającego wyjątkowość takiej potrzeby, po zawarciu stosownej umowy-cywilno prawnej określającej obowiązki stron i określającej tryb wycofania sprzętu z eksploatacji w jednostce policji lub na podstawie decyzji KWP w sprawie wykorzystania sprzętu prywatnego, która uwzględnia aspekty przedstawione w punktach c), d) i e).
d) wycofanie przyjętego do eksploatacji prywatnego sprzętu komputerowego z eksploatacji następuje po ustaniu przyczyn wykorzystywania, za wiedzą kierownika jednostki organizacyjnej Policji, po usunięciu zawartości lub fizycznym zniszczeniu nośnika danych w uzgodnieniu z Naczelnikiem właściwym

ds. łączności/informatyki komendy wojewódzkiej Policji / Komendy Stołecznej Policji, szkoły Policji lub Dyrektorem BŁiI KGP dla komórek organizacyjnych KGP,

e) pod pojęciem „usunięcia zawartości nośnika danych" rozumie się trwałe i skuteczne usunięcie wszystkich danych, w tym też informacji o strukturze nośnika danych.

5.4.3 Użytkowanie sprzętu TI należącego do kontrahenta do wykonywania prac na rzecz Policji

a) używanie sprzętu TI i oprogramowania należącego do kontrahenta, do prac na rzecz Policji, może mieć miejsce w przypadku przetwarzania informacji jawnej, z zachowaniem zasad dających gwarancję bezpieczeństwa danych (przede wszystkim należy zapewnić, że dane utrwalone na nośnikach informacji wchodzących w ukompletowanie urządzeń kontrahenta, zostaną usunięte w sposób uniemożliwiający ich odczytanie),

b) komputery przenośne oraz wymienne nośniki informacji, używane przez kontrahenta do realizacji przedmiotu umowy, powinny być deponowane w siedzibie jednostki organizacyjnej Policji do czasu zakończenia realizacji umowy. Ich ewentualne wynoszenie poza siedzibę jednostki organizacyjnej Policji w trakcie realizacji umowy, może mieć miejsce wyłącznie za zgodą kierownika tej jednostki, po zastosowaniu uzgodnionej przez strony procedury, gwarantującej każdorazowe usunięcie danych utrwalonych na komputerze przenośnym oraz wymiennych nośnikach informacji,

c) dostęp przedstawicieli firm zewnętrznych do systemów policyjnych może odbywać się wyłącznie przy współudziale osoby odpowiedzialnej z Policji,

d) zdalny dostęp przedstawicieli firm zewnętrznych do systemów policyjnych w ramach wdrożenia bądź wsparcia technicznego, może być realizowany w uzasadnionych przypadkach, pod warunkiem zapewnienia pełnej rozliczalności i kontroli tych działań, przy zastosowaniu narzędzi zapewniających wysoki poziom bezpieczeństwa i silne uwierzytelnianie. Warunki takiego dostępu powinny być określone w umowie z wykonawcą a ich realizacja – nadzorowana przez pracowników jednostki organizacyjnej Policji, na rzecz której prace są realizowane.

e) jakiekolwiek odstępstwa od powyższych zasad wymagają każdorazowo zgody Naczelnika Wydziału Utrzymania Systemów Informatycznych BŁiI KGP lub kierownika komórki organizacyjnej jednostki organizacyjnej Policji właściwej do spraw łączności lub informatyki.

Rozdział 6 Wymagania w zakresie oprogramowania.

6.1 Oprogramowanie stanowiska dostępowego

Oprogramowanie instalowane na stanowisku dostępowym służące do uwierzytelnia użytkowników uzyskujących dostęp do niego w oparciu o spersonalizowaną kryptograficzną kartę mikroprocesorową zawierającą dwa komplety danych w postaci klucza prywatnego i certyfikatu, musi gwarantować spełnienie następujących warunków:

- wszystkie niezbędne dane potrzebne do autoryzacji użytkowników stanowiska komputerowego muszą być przechowywane lokalnie na tym stanowisku,

- zarządzanie kontami użytkowników realizuje Administrator Lokalny,
- w danej chwili może być zalogowany w systemie operacyjnym stanowiska dostępowego wyłącznie jeden użytkownik. Funkcjonalność przełączania kont użytkowników dostępna w systemie operacyjnym musi być zablokowana.
- użytkownik musi mieć możliwość zmiany swojego kodu PIN do karty,
- w celu zapewnienia uniwersalności i otwartości oferowanego rozwiązania oprogramowanie realizujące uwierzytelnienie użytkownika w oparciu o kartę musi wyłącznie komunikować się z kartą poprzez interfejs programistyczny PKCS#11 realizowany przez bibliotekę oprogramowania dostarczoną wraz z kartą,
- oprogramowanie musi umożliwiać użytkownikowi korzystanie ze stanowiska dostępowego również za pomocą obecnie posiadanych przez Policję kart CRYPTOTECH MULTI SIGN oraz OBERTUR ID ONE ENCARD.

6.2 Oprogramowanie systemów operacyjnych

Podstawowym systemem operacyjnym, dla Samodzielnych Stanowisk Roboczych i stanowisk dostępowych, jest:

1) oprogramowanie MS Windows PL **lub równoważne**, najnowsze stabilne wersje (z wykluczeniem wersji do tzw. zastosowań domowych).
2) oprogramowanie na licencji typu „freeware", oparte o otwarty kod źródłowy – „Open Source" (najnowsze stabilne wersje):
   - Linux Ubuntu,
   - Linux openSUSE,
   - Linux Fedora,
   - Linux Debian,
   - Linux Mandriva.
3) Oprogramowanie „inne" (komercyjne, kupowane na indywidualne potrzeby wynikające z charakteru realizowanych zadań):
   - Apple Mac OS X Snow Leopard (preinstalowane na komputerach Mac i Macbook), najnowsze stabilne wersje.

6.3 Oprogramowanie biurowe

Do tworzenia dokumentów tekstowych, arkuszy kalkulacyjnych, prezentacji wizualnych, rysunków, formuł i baz danych zaleca się wykorzystywanie na Samodzielnych Stanowiskach Roboczych oraz stanowiskach dostępowych, narzędzi zawartych w darmowych dystrybucjach pakietów OpenOffice/LibreOffice/Lotus Symphony. W uzasadnionych przypadkach dopuszcza się zakup pakietów komercyjnych.

Wykaz standardowych programów obecnie wykorzystywanych w Policji:

1) Edytory tekstowe (format domyślny zapisu danych - „ .doc"):
   - OpenOffice Writer,
   - MS Office Word.
2) Arkusze kalkulacyjne (format domyślny zapisu - „ .xls"):
   - OpenOffice Calc,
   - MS Office Excel.

3) Programy do tworzenia prezentacji (format domyślny zapisu danych - „ .ppt"):
   - OpenOffice Impress,
   - MS Office PowerPoint.
4) Programy do przeglądania dokumentów w formacie „ .pdf":
   - Adobe Reader PL,
   - Foxit Reader.
5) Programy umożliwiające odczyt formatów zapisu danych MS Office:
   - Word Viewer,
   - Excel Viewer,
   - Power Point Viewer,
   - Visio Viewer.

Zalecany wykaz programów **niestandardowych** wykorzystywanych w Policji, z uwagi na szczególne, indywidualne potrzeby:

1) Programy do tworzenia baz danych:
   - MS Access.
2) Programy do OCR (bezpośrednie konwertowanie skanowanych dokumentów na formaty edytowalne):
   - Abbyy Finereader PL.
3) Konwertery i generatory PDF:
   - Bullzip PDF Printer,
   - PDFCreator.

Naczelnik właściwy ds. łączności/informatyki może, w uzasadnionych przypadkach podjąć decyzję o dopuszczeniu, innych niż wymienione powyżej, rodzajów oprogramowania.

6.4 Oprogramowanie internetowe i pocztowe

Wykaz programów **standardowych** wykorzystywanych w Policji:

1) Przeglądarki internetowe:
   - Internet Explorer (obowiązkowy przy stanowiskach dostępowych),
   - Mozilla Firefox (zalecana do przeglądania stron internetowych),
   - Opera.
2) Klienci poczty e-mail:
   - Lotus Notes,
   - MS Outlook Express,
   - MS Outlook,
   - Poczta systemu Windows,
   - Mozilla Thunderbird.

6.5 Oprogramowanie pozostałe

1) Wtyczki i rozszerzenia:
   - Adobe Flash Player,
   - Adobe Shockwave Player,
   - ActiveX,
   - Java.
2) Programy do nagrywania nośników optycznych:

- Nero OEM,
- InfraRecorder.

3) Programy do archiwizacji danych:
   - 7-zip,
   - WinRAR.
4) Oprogramowanie inne niż wymienione w pkt 1-3, dostosowane do szczególnych potrzeb wynikających z charakteru realizowanych zadań, np. oprogramowanie Apple Mac OS X Snow Leopard, stabilne wersje, wspierane przez producenta, preinstalowane na komputerach Mac i Macbook.
5) **Oprogramowanie antywirusowe.** Na Samodzielnych Stanowiskach Roboczych oraz stanowiskach dostępowych powinno być zainstalowane oprogramowanie antywirusowe dystrybuowane centralnie lub zakupione przez jednostki organizacyjne Policji.
6) **Sterowniki i niezbędne oprogramowanie.** Na Samodzielnych Stanowiskach Roboczych oraz stanowiskach dostępowych musi zostać zainstalowane niezbędne oprogramowanie oraz sterowniki.
7) **Oprogramowanie narzędziowe.** Zaleca się administratorom wykorzystywanie oprogramowania do zarządzania środowiskiem stacji roboczych, umożliwiającym zdalne instalowanie poprawek systemowych i aplikacyjnych.

6.6 Niezbędne warunki bezpieczeństwa dla administratora

Administrator musi mieć na uwadze następujące zastrzeżenia:

- fabrycznie stacja robocza dostarczana jest z utworzonym jednym kontem o nazwie "Administrator", dysponującym pełnymi uprawnieniami. Fabrycznie, nie są kreowane żadne dodatkowe konta użytkowników. Wszelkie prawa dostępu do zasobów (plików, urządzeń peryferyjnych, zasobów sieciowych), podobnie jak hasła i konta, ustanawiane są przez administratora, reprezentującego końcowego użytkownika i wynikają wyłącznie z wewnętrznych regulacji obowiązujących dla danego systemu,
- ustawione jest automatyczne kasowanie pliku wymiany podczas procedury wyłączania systemu. Zaleca się niezmienianie tego ustawienia, ze względu na ochronę poufności danych,
- za niedopuszczalne uznaje się manipulowanie przy ustawieniach systemowych dla urządzeń, a w szczególności: portów COM, SCSI, USB i kart sieciowych. Zastrzeżenie to obejmuje również kwestię "ręcznego" (bez używania funkcji: Dodaj/Usuń Programy) dodawania nowych urządzeń do listy zasobów systemowych,

Rozdział 7 Zasady korzystania ze służbowego sprzętu komputerowego

1. Komputery stacjonarne lub przenośne wydawane są w celu usprawnienia realizacji zadań służbowych.
2. Użytkownik zobowiązany jest do ochrony i nieudostępniania informacji przechowywanych na komputerze osobom do tego nieuprawnionym. Komputery wydawane Użytkownikom są

chronione hasłami dostępowymi (bios, konto administratora). Hasła te są znane tylko i wyłącznie uprawnionym funkcjonariuszom oraz pracownikom Policji.

3. Każdy komputer posiada konto użytkownika zabezpieczone hasłem. Hasło to składa się z min. 8 znaków i musi zawierać: duże i małe litery, cyfry lub znaki specjalne. Użytkownik pod żadnym pozorem nie ujawnia nikomu swojego hasła. W przypadku ujawnienia lub podejrzenia ujawnienia hasła Użytkownik bezzwłocznie podejmuje działania mające na celu zmianę hasła (samodzielnie lub z pomocą Administratora systemu).
4. Użytkownik zobowiązany jest zmienić swoje hasło przy pierwszym logowaniu do systemu.
5. Zabrania się wykorzystywania oferowanych przez standardowe oprogramowanie mechanizmów umożliwiających zapamiętywanie haseł.
6. Komputer przypisany do Użytkownika nie może być udostępniony osobie nieuprawnionej.
7. Użytkownik komputera przenośnego zabezpiecza przetwarzane za jego pomocą informacje zapisując je na nośnikach (dysk twardy, pendrive itp.) w postaci zaszyfrowanej z wykorzystaniem specjalizowanego oprogramowania. Zaleca się stosowanie programu „TrueCrypt". Dopuszcza się stosowanie innego oprogramowania rekomendowanego przez komórki właściwe do spraw łączności i informatyki KWP/KSP/WSPol/Szkoły Policji. Wsparcie użytkowników w zakresie posługiwania się tego typu oprogramowaniem winny świadczyć komórki właściwe do spraw łączności i informatyki.
8. Użytkownik nie może dokonywać żadnych zmian w konfiguracji systemu oraz innego oprogramowania mogących mieć wpływ na ich bezpieczeństwo, oraz ingerować w jakikolwiek sposób w komponenty będące częściami składowymi komputera.
9. Użytkownik zobowiązuje się do regularnego zapisywania stanu swojej pracy. Administrator nie ponosi odpowiedzialności za brak zapisu czy też modyfikacji wyników pracy Użytkownika. Pliki starsze, z których Użytkownik już nie korzysta, powinny być regularnie usuwane z dysku twardego lub archiwizowane.
10. Zabrania się Użytkownikowi instalowania programów nieposiadających wykupionej licencji lub wykupionych praw użytkowania (wyjątkiem jest darmowe oprogramowanie dopuszczone do użytku w Policji – instaluje administrator).
11. Niedozwolone jest przechowywanie na dyskach twardych komputera nielegalnych kopii plików zawierających treści, które objęte są prawami autorskimi.
12. Zabronione jest pozostawianie komputera, bez nadzoru, podczas pracy z uruchomionymi programami/aplikacjami. Wymagane jest co najmniej zablokowanie komputera wygaszaczem ekranu z hasłem.
13. Użytkownik zobowiązany jest do korzystania z wygaszacza ekranu z włączona opcją zabezpieczenia hasłem. Hasło nie może być udostępniane nikomu. Hasło składa się z min. 8 znaków i musi zawierać: duże i małe litery, cyfry oraz lub specjalny (jeżeli umożliwia to wygaszacz ekranu). Czas po którym uaktywnia się wygaszacz nie może być dłuższy niż 30 minut.
14. W wyjątkowych, szczególnie uzasadnionych sytuacjach decyzję o dopuszczeniu do pracy w sieci Intranetowej komputera stacjonarnego lub przenośnego, z odblokowanymi uprawnieniami administracyjnymi dla Użytkownika końcowego podejmuje kierownik komórki właściwej do spraw łączności i informatyki lub jego zastępca.

15. Wyżej wymienione zasady i wytyczne nie dotyczą sprzętu komputerowego wykorzystywanego jako rzeczowy środek pracy operacyjnej, zgodnie z § 169-172 Zarządzenia Nr pf-634 KGP z 30 czerwca 2006 r.
16. Wymienione zasady korzystania ze służbowego sprzętu komputerowego powinny się znajdować na odwrocie formularza wykorzystywanego do przekazywania sprzętu użytkownikom. W uzasadnionych przypadkach dopuszcza się inny sposób zapoznawania użytkowników z powyższymi zasadami korzystania ze służbowego sprzętu komputerowego.

Rozdział 8 Ogólna polityka haseł.

Poniższa polityka nie ma zastosowania w przypadku logowania się do systemów operacyjnych, baz danych, aplikacji i innych z wykorzystaniem kart mikroprocesorowych zawierających unikalne klucze i certyfikaty.

1. Ogólna polityka haseł dotyczy przypadków, gdy nie obowiązują w tym zakresie inne polityki lub wymagania prawne.
2. Ogólna polityka haseł służy zapewnieniu bezpieczeństwa informacjom, przetwarzanym za pomocą sprzętu komputerowego.
3. Ogólna polityka haseł jest stosowana na wszystkich możliwych poziomach sprzętu i oprogramowania (BIOS; systemy operacyjne; bazy danych; aplikacje; urządzenia sieciowe).
4. Administratorzy, którym powierzono nowe urządzenia i oprogramowanie, dostarczone przez firmy zewnętrzne, w ramach prac rozwojowych dot. systemów teleinformatycznych Policji, mają obowiązek:
    - przy pierwszym uruchomieniu urządzenia bądź oprogramowania w środowisku produkcyjnym, zmienić wszelkie domyślne hasła, w tym tzw. hasła fabryczne, dostarczone/zaimplementowane przez dostawców – firmy zewnętrzne,
    - zdeponować zmienione hasła, zgodnie z zasadami opisanymi w pkt. 8 niniejszego rozdziału.
5. Hasła muszą być trudne do odgadnięcia dla osób postronnych.
6. Długość i stopień skomplikowania haseł muszą być adekwatne do wagi chronionych nimi zasobów informacyjnych (w tym konfiguracji urządzeń).
7. Przyjmuje się następujące minimalne wymagania:

    b.) hasła ochrony BIOS komputerów;
    - hasła powinny mieć długość minimum 8 znaków lub maksymalną na jaką pozwala BIOS;
    - hasło Administratora winno być inne niż zwykłego Użytkownika;
    - hasła przechowuje się w miejscu, które jest zabezpieczone przed dostępem osób trzecich.

    c.) hasła do systemu operacyjnego komputera;

- dla konta administracyjnego systemu hasło powinno zawierać minimum 12 znaków alfanumerycznych w tym litery duże i małe, cyfry lub znaki specjalne (takie jak @#!+-%). Hasło nie może zawierać w sobie imion, dat urodzenia, popularnych nazw własnych. Haseł nie można przechowywać w czytelnej formie w bezpośrednim otoczeniu komputera. Wymagana jest okresowa zmiana haseł. Hasła nie powinny się powtarzać częściej niż jeden raz na pięć zmian.
- dla konta użytkownika systemu hasło powinno zawierać minimum 8 znaków alfanumerycznych w tym litery duże i małe, cyfry lub znaki specjalne (takie jak @#!+-%). Hasło nie może zawierać w sobie imion, dat urodzenia, popularnych nazw własnych. Haseł nie można przechowywać w czytelnej formie w bezpośrednim otoczeniu komputera. Wymaga się zmiany haseł przynajmniej raz na trzy miesiące. Hasła nie powinny się powtarzać częściej niż jeden raz na pięć zmian.

d.) hasła do systemów baz danych;

- tak jak w punkcie b.), dopuszczając pewne ograniczenia, związane z konkretnym środowiskiem.

e.) hasła do aplikacji;

- tak jak w punkcie b.), dopuszczając pewne ograniczenia, związane z konkretnym środowiskiem.

f.) hasła dostępu do konfiguracji innych urządzeń (w tym sieciowych);

- tak jak w punkcie b.) lub maksymalna długość na jaka pozwala urządzenie, dopuszczając pewne ograniczenia, związane z konkretnym środowiskiem.

8. Hasła administracyjne (do kont administracyjnych) powinny być deponowane w zamkniętych i opisanych bezpiecznych kopertach u bezpośrednich przełożonych Administratorów lub w miejscach wskazanych przez nich. Jeżeli to tylko możliwe i uzasadnione każdy Administrator powinien dysponować własnym kontem, chronionym unikalnym hasłem.
9. Zabrania się wykorzystywania oferowanych przez standardowe oprogramowanie mechanizmów umożliwiających zapamiętywanie haseł.
10. Nowe konto powinno być chronione hasłem tymczasowym. Zmiana hasła wymuszana jest przy pierwszym logowaniu. W przypadku braku możliwości wymuszania zmiany hasła Użytkownik obowiązany jest przy pierwszym zalogowaniu zmienić hasło.
11. Każdy Użytkownik (również Administrator) zobowiązany jest do zachowania swojego hasła w tajemnicy i wykorzystywania go w sposób uniemożliwiający jego podejrzenie przez osoby postronne. W przypadku ujawnienia hasła Użytkownik (również Administrator) obowiązany jest do bezzwłocznego podjęcia działań mających na celu zablokowanie konta lub/i zmianę hasła.
12. Administrator, przełożony ani żadna inna osoba nie ma prawa żądać od Użytkownika ujawnienia jego hasła.

Rozdział 9 Ogólne zasady konfiguracji sprzętu komputerowego wykorzystywanego w jednostkach Policji (komputery stacjonarne, komputery przenośne)

Poniższe ogólne zasady konfiguracji sprzętu i oprogramowania dotyczą sprzętu komputerowego przenośnego i stacjonarnego pracujących w innych sieciach niż sieć PSTD oraz dotyczą przypadków, gdy nie obowiązują w tym zakresie inne polityki lub wymagania prawne.

9.1 Konfiguracja BIOS (Setup)

1. Jeżeli BIOS posiada funkcję monitorowania otwarcia obudowy, należy tę funkcję włączyć.
2. Jeżeli BIOS posiada funkcję uaktywnienia hasła na włączenie komputera, należy tę funkcję włączyć.
3. Dostęp do ustawień BIOS'u powinien być zabezpieczony co najmniej 8 znakowym hasłem (jeżeli wersja BIOS'u uniemożliwia zastosowanie 8 lub więcej znakowego hasła, ustawiamy na maksymalną ilość znaków na jakie pozwala nam BIOS). Hasła należy ustawić na wszystkich kontach dostępu do BIOS.
4. Hasło musi zawierać małe i duże litery, cyfry i znaki specjalne (!@#$, itp., jeżeli BIOS to umożliwia).
5. Hasło do BIOS'u Administrator przechowuje w sposób uniemożliwiający jego ujawnienie, w zamkniętej kopercie u swojego przełożonego lub w miejscu przez niego wskazanym.
6. Sekwencję startową w BIOS'ie należy ustawić tak, aby system startował tylko i wyłącznie z lokalnego dysku twardego w celu uniemożliwienia uruchamiania systemu z innego źródła (typu pamięć przenośna, dysk sieciowy, napęd CD/DVD/BR dodatkowy zewn. dysk twardy, bootowalna karta sieciowa).
7. Jakakolwiek konfiguracja i zmiany parametrów w BIOS'ie jest możliwa tylko i wyłącznie przez uprawnionego Administratora, po podaniu hasła zabezpieczającego, chroniącego BIOS komputera.
8. Obudowa komputera powinna zostać fizycznie zabezpieczona (np. poprzez założenie mini-zamka, plomby, naklejanie naklejki, gilosza) w celu wykrycia i uniemożliwienia ewentualnych prób ingerencji. Jej otwarcie powinno być możliwe tylko przez uprawnione osoby.
9. Należy ustawić funkcję automatycznego kasowania pliku wymiany w stan włączony, podczas procedury wyłączania systemu, ze względu na ochronę poufności danych.

9.2 Konfiguracja systemu operacyjnego

W przypadku konieczności instalacji bądź reinstalacji systemu operacyjnego komputera stacjonarnego lub komputera przenośnego wykorzystujących środowisko Microsoft Windows 2000 lub nowsze należy przeprowadzić tę czynność zgodnie z poniższymi wskazówkami:

1. Należy sformatować wszystkie partycje dysku w systemie plików NTFS;
2. Nie należy instalować innych systemów operacyjnych na tym samym komputerze;

3. Jako hasło dostępu do konta Administratora należy wpisać 12 znakowe hasło o odpowiedniej złożoności (małe i duże litery, cyfry lub znaki specjalne !@#$)
4. Hasło Administratora należy zabezpieczyć w zamkniętej kopercie u bezpośredniego przełożonego, osoby wykonującej zadania Administratora lub w miejscu przez niego wskazanym;
5. Zainstalować program antywirusowy z aktualną licencją i dokonać aktualizacji baz antywirusowych. Zainstalować niezbędne sterowniki do komponentów umieszczonych w obudowie komputera. Ponadto należy zainstalować najnowszy Service Pack oraz wszystkie poprawki krytyczne zalecane przez producenta systemu operacyjnego;
6. Po zakończeniu instalacji systemu należy dokonać wyłączenia zbędnych usług (w zależności od konkretnego zastosowania komputera), skonfigurować system pod kątem bezpieczeństwa, optymalizacji i wydajności (w tym ustawienie wygaszacza ekranu chronionego hasłem, maksymalnie do 30 min. bezczynności) oraz dokonać przeglądu dzienników zdarzeń celem wyeliminowania ewentualnych błędów, które w późniejszej pracy mogłyby spowodować niestabilną pracę systemu;
7. Wszelkie instalacje aplikacji wykonuje Administrator systemu;
8. Dla komputerów przenośnych wymagane jest zainstalowanie oprogramowania „TrueCrypt" (lub podobnego rekomendowanego przez komórki właściwe do spraw łączności i informatyki) w celu zapewnienia możliwości zachowania poufności przetwarzanych informacji poprzez ich zapis na nośnikach (dysk twardy, pendrive itp.) w postaci zaszyfrowanej. W przypadku komputerów przenośnych, w których dostępny jest TPM (Trusted Platform Module) oraz jest on w pełni wspierany przez zainstalowany system operacyjny, zaleca się stosowanie szyfrowania zapewnianego przez system operacyjny pod warunkiem używania systemu TPM. Administrator zobowiązany jest do pomocy Użytkownikowi w opanowaniu zasad wykorzystywania programu szyfrującego.
9. Wyjątkowo, w szczególnie uzasadnionych przypadkach (np. komputery wykorzystywane przez Administratorów lokalnych, technicznych oraz programistów), dopuszcza się możliwość użytkowania komputera z wykorzystaniem konta o uprawnieniach zaawansowanych lub administracyjnych, a także instalację więcej niż jednego systemu operacyjnego. Wymagane jest pisemne uzasadnienie zaakceptowane przez kierownika właściwego ds. informatyki lub jego zastępcę w jednostkach organizacyjnych Policji albo Dyrektora BŁiI KGP lub osobę przez niego upoważnioną, w przypadku komórek KGP. Uzasadnienie musi być zawsze dostępne w przypadku przeprowadzanego audytu lub kontroli;
10. Dopuszcza się także rozszerzanie uprawnień kont użytkowników w przypadkach gdy aplikacje niezbędne do realizacji zadań służbowych, nie pracują prawidłowo na standardowych ustawieniach kont użytkowników. Wymagane jest pisemne uzasadnienie zaakceptowane przez kierownika właściwego ds. informatyki lub jego zastępcę w jednostkach organizacyjnych Policji albo Dyrektora BŁiI KGP lub osobę przez niego upoważnioną, w przypadku komórek KGP. Uzasadnienie musi być zawsze dostępne w przypadku przeprowadzanego audytu lub kontroli;

9.3 Konfiguracja mechanizmów zabezpieczeń

9.3.1 Zasady haseł

1. Maksymalny okres ważności hasła – 90 dni;
2. Minimalny okres ważności hasła – 1 dzień;
3. Minimalna długość hasła – 8 znaków;
4. Wymuszaj tworzenie historii haseł – 5 haseł;
5. Hasło musi spełniać wymagania co do złożoności – włączony:

9.3.2 Zasady blokowania konta

1. Czas trwania blokady konta – 30 min;
2. Próg blokady konta – 5 nieudane próby;
3. Wyzeruj licznik blokady konta po – 30 minutach;

9.3.3 Zasady prowadzenia inspekcji

Przeprowadź inspekcję	Ustawienie		Opis
	Sukces	Porażka	
zdarzeń logowania na kontach	*TAK*	*TAK*	Lokalnie lub zdalnie. Przy logowaniu do domeny
zarządzania kontami	*TAK*	*TAK*	Tworzenie, zmiana, usunięcie konta użytkownika lub grupy, zmiana nazwy, włączenie/wyłączenie konta użytkownika i zmiana hasła.
Dostępu do usługi katalogowej	*NIE*	*NIE*	Nie ma wpływu na nic w stacjach roboczych i member Server
zdarzeń logowania	*TAK*	*TAK*	Logowanie lokalne lub połączenie sieciowe. Zdarzenie rejestrowane jest na komputerze, z którego zalogował się Użytkownik w zależności, jeśli jest używane konto lokalnie czy domeny
dostępu do obiektów	*NIE*	*TAK*	Dostęp do plików, katalogów, drukarek
zmian zasad	*TAK*	*TAK*	Zmiany na prawa Użytkownika lub polityka audytu lub opcje zabezpieczeń użytkownika (opcje hasła)
użycia uprawnień	*NIE*	*TAK*	Działania Użytkownika, prawa Użytkownika (zmiana czasu, Administrator przejmuje uprawnienia)
śledzenia procesów	*NIE*	*NIE*	Śledzenie programu aktywacji
zdarzeń systemowych	*TAK*	*TAK*	Zamykanie lub restart dla stacji komputerowych lokalnych

9.3.4 Ustawienia dzienników zdarzeń

Ustawienia Dziennika Zdarzeń	Wartość Ustawiona
Maksymalny rozmiar dziennika aplikacji	*10240KB*

Maksymalny rozmiar dziennika bezpieczeństwa	***10240KB***
Maksymalny rozmiar dziennika systemowego	***10240KB***
Zachowaj dziennik aplikacji	***90 dni***
Zachowaj dziennik bezpieczeństwa	***90 dni***
Zachowaj dziennik systemowy	***90 dni***

9.3.5 Przypisywanie praw Użytkownikom

Prawa Użytkownika	Stacje robocze Windows	Opis
Uzyskiwanie dostępu do tego komputera z sieci	Administratorzy, Użytkownicy	Zmiana ustawień domyślnych: usunąć grupy: Wszyscy, Operatorzy kopii zapasowych i Użytkownicy zaawansowani. W pewnych środowiskach pracy może być odpowiednie nie przyznanie dopuszczenia Administratorom dostępu do sieci w celu wyeliminowania możliwości ataku na hasło, które posłużyłoby do logowania osobie znającej hasło administratora z pozycji Administrator.
Pomijanie sprawdzania przebiegu	Administratorzy, Użytkownicy	Zmiany: usunąć grupy: Wszyscy, Operatorzy kopii zapasowych i Użytkownicy zaawansowani.
Zmiana czasu systemowego	Administrator	Zmiany: usunąć grupy: Użytkownicy zaawansowani.
Logowanie lokalne	Administratorzy, Użytkownicy	Zmiany: Usuń grupy: Gość, Operatorzy kopii zapasowych, Użytkownicy zaawansowani.
Usuwanie komputera ze stacji dokującej	Administratorzy, Użytkownicy	Zmiany: Usunąć grupę: Użytkownicy.
Zamykanie systemu	Administratorzy, Użytkownicy	Zmiany: Usunąć grupy: Operatorzy kopii zapasowych. Użytkownicy Zaawansowani.

Rozdział 10 Zadania Lokalnych Administratorów

Zadania lokalnych administratorów wykonują policjanci oraz pracownicy komórek łączności i informatyki.

Jeżeli sytuacja tego wymaga, kierownik jednostki lub komórki organizacyjnej Policji może podjąć decyzję o powierzeniu niektórych zadań realizowanych przez administratorów lokalnych, pracownikom zatrudnionym w tej komórce lub jednostce organizacyjnej Policji. Zakres zadań, które mogą być powierzone tym policjantom lub pracownikom Policji jest następujący:

1. Monitorowanie sieci i reagowanie na wszelkie niebezpieczeństwa mogące zagrażać poprawnym działaniu systemów/oprogramowania.
2. Zarządzanie siecią PSTD w ramach sieci wewnątrzwojewódzkiej lub sieci lokalnej, danej komórki organizacyjnej Policji (zgodnie z zakresem przyznanych uprawnień).
3. Ustanawianie wszelkich praw dostępu do zasobów plików, zgodnie z regulacjami obowiązującymi dla danego systemu.

4. Definiowanie i konfigurowanie stacji lokalnych.
5. Weryfikacja legalności oraz aktualizacja zainstalowanego oprogramowania.
6. Szkolenie policjantów i pracowników komórki organizacyjnej jednostki Policji w zakresie użytkowania posiadanych stanowisk dostępowych oraz SSR.
7. Nadzór nad prawidłową obsługą urządzeń teleinformatycznych, w tym diagnostyka i nadzór, przez użytkowników końcowych i współpraca z komórkami ds. łączności i informatyki w usuwaniu awarii.
8. Wykonywanie podłączeń i konfiguracji sprzętu informatycznego użytkowników końcowych do urządzeń peryferyjnych
9. Wymiana tuszy i tonerów w urządzeniach drukujących.
10. Wymiana uszkodzonych peryferii komputerowych.
11. Wykonywanie zestawień zawierających dane sprzętu teleinformatycznego użytkowanego w biurze/jednostce uwzględniające wersję programu antywirusowego, adresu IP, lokalizacji i sprzętu, haseł dostępowych, nr inwentarzowych i seryjnych urządzenia oraz danych użytkowników.

Zadania administratorów lokalnych, w odniesieniu do systemów teleinformatycznych, w których są przetwarzane informacje niejawne, są uregulowane w dokumentacji bezpieczeństwa tych systemów.

Rozdział 11 Wymagania w zakresie dokumentacji systemu teleinformatycznego

Wraz z systemami teleinformatycznymi, budowanymi na potrzeby jednostek organizacyjnych Policji, powinna być dostarczana dokumentacja, umożliwiająca ich poprawne użytkowanie i administrowanie a także dalszy rozwój i modyfikacje, w tym takie rodzaje dokumentacji, jak:

I. **Dokumentacja Systemowa**, obejmująca m.in.:

- opis otoczenia systemu;
- opis wymagań funkcjonalnych i niefunkcjonalnych systemu;
- opis architektury systemu w podziale na komponenty/moduły;
- opis modelu logicznego i fizycznego systemu;
- opis relacji pomiędzy komponentami/modułami systemu oraz powiązań z innymi systemami;
- specyfikacje przypadków użycia komponentów/modułów systemu.

II. **Dokumentacja Techniczna**, obejmująca m.in.:

- opis wykonanych instalacji technicznych;
- opis struktur danych;

- opis zainstalowanego sprzętu i oprogramowania wraz z informacjami o parametrach i sposobie konfiguracji;
- instrukcje obsługi sprzętu i oprogramowania, dostarczane standardowo przez wykonawcę, wraz z informacjami o warunkach licencjonowania;
- materiały szkoleniowe i podręczniki w zakresie dotyczącym administracji i użytkowania systemu;
- opis struktury i mechanizmów funkcjonowania wszystkich interfejsów systemu;
- kod źródłowy oprogramowania z objaśnieniami/komentarzem (jeżeli wytworzono, bądź zmodyfikowano oprogramowanie dedykowane na potrzeby systemu).

III. **Dokumentacja Eksploatacyjna (procedury utrzymaniowe i awaryjne), obejmująca** m.in.:

- procedury związane z administracją i eksploatacją systemu, w tym procedury działania administratorów systemu oraz procedury działania użytkowników systemu;
- procedury o charakterze testowym;
- procedury konserwacji systemów;
- procedury awaryjne.

IV. **Dokumentacja Bezpieczeństwa Systemu** (dokumentacja zgodna z wymaganiami ustaw: o ochronie informacji niejawnych bądź/i o ochronie danych osobowych, obligatoryjnie - jeżeli system przetwarza informacje niejawne bądź/i dane osobowe).

Szczegółowy zakres dokumentacji powinna determinować architektura systemu teleinformatycznego oraz wymagania prawa (w przypadku dokumentacji, o której mowa w pkt. IV). Jakość i kompletność dokumentacji należy zweryfikować w trakcie odbioru systemu.

Rozdział 12 Procedura aktualizacji dokumentu

W związku z koniecznością okresowego dostosowywania niniejszych zaleceń do zmian, zachodzących w obszarze technologii teleinformatycznych, wprowadza się następującą procedurę aktualizacji dokumentu:

1. O wprowadzenie zmian do dokumentu, może wnioskować:
   - Naczelnik wydziału w BŁiI KGP,
   - Naczelnik właściwy ds. łączności/informatyki, Komendy Wojewódzkiej Policji / Komendy Stołecznej Policji / Szkoły Policji,
   - Kierownik komórki organizacyjnej Policji, za pośrednictwem właściwego Naczelnika ds. łączności/informatyki KGP/KWP/KSP/Szkoły Policji.
2. Wnioski o wprowadzenie zmian w dokumencie wraz z uzasadnieniem, należy kierować do Dyrektora BŁiI KGP.
3. W przypadku uznania merytorycznych przesłanek, uzasadniających wprowadzenie zmiany, Dyrektor BŁiI KGP występuje do właściwego Zastępcy Komendanta Głównego Policji, o zatwierdzenie zmian w dokumencie.

DYREKTOR
BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI
insp. Jerzy SIPA