

ZATWIERDZAM

KOMENDANT GŁÓWNY POLICJI
z powołania
ZASTĘPCA
KOMENDANTA GŁÓWNEGO POLICJI
nadinsp. Roman KUSTER

dj - 2466 / 2024

**WYMAGANIA
DOTYCZĄCE STANDARDÓW TECHNICZNYCH,
UŻYTKOWYCH ORAZ BEZPIECZEŃSTWA, STOSOWANYCH W POLICJI,
W ZAKRESIE INFORMATYKI I ŁĄCZNOŚCI**

KWIECIEŃ 2024

Matryca odpowiedzialności:

	Jednostki organizacyjne Policji	Komórki organizacyjne KGP	Biuro Łączności i Informatyki KGP	Komendant Główny Policji
Odpowiedzialny za dokument (R)			X	
Zatwierdzający dokument (A)				X
Merytorycznie konsultowany (C)	X	X		
Informowany (I)	X	X		

Opis dokumentu

Nazwa dokumentu	Wymagania dotyczące standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie informatyki i łączności
Wersja	2
Data ostatniej modyfikacji	2024-04-03
Autor dokumentu	Biuro Łączności i Informatyki Komendy Głównej Policji
Status dokumentu (projekt, zatwierdzony)	Zatwierdzony
Liczba stron	98

Wymagane podpisy:

Imię i nazwisko	Rola/stanowisko	Podpis	Data
insp. Przemysław Więclaw	Dyrektor Biura Łączności i Informatyki KGP		04.04.2024
ml. insp. dr Krzysztof Tomaszewski	Naczelnik Wydziału Zarządzania Projektami BLiI KGP		04.04.2024
ml. insp. Adam Bogucki	Naczelnik Wydziału Ochrony Systemów Informatycznych BLiI KGP		3.04.2024
ml. insp. Tadeusz Antonowicz	Naczelnik Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych BLiI KGP		4.04.2024
nadkom. Sylwia Brzyska	p.o. Naczelnik Wydziału Utrzymania Systemów Informatycznych Międzynarodowych BLiI KGP		04.04.24
nadkom. Zbigniew Królikowski	Naczelnik Wydziału Utrzymania Systemów Telekomunikacyjnych BLiI KGP		17.04.2024
ml. insp. Dariusz Żabicki	Naczelnik Wydziału Technicznego Wsparcia Systemu Powiadamiania Ratunkowego BLiI KGP		17.04.2024
nadkom. Tomasz Mendoń	Naczelnik Wydziału Radiokomunikacji BLiI KGP		17.04.2024
kom. Agnieszka Cybulska	Naczelnik Wydziału Obsługi Końcowego Użytkownika BLiI KGP		17.04.2024
ml. insp. Grażyna Ryszkowska	Naczelnik Wydziału Wsparcia Programistycznego BLiI KGP		4.04.24
asp. szt. Marcin Tęgos	Naczelnik Wydziału Cyberbezpieczeństwa BLiI KGP		18.04.24

SPIS TREŚCI

ROZDZIAŁ 1	POSTANOWIENIA WSTĘPNE	5
1.1	CELE I ZAKRES DOKUMENTU	5
1.2	AKTY PRAWNE OBOWIĄZUJĄCE W ZAKRESIE PRZEDMIOTOWYM OBJĘTYM DOKUMENTEM	5
1.3	TERMINOLOGIA PRZYJĘTA W DOKUMENCIE	5
ROZDZIAŁ 2	OGÓLNE ZASADY I STANDARDY	13
2.1	NORMY I MIĘDZYNARODOWE STANDARDY	14
2.2	POLSKIE NORMY	16
ROZDZIAŁ 3	WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA	18
3.1	WYMAGANIA W ZAKRESIE WYPOSAŻENIA CENTRÓW PRZETWARZANIA DANYCH (PCPD – PODSTAWOWEGO CENTRUM PRZETWARZANIA DANYCH, ZCPD – ZAPASOWEGO CENTRUM PRZETWARZANIA DANYCH ORAZ RCPD – REGIONALNYCH CENTRÓW PRZETWARZANIA DANYCH)	18
3.2	POSTĘPOWANIE Z INFORMATYCZNYMI NOŚNIKAMI DANYCH NIEZAWIERAJĄCYMI INFORMACJI NIEJAWNYCH	18
3.3	ELEMENTY BEZPIECZEŃSTWA SIECI TELEINFORMATYCZNEJ	18
3.4	ŚRODKI OCHRONY KRYPTOGRAFICZNEJ	21
3.5	MECHANIZMY OCHRONY KORESPONDENCJI GŁOSOWEJ	22
3.6	ORGANIZACJA DOSTĘPU DO INTERNETU	24
3.7	ZASILANIE ELEKTROENERGETYCZNE	25
ROZDZIAŁ 4	WYMAGANIA DOTYCZĄCE PROJEKTOWANIA, IMPLEMENTACJI I WDRAŻANIA	33
4.1	SIECI TELEINFORMATYCZNE	33
4.2	OKABŁOWANIE STRUKTURALNE	36
4.3	SYSTEMY OPERACYJNE, PROTOKOŁY I SYSTEMY ZARZĄDZANIA BAZAMI DANYCH	38
4.4	POSTĘPOWANIE Z DANymi – ZARZĄDZANIE POJEMNOŚCIĄ	40
4.5	SYSTEMY TELETRANSMISYJNE	40
4.6	SYSTEMY ŁĄCZNOŚCI TELEFONICZNEJ	44
4.7	SYSTEMY RADIOKOMUNIKACYJNE	49
4.8	TERMINALE MOBILNE	72
4.9	INNE SYSTEMY	75
ROZDZIAŁ 5	WYMAGANIA DOTYCZĄCE UŻYTKOWANIA	80
5.1	STANOWISKA DOSTĘPOWE SIECI PSTD	80
5.2	SAMODZIELNE STANOWISKO ROBOCZE	82
5.3	SPRZĘT PERYFERYJNY, URZĄDZENIA WIELOFUNKCYJNE	83
5.4	SPRZĘT POZAPOLICYJNY	84
ROZDZIAŁ 6	WYMAGANIA W ZAKRESIE OPROGRAMOWANIA STANOWISK DOSTĘPOWYCH	85

6.1	OPROGRAMOWANIE STANOWISKA DOSTĘPOWEGO.....	85
6.2	OPROGRAMOWANIE SYSTEMÓW OPERACYJNYCH.....	86
6.3	OPROGRAMOWANIE BIURÓWE.....	86
6.4	OPROGRAMOWANIE INTERNETOWE I POCZTOWE.....	87
6.5	OPROGRAMOWANIE POZOSTAŁE.....	87
ROZDZIAŁ 7 GENERALNE ZASADY KORZYSTANIA ZE SŁUŻBOWEGO SPRZĘTU		
	KOMPUTEROWEGO.....	88
ROZDZIAŁ 8 OGÓLNA POLITYKA HASEŁ.....		90
ROZDZIAŁ 9 OGÓLNE ZASADY KONFIGURACJI SPRZĘTU KOMPUTEROWEGO		
WYKORZYSTYWANEGO W JEDNOSTKACH POLICJI (KOMPUTERY STACJONARNE, KOMPUTERY		
PRZENOŚNE, SPRZĘT TYPU NAS (NETWORK ATTACHED STORAGE).....		92
9.1	KONFIGURACJA BIOS/UEFI (SETUP).....	92
9.2	KONFIGURACJA SYSTEMU OPERACYJNEGO.....	93
9.3	KONFIGURACJA MECHANIZMÓW ZABEZPIECZEŃ.....	94
9.4	KONFIGURACJA SPRZĘTU TYPU NAS (NETWORK ATTACHE STORAGE).....	95
ROZDZIAŁ 10 ZADANIA LOKALNYCH ADMINISTRATORÓW.....		96
ROZDZIAŁ 11 WYMAGANIA W ZAKRESIE DOKUMENTACJI SYSTEMU		
TELEINFORMATYCZNEGO.....		97
ROZDZIAŁ 12 WPROWADZANIE ZMIAN DO DOKUMENTU.....		98

Rozdział 1 Postanowienia wstępne

1.1 Cele i zakres dokumentu

Niniejszy dokument ustanawia wymagania w zakresie planowania, projektowania, wdrażania, użytkowania oraz bezpieczeństwa systemów łączności i informatyki w Policji. Wymagania te winny być stosowane w jednostkach organizacyjnych Policji, w celu stworzenia warunków do zapewnienia interoperacyjności, spójności, integralności oraz efektywności rozwiązań w obszarach łączności i informatyki.

W przypadku, gdy obecnie użytkowane komponenty systemów łączności i informatyki nie spełniają wymagań określonych w niniejszym dokumencie, należy zaplanować i podjąć działania prowadzące do zapewnienia zgodności. Tempo tych działań należy dostosować do możliwości finansowych i organizacyjnych jednostek Policji.

Za wdrożenie i przestrzeganie wymagań określonych w niniejszym dokumencie odpowiadają kierownicy jednostek organizacyjnych Policji.

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) AAA (<i>Authentication, Authorization and Accounting</i>) | Uwierzytelnianie, Autoryzacja, Rozliczalność. |
| 2) 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. |

- 3) **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.
- 4) **AGA (*Air-Ground-Air*)** łączność radiowa z obiektami latającymi w relacji ziemia-powietrze i powietrze-ziemia.
- 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) **API (*Application Programming Interface*)** interfejs programistyczny aplikacji, rozumiany jako zestaw reguł i opisów wzajemnej komunikacji oprogramowania.
- 8) **APN (*Access Point Name*)** dedykowany punkt dostępu do sieci operatora GSM, umożliwiający transmisję danych.
- 9) **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.
- 10) **Autoryzacja** proces, w którym sprawdzane jest czy dany podmiot (o ustalonej własnie tożsamości) ma prawo dostępu do żądanych zasobów.
- 11) **Bezpieczeństwo danych** zbiór zagadnień z dziedziny teleinformatyki 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) **BLiI KGP** Biuro Łączności i Informatyki Komendy Głównej Policji.
- 14) **BS** (*Basic Station*) stacja bazowa, urządzenie wyposażone w antenę, łączące terminal ruchomy z częścią stałą cyfrowej sieci telekomunikacyjnej.
- 15) **BTUU** Bezpieczny Tryb Uwierzytelniania Użytkownika - centralny policyjny system autoryzacji i uwierzytelniania, specjalizowane oprogramowanie uprawniające zidentyfikowanych użytkowników do dostępu do zasobów informacyjnych Systemów BLiI.
- 16) **CDO** Centrum Dystrybucji Oprogramowania, usługa dostępna w sieci PSTD zawierająca produkty: instrukcje, oprogramowanie, zarządzenia, formularze i informacje wykorzystywane do pracy z systemami teleinformatycznymi Policji.
- 17) **CLIP** (*Calling Line Identification Presentation*) identyfikacja numeru (identyfikatora) abonenta wywołującego.
- 18) **CSD** Centralny System Dostępowy - system dla potrzeb platformy lokalizacyjno-informacyjnej z Centralną Bazą Danych oraz dostępu do innych systemów oraz zasobów zewnętrznych.
- 19) **CWI** Centralny Węzeł Internetowy - wydzielony w BLiI KGP technicznie i organizacyjnie punkt dostarczania usług internetowych dla KGP z możliwością dostarczania takich usług dla innych jednostek organizacyjnych Policji.
- 20) **DMO** (*Direct Mode Operation*) funkcjonalność standardu TETRA, dająca możliwość nawiązania łączności terminal-terminal bez pośrednictwa sieci, czyli w trybie bezpośrednim.
- 21) **DMR** (*Digital Mobile Radio*) otwarty standard cyfrowej łączności radiowej opracowany przez ETSI wykorzystujący wielodostęp z podziałem czasowym TDMA (Time Division Multiple Access).
- 22) **Dostępność** właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot upoważniony do pracy w systemie teleinformatycznym.

- | | |
|---|---|
| 23) EDACS (<i>Enhanced Digital Access Communication System</i>) | system trunkingowy, umożliwiający cyfrową transmisję danych oraz cyfrową lub analogową transmisję sygnałów mowy w kanale radiowym. |
| 24) FCAPS (<i>Fault, Configuration, Accounting, Performance, Security</i>) | część modelu zarządzania siecią telekomunikacyjną, określająca kategorie: usterki, konfiguracja, różniczenia, wydajność, bezpieczeństwo. |
| 25) GDOI (<i>Group Domain Of Interpretation</i>) | protokół zarządzania kluczami, odpowiedzialny za ustanawianie wspólnej polityki bezpieczeństwa (IPsec SA) pomiędzy routerami będącymi członkami tej samej "zaufanej" grupy. |
| 26) GET VPN (<i>Group Encrypted Transport</i>) | zbiór protokołów służących implementacji bezpiecznych, szyfrowanych połączeń typu tunel-less VPN. |
| 27) GUI (<i>Graphical User Interface</i>) | graficzny interfejs użytkownika, określenie sposobu prezentacji informacji przez komputer oraz interakcji z użytkownikiem |
| 28) Informatyczny nośnik danych | materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej (np. pendrive, dysk twardy, dysk przenośny oraz płyty CD/DVD, pamięć masowa, taśma magnetyczna lub inne nośniki oraz repozytoria danych). |
| 29) Integralność | właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony. |
| 30) IPsec (<i>Internet Protocol Security</i>) | 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) ISSI (<i>Individual Short Subscriber Identity</i>) | indywidualny identyfikator użytkownika w systemie TETRA. |
| 32) KGP | Komenda Główna Policji. |
| 33) KSP | Komenda Stołeczna Policji. |
| 34) KWP | Komenda Wojewódzka Policji. |

- | | |
|--|---|
| 35) MOS (<i>Mean Opinion Score</i>) | subiektywny współczynnik jakości dźwięku używany w telefonii, zwłaszcza w telefonii VoIP. MOS podawany jest w skali od 1 do 5 (1 – zła, 5 – znakomita). |
| 36) MPLS | technologia w sieci operatorskiej OST 112 z zaimplementowanymi mechanizmami technologii Multi-Protocol Label Switching. |
| 37) MTN | Mobilny Terminal Noszony – komputer przenośny komunikujący się z systemami teleinformatycznymi dostępnymi poprzez sieć PSTD z wykorzystaniem bezprzewodowej transmisji danych. |
| 38) MTP | Mobilny Terminal Przewoźny – komputer zainstalowany w pojeździe, komunikujący się z systemami teleinformatycznymi dostępnymi poprzez sieć PSTD z wykorzystaniem bezprzewodowej transmisji danych. |
| 39) NAC (<i>Network Access Control</i>) | kontrola dostępu do sieci. |
| 40) NAS (<i>Network Attached Storage</i>) | urządzenie sieciowe umożliwiające podłączenie zasobów pamięci dyskowych bezpośrednio do sieci komputerowej. |
| 41) Napięcie gwarantowane | napięcie zasilające gwarantujące parametry zgodnie z normami/zaleceniami dla sprzętu teleinformatycznego. |
| 42) 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. |
| 43) OTAR (<i>Over the Air Rekeying</i>) | usługa zdalnej aktualizacji kluczy maskujących poprzez interfejs radiowy w systemie TETRA. |
| 44) PEL | Punkt Elektryczno-Logiczny min. 4xRJ45 i min. 4x230V. |
| 45) Poczta Elektroniczna | Usługa realizowana w oparciu o infrastrukturę teleinformatyczną Policji, z wykorzystaniem protokołów komunikacyjnych SMTP, POP3/IMAP i innych, umożliwiających wymianę wiadomości tekstowych i multimedialnych w formie elektronicznej. |
| 46) Polifax-A i Polifax-Z | podsieci przeznaczone do transmisji telekopiowej jawnej. |

- | | |
|--|--|
| 47) Poufność | właściwość określająca, że informacja nie jest ujawniania podmiotom do tego nieuprawnionym. |
| 48) PPU | Policyjna Platforma Usługowa - narzędzie wymiany danych pomiędzy systemami za pośrednictwem usług sieciowych (ang. web services). |
| 49) PSTD (Policyjna Sieć Transmisji Danych) | wirtualna sieć prywatna VPN, działająca na bazie wydzielonej sieci szkieletowej OST 112 w technologii IP MPLS z zaimplementowaną kryptografią, umożliwiającą łączenie sieci LAN na obszarze całego kraju w jedną sieć korporacyjną i zapewniającą użytkownikom policyjnym bezpieczny dostęp do centralnych systemów informatycznych Policji. |
| 50) PSTN (Public Switched Telephone Network) | publiczna komutowana sieć telefoniczna. |
| 51) RADIUS (Remote Authentication Dial In User Service) | protokół opisany w RFC2865 dotyczący uwierzytelniania, autoryzacji oraz informacji o jego konfiguracji. |
| 52) 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.). |
| 53) Router CE (Customer Edge) | router kliencki sieci operatorskiej MPLS. |
| 54) Router PE (Provider Edge) | router brzegowy w sieci operatorskiej MPLS. |
| 55) Rozliczalność | właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi. |
| 56) SDS (Short Data Service) | usługa krótkich wiadomości tekstowych. |
| 57) Sieć TI (teleinformatyczna) | element składowy Systemu TI Policji zapewniający transport danych w sposób automatyczny. |
| 58) SMDB | System Mobilnego Dostępu do Baz Danych. |
| 59) SSR | Samodzielne Stanowisko Robocze – stanowisko komputerowe, które nie jest Stanowiskiem Dostępowym (komputer stacjonarny/komputer przenośny). |

- | | |
|---|---|
| 60) Stanowisko Dostępowe | stanowisko komputerowe, podłączone do sieci TI w celu dostępu do centralnych zasobów informatycznych Systemów TI BELI. |
| 61) SULTelP | System Utajnionej Łączności Telekopiowej Policji funkcjonujący w oparciu o podsieć komutowaną przeznaczony do szyfrowanej transmisji telekopiowej. |
| 62) SwMI (<i>Switching and Management Infrastructure</i>) | elementy infrastruktury systemu TETRA odpowiedzialne za zarządzanie i komutację. |
| 63) SWWN | System Wykrywania Włamań i Napadów. |
| 64) System TI (<i>teleinformatyczny</i>) | w myśl ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 Nr 144 poz. 1204) 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. z 2018 r. poz. 1954 i 2245). |
| 65) TACACS (<i>Terminal Access Controller Access Control System</i>) | protokół opisany w RFC1492. Jest to protokół uwierzytelnienia, autoryzacji i rozliczenia [AAA - Authentication, Authorization and Accounting], który realizuje kontrolę dostępu dla routerów, przełączników, punktów dostępowych, czy sieciowych serwerów dostępu. |
| 66) TDM (<i>Time Division Multiplexing</i>) | multipleksowanie sygnału z podziałem czasu transmisji. |
| 67) TETRA (<i>Terrestrial Trunked Radio</i>) | otwarty standard cyfrowej radiotelefonicznej łączności trunkingowej, powstały z przeznaczeniem zwłaszcza dla służb bezpieczeństwa publicznego i ratownictwa, stworzony przez Europejski Instytut Norm Telekomunikacyjnych (ETSI). |
| 68) TI | teleinformatyczny |
| 69) TMO (<i>Trunking Mode Operation</i>) | tryb pracy trunkingowej systemu TETRA. |
| 70) Urządzenie wielofunkcyjne | urządzenie z funkcjami skanowania, kopiowania, faksowania oraz drukowania, wyposażone w kartę |

- sieciową, wysyłające i odbierające dane za pośrednictwem sieci telekomunikacyjnej.
- 71) **Uwierzytelnianie** proces polegający na weryfikacji zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych.
- 72) **VHF (*Very High Frequency*)** fale ultrakrótkie, zakres fal radiowych o częstotliwości 30 MHz-300 MHz (10 m - 1 m).
- 73) **VLAN (*Virtual Local Area Network*)** Wirtualna Sieć Lokalna – lokalna sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.
- 74) **VLSM (*Variable Length Subnet Mask*)** maski podsieci o zmiennej długości umożliwiające podział adresu (np.: klasy A, B, C) na kilka mniejszych podsieci zawierających różne liczby hostów.
- 75) **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.
- 76) **WFS (*Współczynnik Fali Stożącej*)** stosunek wartości amplitudy maksymalnej do amplitudy minimalnej napięcia elektrycznego fali stojącej w linii zasilającej odbiornik, określa stopień dopasowania obciążenia do linii zasilającej.
- 77) **Zalecenia (rekomendacje) ITU-T** zalecenia (rekomendacje) dla sektora rynku telekomunikacyjnego wydawane przez Sektor Normalizacji Telekomunikacji Międzynarodowego Związku Telekomunikacyjnego.
- 78) **Zasilanie bezprzerwowe** zasilanie pozwalające osiągnąć parametry napięcia gwarantowanego bez względu na zaniki zasilania podstawowego.
- 79) **Zasilanie podstawowe** zasilanie z publicznej sieci elektroenergetycznej.
- 80) **Zasilanie rezerwowe** zasilanie z baterii akumulatorów i/lub zespołu spalinowo-elektrycznego.
- 81) **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.

Rozdział 2. Ogólne zasady i standardy

Prowadzenie projektów teleinformatycznych i telekomunikacyjnych w Policji regulują odrębne przepisy¹. Za generalną zasadę przyjmuje się uzgadnianie wszelkich inicjowanych projektów z zakresu TI, z Biurem Łączności i Informatyki KGP, celem zapewnienia kompletności i kompatybilności wdrażanych rozwiązań z rozwiązaniami już funkcjonującymi bądź planowanymi do realizacji.

Policyjne systemy TI muszą zapewniać bezpieczeństwo informacjom w nich przetwarzanych, w stopniu adekwatnym do oszacowanego poziomu ryzyka. Realizacji powyższego mają służyć następujące działania i zasady:

- 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 należy stosować Polskie Normy, 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 przetwarzające 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. Dla systemów informatycznych przetwarzających dane osobowe, musi być opracowana polityka bezpieczeństwa oraz instrukcja zarządzania systemem, a także winni być wyznaczeni przeszkoleni administratorzy, ponoszący odpowiedzialność za utrzymanie danego systemu.

¹ Zarządzenie nr 5 Komendanta Głównego Policji z dnia 16 lutego 2017 r. w sprawie metod realizacji projektów teleinformatycznych i telekomunikacyjnych w Policji (Dz. Urz. KGP poz. 11, z 2018 r. poz. 107 oraz z 2019 r. poz. 19 i 94 z późn. zm.)

2.1 Normy i międzynarodowe standardy

Jednolite kryteria oceny bezpieczeństwa Systemów TI zapewnia stosowanie międzynarodowych standardów. Do najważniejszych dokumentów o znaczeniu międzynarodowym należą²:

2.1.1 w zakresie technologii informatycznych oraz kompatybilności elektromagnetycznej:

- 1) **PN-ISO/IEC 15408: 2016-10** - Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych:

Część 1 - Wprowadzenie i model ogólny,

Część 2 – Komponenty funkcjonalne zabezpieczeń,

Część 3 - Komponenty uzasadnienia zaufania do zabezpieczeń.

- 2) **dyrektywa Parlamentu Europejskiego i Rady 2014/30/UE** z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej (wersja przekształcona) (*Dz. Urz. UE L 96/77 z 29.3.2014*).
- 3) **dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE** z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (*Dz. Urz. UE L 153/62 z 22.5.2014*).
- 4) **rozporządzenie Parlamentu Europejskiego i Rady (WE) 174/2013** z dnia 5 lutego 2013 r. zmieniające rozporządzenie (WE) nr 106/2008 w sprawie wspólnotowego programu znakowania efektywności energetycznej urządzeń biurowych (*Dz. Urz. UE L 63/I z 6.3.2013*).

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:

² W dokumencie przywołano normy i standardy oraz ich wersje, dostępne w dniu wprowadzenia niniejszych wytycznych w życie. W dłuższej perspektywie czasowej należy uwzględnić aktualne wersje norm i standardów oraz nowe normy i standardy, stanowiące w obszarach objętych wymaganiami.

- **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.
- **ETSI EN 300 392 -xxx** Zestaw Norm zharmonizowanych dla standardu TETRA
- **ETSI EN 300 396 -xxx** Zestaw Norm zharmonizowanych dla standardu TETRA – DMO

- ETSI TR 102 398 V1.4.1 DMR General System Design (2018-11)
- ETSI TS 102 361-1 Part 1: DMR Air Interface (AI) protocol V2.5.1 (2017-10)
- ETSI TS 102 361-2 Part 2: DMR voice and generic services V2.4.1 (2017-10)
- ETSI TS 102 361-3 Part 3: DMR data protocol V1.3.1 (2017-10)
- ETSI TS 102 361-4 Part 4: DMR trunking protocol V1.9.2 (2018-04)

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 standardów ISO/IEC z zakresu bezpieczeństwa, należą ustanowione normy:

- 1) PN-ISO/IEC 2382-8:2001 - Technika informatyczna - Terminologia - Bezpieczeństwo.
- 2) PN-I-13335-1:1999 - Technika informatyczna - wytyczne do zarządzania bezpieczeństwem systemów informatycznych - pojęcia i modele bezpieczeństwa systemów informatycznych.
- 3) PN-ISO/IEC 27001 - Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania.
- 4) PN-ISO/IEC 27002 - Technika informatyczna - Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji.
- 5) PN-ISO/IEC 27005 - Technika informatyczna - Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.
- 6) PN-ISO/IEC 20000 - Technika informatyczna - Zarządzanie usługami.
- 7) PN-ISO/IEC 22301 – Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania.
- 8) PN-EN 60950-23:2007 - Urządzenia techniki informatycznej - Bezpieczeństwo użytkowania - Część 23: Wielkogabarytowe urządzenia do magazynowania danych.

- 9) **PN-EN-1047-2:2019** - Pomieszczenia i urządzenia do przechowywania wartości-
Klasyfikacja i metody badań odporności ogniowej - Część 2: Pomieszczenia oraz pojemniki
do przechowywania nośników informacji.
- 10) **PN-EN 60950-22:2017** - Urządzenia techniki informatycznej - Bezpieczeństwo użytkowania
- Część 22: Urządzenia instalowane na zewnątrz.
- 11) **PN-EN 60950:2002** - Bezpieczeństwo urządzeń techniki informatycznej.
- 12) **PN-EN 62368-1:2015-03** - Urządzenia techniki fonicznej/wizyjnej, informatycznej
i telekomunikacyjnej. Część 1 - Wymagania bezpieczeństwa.

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

3.1 Wymagania 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 jakiegokolwiek 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. kąt. 6;
- g) Wymaga się stosowanie rozwiązań, ograniczających zjawisko tzw. ulotu elektromagnetycznego (emisji ujawniającej).

3.2 Postępowanie z informatycznymi nośnikami danych niezawierającymi informacji niejawnych

- a) służbowe informatyczne nośniki danych, na których zapisane zostały informacje służbowe lub informacje służbowe zawierające dane osobowe, muszą być przechowywane i wykorzystywane w sposób uniemożliwiający dostęp osobom nieuprawnionym do zapisanych na nośniku danych, poprzez zabezpieczenie ich algorytmem szyfrującym (należy stosować odpowiednio wymagania określone w Rozdziale 7 pkt 6) oraz dostęp fizyczny do nośnika, na którym dane te zostały zapisane.
- b) użytkownik końcowy jest odpowiedzialny za wydane mu elektroniczne nośniki danych. Nadzoruje ich sposób przechowywania a także inicjuje proces wymiany nośników i ich kwalifikacji do utylizacji.
- c) utylizacja oraz nadzór nad elektronicznymi nośnikami danych musi odbywać się zgodnie z:
 - przepisami w sprawie szczegółowego sposobu gospodarowania składnikami rzeczowymi majątku ruchomego Skarbu Państwa,
 - procedurami przyjętymi w jednostce organizacyjnej Policji.
- d) czynność niszczenia/utylizacji nośników należy udokumentować.

3.3 Elementy bezpieczeństwa sieci teleinformatycznej

- 3.3.1 Podstawowym zadaniem systemu bezpieczeństwa jest zapewnienie poufności, integralności, dostępności informacji przetwarzanych w systemie TI a także

rozliczalności, autentyczności i niezawodności w dostępie do tych informacji. W tym celu należy zapewnić funkcjonowanie w warstwie sieciowej takich rozwiązań jak:

- stosowanie technologii VPN z kryptografią, zapewniających akceptowany poziom bezpieczeństwa przesyłania danych w różnych środowiskach WAN,
- stosowanie co najmniej dwóch podstawowych typów systemów zaporowych: działające w warstwie aplikacji oraz w warstwie sieciowej modelu ISO OSI RM (ISO Open Systems Interconnection Reference Model).

oraz zapewnić realizację następujących zasad:

- 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 specyfiki i zawartości informacyjnej systemu (systemy jawne, systemy w których przetwarzane są dane osobowe, systemy niejawne),
- wszystkie centralne systemy teleinformatyczne dołączone do sieci PSTD muszą korzystać z systemu BTUU, jako podstawowego mechanizmu kontroli dostępu użytkowników. W uzasadnionych przypadkach Dyrektor BLiI 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.

3.3.2 Cele systemu bezpieczeństwa:

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

3.3.3 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 BLiI 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.
- 3.3.4** Zachowanie poufności danych przesyłanych w sieci poprzez wykorzystanie protokołów np. IPsec, GDOI, SSL/TLS, SSH, SNMP (auth, priv).
- 3.3.5** Wykorzystanie certyfikowanego systemu szyfrowania dla zachowania poufności, integralności i autentyczności informacji niejawnych.
- 3.3.6** Udostępnianie zasobów poprzez podsieć PSTD dla odbiorców zewnętrznych powinno następować w jednym punkcie, którego ochronę stanowi system SMDB.
- 3.3.7** System, 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.
- 3.3.8** 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) kontrolę ruchu HTTPS,
 - e) wydajną translację adresów (NAT, PAT),
 - f) chronić przed atakiem fragmentacji pakietów IP,
 - g) współpracę z serwerami uwierzytelniania, filtrowania adresów URL itp.,
 - h) możliwość blokowania apletów Javy oraz ActiveX,
 - i) gromadzenie informacji o dokonanych połączeniach,
 - j) implementację transmisji z użyciem standardu IPsec lub min. TLS 1.2.
- 3.3.9** Architektura systemu firewall musi być redundantna i implementowana w oparciu o wielopoziomowe (co najmniej trójstopniowe) systemy zabezpieczeń, w których muszą być szeregowo połączone urządzenia różnych producentów.
- 3.3.10** W celu uwierzytelniania i autoryzacji zdalnych użytkowników w sieci wymaga się, tam gdzie jest to możliwe, stosowanie standardowego protokołu HTTPS.
- 3.3.11** W celu monitorowania zagrożeń i zdarzeń w ruchu sieciowym, należy stosować systemy wykrywania i ochrony przed włamaniami typu IPS/IDS (Intrusion Prevention System/Intrusion Detection System).
- 3.3.12** 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 uwierzytelniania, autoryzacji, rozliczalności (AAA-Authentication, Authorization and Accounting),
 - Stosowanie bezpiecznych protokołów komunikacji administracyjnej: SSH, TSL,

- Stosowanie dedykowanych fizycznych portów do zarządzania urządzeniami, typu out-of-band, z wykorzystaniem dedykowanej infrastruktury połączeń do realizacji administracji urządzeniami,
- c) 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. Uwierzytelnianie sesji administracyjnej może być realizowane poprzez zewnętrzny serwer Tacacs+/Radius, który dodatkowo może współpracować z serwerem obsługującym hasła jednokrotne (one-time-passwords).

3.4 Środki ochrony kryptograficznej

PSTD jest wirtualną siecią prywatną L3 VPN, działającą na bazie wydzielonej sieci szkieletowej OST 112, w której przetwarzane są głównie informacje jawne niebędące jednak informacją publiczną oraz podlegające regulacjom prawnym w zakresie ochrony danych osobowych. W ramach istniejącej sieci policyjnej wydzielono i zabezpieczono kryptograficznie pojedyncze podsieci z systemami służącymi do przetwarzania informacji niejawnych, urządzeniami certyfikowanymi odpowiednio przez ABW lub SKW.

3.4.1 Standardem w zapewnieniu poufności i bezpieczeństwa przesyłanych danych w sieciach VPN MPLS w ramach sieci WAN/OST 112 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) w sieciach VPN MPLS OST 112 lub SSL/TLS dla przesyłania informacji jawnych.

3.4.2 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.

3.4.3 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), listy CRL.

3.5 Mechanizmy ochrony korespondencji głosowej

3.5.1 Bezpieczeństwo korespondencji w systemach łączności radiowej

3.5.1.1 Bezpieczeństwo korespondencji w systemie TETRA

- a) System musi zapewniać pracę w klasach bezpieczeństwa SC1, SC2, SC3 (z i bez kluczy GCK).
- b) W klasach SC2 i SC3 (z i bez kluczy GCK) maskowany w interfejsie radiowym musi być cały ruch radiowy z sygnalizacją i adresowaniem włącznie.
- c) Maskowanie korespondencji musi być realizowane w interfejsie radiowym za pomocą zmiennych nw. kluczy szyfrujących:
 - Wspólny klucz szyfrujący - CCK;
 - Grupowy klucz szyfrujący - GCK;
 - Pochodny klucz szyfrujący - DCK;
 - Statyczny klucz szyfrujący - SCK;
- d) System musi umożliwiać pracę w klasie bezpieczeństwa SC1 niezależnie od pracy z klasami SC2 lub SC3 (z i bez kluczy GCK).
- e) W klasie bezpieczeństwa SC1 i SC2 system musi zapewniać przynajmniej uwierzytelnianie terminala przez system, przy czym funkcjonalność ta musi mieć charakter opcjonalny, zależny od bieżących potrzeb konfiguracyjnych.
- f) BS w trybie trunkingu lokalnego musi umożliwiać przynajmniej maskowanie korespondencji kluczem SCK, gdy możliwość maskowania korespondencji kluczem DCK jest niedostępna.
- g) System musi zapewniać uwierzytelnianie terminali przy rejestracji do systemu, zmianie BS i wyjściu BS z trunkingu lokalnego, w którym uwierzytelnianie nie było dostępne.
- h) W klasie bezpieczeństwa SC3 (z i bez kluczy GCK) system musi realizować procedury autoryzacji terminali poprzez uwierzytelnienie inicjowane przez SwMI. System musi także umożliwiać uwierzytelnienie SwMI na żądanie terminala.
- i) System musi umożliwiać stosowanie maskowania korespondencji E2E w relacjach terminal - terminal, oraz terminal - konsola dyspozytorska za pomocą klucza o długości 256 bitów (AES256). Wymaganie to nie może ograniczać pracy terminali bez funkcji szyfrowania E2E.
- j) System musi realizować maskowanie korespondencji radiowej z wykorzystaniem algorytmu TEA2.
- k) W zakresie zarządzania kluczami:
 - System musi być wyposażony w centrum dystrybucji kluczy maskujących,
 - System musi być wyposażony w centrum zarządzania kluczami do celów uwierzytelniania,
 - Każda z Agencji musi mieć możliwość techniczną generowania i zarządzania własnymi kluczami GCK;

- Bazy danych przechowujące klucze służące do uwierzytelniania i maskowania interfejsu radiowego muszą być zaszyfrowane z wykorzystaniem narzędzi odpornych na próby włamania i uniemożliwiających dostęp osób nieuprawnionych.
- System musi zapewniać dynamiczną zmianę kluczy maskujących SCK, CCK i GCK drogą radiową (OTAR) oraz umożliwiać przekazywanie drogą radiową danych potrzebnych do wygenerowania klucza DCK.

3.5.1.2 Bezpieczeństwo korespondencji w systemie DMR

Wdrażane rozwiązania muszą zapewniać maskowanie korespondencji głosowej algorytmem ARC4 o długości klucza 40 bitów, kodek głosu AMBE+2.

3.5.2 Telefonía IP

Wymagania techniczno-użytkowe, w systemach łączności IP:

- a) CallProcessor – system sterujący połączeniami telefonicznymi;
- b) Brama głosowa – styk sieci VoIP z innymi systemami teleinformatycznymi z pomocą technologii ISDN;
- c) Session Border Controller – styk sieci VoIP z innymi systemami telefonicznymi opartymi o technologie VoIP;
- d) Gatekeeper – urządzenie sterujące połączeniami telefonicznymi, zapewniające między innymi call admission controll, translację adresów itp.
- e) Urządzenia końcowe – aparaty telefoniczne, aparaty video, aplikacje
- f) Sieć IP – transport dla pakietów rozmównych,
- g) Protokoły sygnalizacyjne:
 - H.323
 - MGCP,
 - SIP,
 - SCCP
- h) Protokoły transmisji danych:
 - RTP (Real-Time Transport Protocol),
 - RTCP (Real-Time Transport Control Protocol)
 - cRTP, Compresses IP/UDP/RTP,
 - SRTP.
- i) Kodeki i pasmo:
 - G.711 (bandwidth 64 kb/s, sample size 240, packets 33),
 - G.729 ((bandwidth 8kb/s, sample size 40, packets 25),
- j) W zakresie sieci lokalnej – kodek VOIP G.722 oraz G.711.

3.6 Organizacja dostępu do Internetu

- 3.6.1** Dostęp do sieci INTERNET w jednostkach organizacyjnych Policji, powinien być realizowany z wykorzystaniem kanałów VRF (Virtual Routing and Forwarding) sieci OST 112, za pośrednictwem CWI KGP/CSD sieci OST 112.
- 3.6.2** Zabrania się łączenia do wewnętrznych sieci Policji, SSR pracujących jednocześnie w sieci INTERNET.
- 3.6.3** 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, szyfrotora dysków twardych oraz klienta IPsec VPN.
- 3.6.4** Jeżeli dostęp do sieci Internet nie odbywa się za pośrednictwem kanałów VRF sieci OST 112, to węzeł dostępu do sieci INTERNET musi składać się z: routera brzegowego, firewalla, serwera DNS, serwera PROXY lub specjalizowanych urządzeń zawierających wszystkie te funkcjonalności nie wykluczając także systemów IPS/IDS. Poniżej zamieszczono wymagania dla urządzeń typu router brzegowy oraz firewall, wchodzących w skład Węzła Dostępu do sieci INTERNET:
- a) router brzegowy – konfiguracja sprzętowa i programowa powinna pozwalać na wstępną kontrolę i odrzucanie ruchu niepożądanego (funkcja screening router),
 - b) firewall powinien zapewniać co najmniej:
 - mechanizmy zabezpieczeń: kontrole poprawności transmisji na poziomie konkretnych protokołów ruchu wchodzącego i wychodzącego, z funkcjami blokowania ataków typu DoS (Denial of Service/) i DDoS (Distributed Denial of Service),
 - filtrowanie treści: (JAVA/ActiveX), URL,
 - funkcję NAT,
 - współpracę z systemami uwierzytelniania,
 - możliwość współpracy z systemami antywirusowymi,
 - współpracę z systemami ochrony przed włamaniami typu IPS,
 - tworzenie sieci VPN.
- 3.6.5** Wymaga się, aby węzeł dostępowy znakował wiadomości typu SPAM i posiadał oprogramowanie antywirusowe skanujące ruch przychodzący i wychodzący dla wiadomości pocztowych.
- 3.6.6** W newralgicznych punktach węzła wymaga się stosowanie sond typu IPS.
- 3.6.7** Podstawowe usługi udostępniane przez węzeł internetowy: firmowa/wewnętrzna poczta elektroniczna, www, ftp, połączenia Site-to-Site VPN,
- 3.6.8** Oprogramowanie użytkowe:
- a) przeglądarka internetowa: Internet Explorer, Microsoft Edge, Google Chrome, Firefox, Opera,
 - b) klienci poczty wskazani w punkcie 6.4.

- c) bezpieczni klienci FTP, z obsługą połączeń SSL: Total Commander lub inny posiadający wsparcie dla połączeń szyfrowanych, np. FileZilla,
- d) oprogramowanie antywirusowe z możliwością centralnego zarządzania, lub zarządzane lokalnie, zakupione niezależnie przez komórki organizacyjne Policji (po uzyskaniu uprzednio akceptacji Dyrektora BLiI KGP),
- e) centralnie zarządzane oprogramowanie zabezpieczające do stacji roboczych oraz komputerów przenośnych typu „Firewall” np. Symantec, Checkpoint, Dr Web McAfee, Outpost, itp., przy czym konfiguracja personalnego Firewall’a musi umożliwiać administratorom systemu diagnozowanie połączenia sieciowego na stacjach roboczych np. poprzez polecenie ping i zapewniać możliwość aktualizowania oprogramowania antywirusowego.

3.6.9 Zabrania się w szczególności:

- a) podłączania stanowisk komputerowych 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 i komputerów przenośnych, bez zgody administratora sieci.

3.6.10 Należy okresowo (nie rzadziej niż raz w miesiącu) zapewnić aktualizację tzw. krytycznych poprawek systemu operacyjnego (jeżeli są udostępniane przez producenta).

3.7 Zasilanie elektroenergetyczne

3.7.1 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.

3.7.1.1 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 lub bezprzerwowym, na poziomie pozostałych komisariatów Policji,
- wymaga 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.

3.7.1.2 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 w zakresie krytycznych systemów i stanowisk pracy (stanowisko kierowania, kontrola dostępu, monitoring wizyjny) dedykowanej dla infrastruktury sieci LAN,
- systemów telewizji przemysłowej CCTV,
- kontroli dostępu,
- systemów rozgłoszeniowych.

3.7.1.3 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.

3.7.1.4 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, wymaga się stosowanie zasilaczy UPS lub siłowni telekomunikacyjnych małej mocy.

3.7.2 Zasilanie węzłów TI

Przy projektowaniu podstawowych parametrów siłowni telekomunikacyjnych wymaga się 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 $n + 1$.

3.7.2.1 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 24 godzin,
- e) baterie bezobsługowe, o żywotności zgodnie z normą EUROBAT 12,
- f) czas rezerwy baterijnej 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.

3.7.2.2 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:
 - wymaga się stosowanie akumulatorów w technologii VRLA:
 - o o żywotności min. 10 lat (UPSy >20kVA),
 - o o żywotności min. 6 lat (UPSy <20kVA),
 - o 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 Parlamentu Europejskiego i Rady 2008/103/WE z dnia 19 listopada 2008 r. zmieniającej dyrektywę 2006/66/WE w sprawie baterii i akumulatorów oraz zużytych baterii i

akumulatorów w odniesieniu do wprowadzania baterii i akumulatorów do obrotu (Dz. Urz. UE L 327/7 z 5.12.2008).

- 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) wymaga 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.

3.7.2.3 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) wymagania dot. siłowni telekomunikacyjnych 48V DC:
 - 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,
 - aktywny podział prądu obciążenia zespołów prostownikowych,
 - zarządzanie energią pobieraną przez zespoły prostownikowe,
 - układ pomiaru prądu zbiorczego baterii 1, baterii 2 i odbiorów,
 - układ ładowania dozoru baterii,
 - czujnik temperatury baterii do kompensacji napięcia buforowania,
 - czujnik temperatury w pomieszczeniu technicznym,
 - pole dystrybucji DC: zabezpieczenia typu „S” i (lub) NH00,
 - 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) wymagania dot. siłowni inwertorowych 230V AC:
 - 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 baterijnym $\geq 91\%$,
 - 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,
 - 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. 12 lat,
 - praca przy napięciu buforu regulowanym w zależności od temperatury w pomieszczeniu baterii,
 - montaż na stojaku.

3.7.2.4 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,
 - prądnicą synchroniczną, samowzbudną, bezszczotkową, posiadającą automatyczny, elektroniczny regulator napięcia prądnicy, zapewniający stabilność napięcia $\pm 0,5$ % 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 \geq 91,5%, 150 kVA \geq 92,2%, 250 kVA \geq 92,4%, 400kVA \geq 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.

3.7.3 Monitoring urządzeń:

- a) w pomieszczeniach całodobowej służby dyżurnej jednostek Policji należy montować wizualno-akustyczne panele sygnalizacyjne informujące o aktualnym stanie urządzeń zasilających (UPS, siłownie, 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 wymaga się wyposażać w przyłącze dla agregatu przewoźnego,
- e) wymaga się przeprowadzanie okresowych testów potwierdzających sprawność urządzeń zasilających.

3.7.4 Zasilanie urządzeń radiotelefonicznych

3.7.4.1 Zasilanie stacjonarnych obiektów infrastruktury TETRA

- 1) Urządzenia Systemu muszą zostać zaprojektowane i wykonane z uwzględnieniem przepisów bezpieczeństwa użytkowania, ograniczenia zaburzeń radioelektrycznych oraz ochrony środowiska.
- 2) Użyte określenia:
 - Zasilanie podstawowe - zasilanie z sieci elektroenergetycznej niskiego napięcia 230/400V AC 50 HZ;

- Zasilanie dwustronne - zasilanie dwiema liniami niskiego napięcia z dwóch niezależnych stacji transformatorowych;
 - Zasilanie jednostronne - zasilanie z jednej linii niskiego napięcia;
 - Zasilanie rezerwowe - zasilanie z baterii akumulatorów lub spalinowego agregatu prądotwórczego lub ogniw paliwowych;
 - Czas rezerwy baterijnej - czas, w ciągu którego baterie akumulatorów mogą zasilać urządzenia przy maksymalnym poborze prądu i zachowaniem dolnej dopuszczalnej wartości napięcia rozładowania baterii;
- 3) Odnosnie warunków zasilania urządzeń infrastruktury przyjęto następujące wymagania:
- Czas zasilania ze źródła rezerwowego określony w niniejszych wymaganiach jest czasem minimalnym;
 - Pojemność baterii akumulatorów musi być dobrana z uwzględnieniem zasilania wszystkich urządzeń wymagających rezerwowania;
 - Obiekty, których dotyczą niniejsze wymagania powinny być wyposażone w przyłącza do przewoźnego zespołu agregatu prądotwórczego;
 - Moc zespołu agregatu prądotwórczego (lub ogniw paliwowego) musi być wystarczająca do zasilania wszystkich urządzeń wymagających rezerwowania;
 - Zanik / powrót napięcia lub zmiana źródła zasilania nie mogą przerywać lub zakłócać działania zasilanych urządzeń;
 - Obiekty, zależnie od ich rodzaju i wymaganego czasu zasilania ze źródła rezerwowego, muszą być zasilane w sposób określony w poniższej tabeli.
- 4) Wymagana dokumentacja dostarczonych urządzeń zasilania:
- Deklaracje zgodności, potwierdzające spełnienie wymagań zasadniczych w zakresie bezpieczeństwa użytkowania w związku z dyrektywą 2014/35/UE oraz w zakresie kompatybilności elektromagnetycznej w związku z dyrektywą 2014/30/UE;
 - Aktualne pomiary elektryczne, potwierdzone protokołem i wykonane przez uprawnioną osobę, zastosowanych urządzeń i instalacji zasilającej urządzenia (od tablicy głównej zasilania do urządzeń, w tym zasilania rezerwowego).
- 5) Ponadto w pomieszczeniu musi być dostępna tablica główna zasilania (TGZ) a obwody zasilania zabezpieczone wyłącznikiem nadprądowym typu „S” o parametrach wynikających z projektu technicznego. Dedykowany obwód BS musi być zakończony złączem umożliwiającym podłączenie BS oraz zasilania rezerwowego. Obwód zasilania BS musi zawierać elementy ochrony przepięciowej I i II stopnia. W pomieszczeniu gdzie wykonana będzie instalacja BS musi być dostępna listwa wyrównania potencjałów.
- 6) Ogólne wymagania dotyczące zasilania obiektów:

Lp.	Rodzaj obiektu	Zasilanie	
		podstawowe	rezerwowe (rodzaj zasilania, czas rezerwy)
1	węzły komutacji i sterowania, centra zarządzania, utrzymania i monitorowania sieci: krajowe, rezerwowe krajowe i wojewódzkie	dwustronne	stacjonarny agregat prądotwórczy (72h) oraz bateryjne (2h) lub ogniwa paliwowe (2h)
2	BS klasy B	jednostronne	Opcja 1 możliwość podłączenia agregatu przewoźnego oraz zasilanie bateryjne (12h) lub ogniwa paliwowe (12h)

Lp.	Rodzaj obiektu	Zasilanie	
		podstawowe	rezerwowe (rodzaj zasilania, czas rezerwy)
			Opcja 2 stacjonarny agregat prądotwórczy (48h) wraz z UPS zapewniającym bezprzerwowe przełączenie zasilania
3	BS klasy C	jednostronne	Opcja 1 możliwość podłączenia agregatu przewoźnego oraz zasilanie bateryjne (18h) lub ogniwa paliwowe (18h) Opcja 2 stacjonarny agregat prądotwórczy (48h) wraz z UPS zapewniającym bezprzerwowe przełączenie zasilania
4	BS klasy D	jednostronne	Opcja 1 możliwość podłączenia agregatu przewoźnego oraz zasilanie bateryjne (24h) lub ogniwa paliwowe (24h) Opcja 2 stacjonarny agregat prądotwórczy (48h) wraz z UPS zapewniającym bezprzerwowe przełączenie zasilania

- 7) Wymagania dotyczące zasilania poszczególnych typów urządzeń abonenckich zostały opisane w rozdziale „Wymagania dla sprzętu abonenckiego”.
- 8) Wszystkie elementy aktywne wchodzące w skład SwMI, przesył teletransmisyjnych oraz innych modułów Systemu istotnych ze względu na ciągłość działania oraz poziom świadczonych usług muszą być dołączone do obwodów gwarantowanego, bezprzerwowego zasilania.

3.7.4.2 Zasilanie stacjonarnych obiektów infrastruktury pozostałych systemów radiokomunikacyjnych Policji

3.7.4.2.1 Radiotelefon bazowy, stacja retransmisyjna:

- zasilanie sieciowe 230V \pm 10%, 50 Hz,
- zasilanie rezerwowe zespołu nadawczo-odbiorczego z akumulatora 12V lub 24V zapewniające czas pracy nie mniej niż 8 godzin przy proporcjach nadawanie/odbior/nasłuch równych 10%/10%/80% i mocy nadajnika dla stacji bazowej i retransmisyjnej 25W,
- dla wydzielonego manipulatora operatorskiego wymagane jest także zasilanie rezerwowe z akumulatora 12V, zapewniającego czas pracy nie mniejszy niż 8 godzin przy proporcjach nasłuch/odbior równych 90%/10% i mocy m.cz. 3W.

3.7.4.2.2 Radiotelefony przewoźne:

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

3.7.4.2.3 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 $\pm 10\%$ 50 Hz ma zapewnić:
 - o ładowanie akumulatorów z sygnalizacją cyklu pracy,
- ładowarka wielopozycyjna z funkcją regeneracji zasilana z sieci 230V $\pm 10\%$ 50 Hz ma zapewnić:
 - o ładowanie akumulatorów z sygnalizacją cyklu pracy oraz funkcję wstępnego rozładowania,
 - o regenerację akumulatorów,
 - o określenie pojemności akumulatorów,
 - o każdą z ww. funkcji ma być realizowana przez wszystkie stanowiska ładowarki.

3.7.4.3 Łączność satelitarna

Telefony satelitarne muszą posiadać możliwość:

- a) zasilania z sieci energetycznej 230V $\pm 10\%$ 50 Hz,
- b) zasilania prądem stałym o napięciu 13,2V ($\pm 20\%$) 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

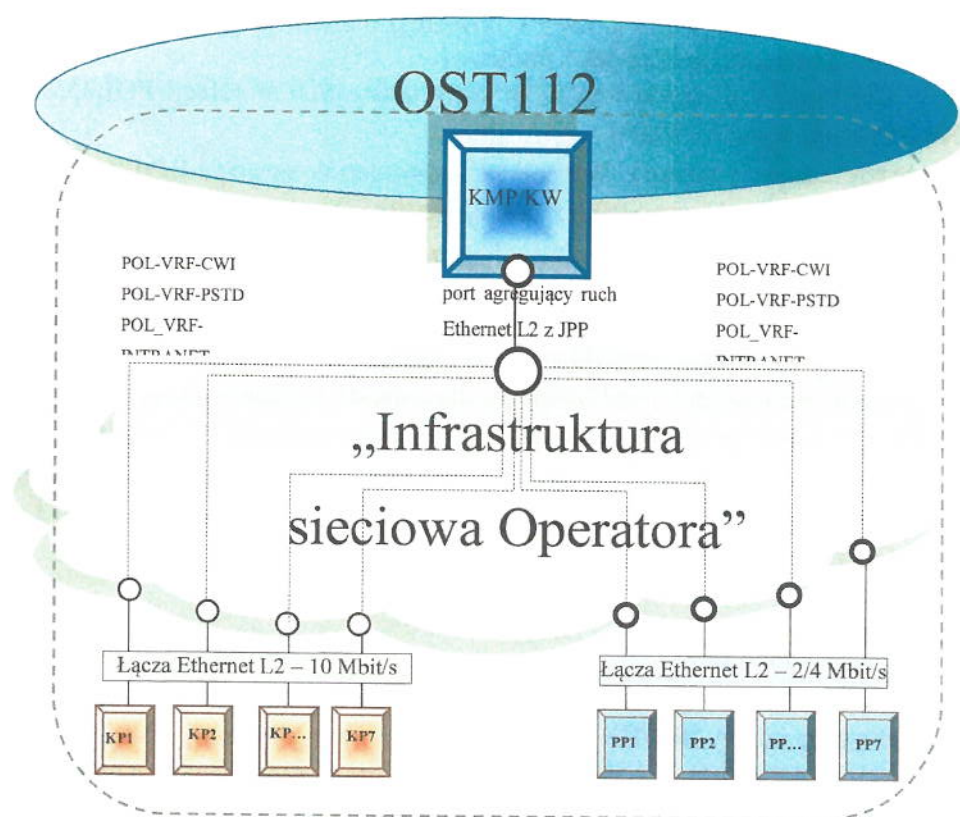
- a) Biuro Łączności i Informatyki KGP do identyfikacji urządzeń w sieciach teleinformatycznych Policji przyjęło system adresacji oparty na protokole IPv4. Ponadto z puli adresów dostępnych dla klasy A wybrano prywatną (specjalną) przestrzeń adresową zaczynającą się od 10.X.X.X.. W celu efektywnego przydziału jednostkom i komórkom Policji adresów IP dostępnych w puli prywatnej przestrzeni adresowej wymaga 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) lokalnie 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 sieciach teleinformatycznych Policji jest standard ETHERNET: 10/100/1000 Mb full-duplex oraz 10/40 Gb full-duplex z wykorzystaniem kabli miedzianych lub światłowodowych,
- i) skanowania sieci zarządzanych przez służby Policji w obrębie kraju lub BLiI 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 BLiI KGP,
- j) dopuszcza się w Policji metodę budowy sieci teleinformatycznych LAN/MAN/WAN opartej na specjalistycznym oprogramowaniu zainstalowanym na centralnym kontrolerze sieci. Oprogramowanie to pozwala na pełne zarządzanie urządzeniami sieciowymi (np.: routerami i przełącznikami itp.) w zakresie bezpieczeństwa sieci, konfiguracji urządzeń oraz pozwala na automatyzację czynności związanych z administracją i utrzymaniem sieci,
- k) realizacja połączeń sieciowych odbywa się poprzez łącza stałe, radioliniowe oraz usługi prywatnego APN w technologii GPRS/EDGE/3G/HSDPA/LTE/5G, możliwość realizacji dostępu do centralnych systemów Policji oraz dostępu do usług głosowych i wideo sieci OST112 z wykorzystaniem prywatnego APN.
- l) połączenia typu Wi-Fi (łączność bezprzewodowa) muszą być implementowane w oparciu o międzynarodową specyfikację IEEE 802.11i. Sieć Wi-Fi musi dawać gwarancję dostępności tylko i wyłącznie uprawnionym podmiotom oraz zapewniać poufność transmisji danych. Rozwiązanie dopuszcza się jedynie w przypadku korzystania z zewnętrznego dostępu do sieci Internet (z wyłączeniem dostępu realizowanego przez CWI). Zgodę na uruchomienie takiego połączenia, niezbędnego dla realizacji zadań służbowych, może wydać Dyrektor BLiI KGP, właściwy ds. informatyki Naczelnik wydziału Komendy Wojewódzkiej (Stołecznej) Policji lub właściwy ds. łączności/informatyki kierownik komórki organizacyjnej szkoły Policji, na podstawie pisemnego wniosku oraz wyników analizy ryzyka,

- m) dostęp do policyjnych systemów teleinformatycznych z wykorzystaniem technologii GSM może być realizowany, pod warunkiem zapewnienia szyfrowania danych oraz terminowania połączeń przez prywatny APN Policji i SMDB (System Mobilnego Dostępu do Baz Danych), administrowany przez BLiI KGP,
- n) wymianę informacji o routingu pomiędzy routerami w sieci PSTD należy opierać o protokoły dynamiczne IGP.

4.1.1 Podłączenie Jednostek Podstawowych Policji (JPP) do węzłów sieci OST112

1. Do węzłów sieci OST112 powinny zostać podłączone Jednostki Podstawowe Policji (JPP) nie posiadające łączy własnych, a jedynie je dzierżawiące.
2. Realizacja powinna nastąpić poprzez zakup usługi transmisji danych Carrier Ethernet w warstwie drugiej (L2) o przepływnościach:
 - do szczebla komisariatu Policji (KP) 10 Mbit/s;
 - do szczebla posterunku Policji (PP) od 2 do 4 Mbit/s *(w zależności od wielkości jednostki)*.
 - Transmisja z wykorzystaniem Prywatnego APN.
3. Jednostki Podstawowe Policji (POL600) powinny być dołączone do KMP (POL35) lub do KWP (POL20) w zależności od możliwości technicznych Wykonawcy.
4. Sposób podłączenia JPP (POL600) do jednostek szczebla wyższego KMP/KWP (POL35/POL20) i agregacji ruchu obrazuje poniższy rysunek:



Rys. Sposób podłączania jednostek KP i PP (POL600) do KMP/KWP (POL35/20) oraz agregacji ruchu.

5. Priorytetem jest zapewnienie jednostce podstawowej na poziomie KP dostępu do PSTD oraz możliwości komunikacji głosowej w technologii IP. Rekomendowana przepływność z KP do jednostki nadrzędnej KMP/KWP to min. 10 Mbit/s.
Z poziomu jednostki podstawowej szczebla PP konieczne jest zapewnienie przepływności łączy min. 2 Mb/s. W zależności od potrzeb danej jednostki minimalna wymagana przepływność może zostać zwiększona.
6. Jednostki nadrzędne do których będą podłączone KP/PP, zostaną wyposażone w odpowiednie wkładki Ethernet.
7. Wymagana jest obsługa tagowania ramek Ethernet zgodnie z 802.1Q od strony interfejsów GE w węzłach POL35/20, co oznacza, że poszczególne zakończenia łączy Ethernet 10/100/1000 od strony węzłów POL600, odpowiadać będą ściśle określonej i uzgodnionej pomiędzy Wykonawcą i Zamawiającym sieci VLAN na określonym porcie zbierającym.
Oznakowanie ramek Ethernet znacznikami VLAN dla ruchu z węzła POL600 do POL35/20 (*upstream*) oraz zdjęcie znacznika VLAN przed dostarczeniem ramki Ethernet do węzła POL600 (*downstream*) realizowane jest przez Wykonawcę.
Numery sieci VLAN nie mogą się powtarzać na różnych interfejsach agregujących w ramach tego samego węzła POL35/20.
Łącza Ethernet muszą przeźroczyście przenosić ramki Ethernet o wartości MTU minimum 1522 bajtów i VLAN-y o dowolnej numeracji (QinQ). Powinny obsługiwać ruch typu broadcast, unicast jak i multicast.
8. SLA (*Service Level Agreement*) dla łączy cyfrowych w relacji POL35/20 – POL600 (KP/PP) musi wynosić 99,0%.
9. W ramach realizacji zadania, Wykonawca powinien wyposażyć KP/PP w sprzęt sieciowy w postaci routerów dostępowych z funkcją bramy głosowej oraz przełączników 24 lub 48 portowych. (*Ilości urządzeń sieciowych wynikają wprost z potrzeb danej jednostki*).
Zamawiający na dostarczonych urządzeniach, na potrzeby obecnie działających usług głosowych OST112, musi mieć możliwość uruchomienia technologii szyfrowania Cisco GET (*Group Encrypted Transport*) VPN oraz *Virtual Routing and Forwarding* (VRF).
10. Urządzenia sieciowe powinny zostać podłączone do zasilania gwarantowanego w danym KP/PP, umożliwiające pracę w/w urządzeń przez minimum 1 godzinę.
11. Routery muszą umożliwiać szyfrowanie transmisji danych i głosu z wykorzystaniem infrastruktury sieci OST112 w nowo podłączanych lokalizacjach (KP/PP) i zarządzanie przez Operatora sieci OST112.

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 światłowodowe lub kable skrętkowe miedziane kategorii min. 6a lub wyższej;

- b) nowo budowane okablowanie strukturalne należy wykonywać w standardzie kategorii min. 6 channel, poświadczone certyfikatem producenta,
- c) Centralne i Lokalne Punkty Dystrybucyjne wymaga 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) wymaga 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) wymaga się, aby system okablowania w szafie dystrybucyjnej składał się z 24 lub 48 portowych paneli, z gniazdami RJ45,
- g) oznaczenie gniazd powinno być spójne (przynajmniej dla całego obiektu) i jednoznacznie je identyfikujące,
- h) stosowane komponenty powinny pochodzić od jednego producenta oraz posiadać odpowiednie poświadczenie dopuszczenia do danej kategorii,
- i) wymaga się stosowanie szaf dystrybucyjnych o konstrukcji zgodnej do zastosowanego w pomieszczeniu systemu klimatyzacji,
- j) szafa dystrybucyjna powinna posiadać odpowiednie dedykowane do danego typu produktu: organizery kabli i uchwyty kablów zapewniające uporządkowanie i zarządzanie kablami,
- k) szafa powinna być uziemiona w sposób zapewniający poprawną pracę instalacji elektrycznej,
- l) wymaga się, aby całość oferowanej instalacji okablowania strukturalnego dla wskazanych lokalizacji miała możliwość dalszej rozbudowy w części logicznej: posiadać przekroje tras kablów oraz wielkość szafy dystrybucyjnej dostosowane do zwiększenia struktury o 25%,
- m) wymaga się, aby w Centralnych i Lokalnych Punktach Dystrybucyjnych w pomieszczeniach technicznych stosować odpowiednie urządzenia klimatyzacyjne zapewniające poprawną pracę urządzeń aktywnych sieci,
- n) wymaga się, aby w trakcie budowy lub modernizacji systemów okablowań strukturalnych dokonywać integracji z istniejącą siecią telefoniczną,
- o) gwarancja producenta na okablowanie powinna wynosić min. 20 lat,
- p) pomiary połączenia powinny być wykonane metodą Permanent Link za pomocą mierników dla danej kategorii kabla i posiadających aktualną kalibrację,
- q) dokumentacja powykonawcza powinna zawierać przynajmniej: informacje ogólne, normy i zalecenia techniczne, ogólną strukturę okablowania, okablowanie pionowe, okablowanie poziome, opis instalacji zasilającej - gdy wchodzi w skład projektu, punkty dystrybucyjne, testowanie systemu, opis sposobu oznaczania przebiegów poziomych, specyfikacje materiałową oraz certyfikat zastosowanych komponentów, rysunki i schematy, wyniki pomiaru sieci, informację na temat posiadanych przez

pracowników świadczących usługę uprawnień, kalibrację miernika, jak również dane na temat udzielanej gwarancji,

- r) okablowanie strukturalne powinno być zakończone w pomieszczeniu punktem PEL 4xRJ45 i 4x230V,
- s) liczba PEL-i w danym pomieszczeniu powinna być określana na etapie projektowania sieci LAN w uzgodnieniu z użytkownikami końcowymi,
- t) wymaga się aby w miarę możliwości projektowych, w serwerowniach projektować podłogę teletechniczną zgodnie z obowiązującymi standardami, w przypadku braku możliwości wykonania podłogi teletechnicznej w pomieszczeniach takich jak serwerownia lub lokalny punkt dystrybucyjny, należy zastosować wykładzinę antyelektrostatyczną,
- u) wymaga się aby w miarę możliwości budowlanych, projektować na korytarzach wnęki dla urządzeń wielofunkcyjnych,
- v) okablowanie strukturalne dla systemów niejawnych musi być budowane zgodnie z wymaganiami instytucji akredytujących takie systemy.

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 *PN-ISO/IEC 15408-3: 2016-10*),
- b) standardami systemów operacyjnych dla serwerów baz danych oraz serwerów aplikacji są:
 - RedHat Linux,
 - HP-UX,
 - IBM-AIX,
 - SUN-Solaris,
 - SUSE Linux Enterprise Server,
 - system operacyjny z rodziny Windows Server,
 - wymaga się stosowanie komercyjnych wersji systemów LINUX i UNIX, tym niemniej dopuszcza się wykorzystanie innych dystrybucji, spośród których zalecany jest CentOS, openSUSE, 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 (preferowane jest UTF-8),
- d) interfejs użytkownika w aplikacjach policyjnych (wszystkie systemy) musi być w języku polskim,
- e) zarządzanie serwisami, systemami operacyjnymi/wirtualizatorami centralnych systemów odbywa się tylko i wyłącznie z poziomu Biura Łączności i Informatyki KGP. Wyjątek mogą stanowić elementy systemów budowanych w architekturze rozproszonej zlokalizowane w jednostkach terenowych,
- f) wymaga się stosowanie formatu XML jako standardu wymiany danych pomiędzy systemami w strukturze organizacyjnej Policji, w tym dla nowo tworzonych rozwiązań, dopuszcza się także stosowanie formatu JSON,

- g) wymaga się, aby wymiana danych pomiędzy systemami odbywała się za pośrednictwem usług sieciowych (web services) z wykorzystaniem PPU, dla nowo tworzonych rozwiązań,
- h) wymaga się, aby bezpieczeństwo logowania na serwerach z systemami UNIX, LINUX 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 – Active Directory),
- k) do identyfikacji użytkowników i zasobów stosowane są metody oparte o PKI,
- l) funkcjonujące środowiska rozwojowe, testowe i produkcyjne muszą być odpowiednio odseparowane. Wybrana metoda separacji (np. separacja logiczna z zastosowaniem wirtualizacji, separacja fizyczna itp.) powinna odpowiadać poziomowi ryzyka i uwarunkowaniom technicznym związanym z danym środowiskiem i funkcjonującymi w nim systemami. Środowiska rozwojowe i testowe nie mogą zawierać danych rzeczywistych (produkcyjnych). Dane wykorzystywane na potrzeby tych środowisk muszą być zanonimizowane w sposób nieodwracalny lub testowo wprowadzone, np. w trakcie szkoleń.
- m) w systemie, w którym jego gestor zarządzi anonimizację danych i wskaże, które z tabel (danych) muszą być zanonimizowane, proces anonimizacji polegać będzie na losowym wymieszaniu danych (lub nadpisaniu danych wg ustalonych zasad) uniemożliwiających powtórne zestawienie oryginalnych informacji a w szczególności umożliwiających identyfikację osoby. Procedura anonimizacji z użyciem odpowiednich technik programistycznych będzie podlegać akceptacji gestora systemu i inspektora ochrony danych. Dostęp do procesu generowania danych testowych jak i do danych "wyjściowych" będzie się odbywać na zasadach dostępu do danych produkcyjnych ewentualnie przy udziale przedstawiciela gestora systemu i inspektora ochrony danych.
- n) przy przygotowywaniu projektów umów na budowę nowych systemów IT w szczególności takich które mają przetwarzać dane osobowe lub dane niejawnie należy uwzględnić jako element niezbędny do odbioru umowy pozytywne przejście przez system testów bezpieczeństwa. Scenariusze testowe i warunki realizacji przygotowuje wykonawca i będą podlegać akceptacji zamawiającego. Jeżeli testy wykażą konieczność wzmocnienia bezpieczeństwa systemu wykonawca ma być zobowiązany do jego przeprowadzenia w ramach umowy. Od testów można odstąpić gdy przedmiotem zamówienia będzie rozbudowa istniejącego systemu lub nowy system będzie współdzielił zasoby z istniejącymi systemami a przeprowadzenie testów może mieć negatywny wpływ na te systemy.
- o) 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.

4.4 Postępowanie z danymi – zarządzanie pojemnością

- 4.4.1 Gestor systemu (administrator danych), na etapie tworzenia założeń do nowo tworzonego lub modernizowanego systemu, określa wymagania odnośnie okresu, zakresu i sposobu przetwarzania danych (w tym również danych audytowych) w systemie. Określa również wymagania odnośnie postępowania z danymi po okresie przetwarzania. Wskaże również maksymalny czas, do którego można będzie przywrócić system w przypadku konieczności odtworzenia systemu.
- 4.4.2 Po okresie przetwarzania Gestor systemu (administrator danych) inicjuje proces usuwania danych zgodnie z wymaganiami określonymi na podstawie pkt. 4.4.1 oraz procedurami ich usuwania
- 4.4.3 Architekt systemu określa wymagania jakie należy spełnić aby gromadzić na nośnikach elektronicznych dane wytwarzane podczas pracy systemu, dotyczy to między innymi łącznej pojemności nośników (przestrzeni zarezerwowanej na przetwarzanie danych łącznie z danymi audytowymi), analogicznie dotyczy kopii bezpieczeństwa. Ocenia jaki będzie przyrost gromadzonej informacji w określonym czasie, np. w okresie jednego miesiąca i na podstawie tej oceny wyznacza zasób nośników wymagany do zgromadzenia informacji w okresie określonym w pkt. 4.4.1 należy również podać ww. dane dla 5 lat od uruchomienia systemu.
- 4.4.4 W trakcie projektowania systemu należy podjąć decyzję odnośnie pozyskania niezbędnych zasobów zgodnie z parametrami określonymi w pkt. 4.4.3 na cały okres przetwarzania danych określony w pkt. 4.4.1 a jeżeli to niemożliwe na okres minimum 5 lat.
- 4.4.5 Administrator systemu, zarządzający pojemnością, zobowiązany jest do analizy przyrostu danych, ubytku wolnej przestrzeni. Na tej podstawie powinien opracować trend przyrostu danych na okres przynajmniej 1 roku. Jeżeli opracowany trend znacząco przewyższa prognozy przygotowane przez architekta sygnalizuje możliwość przekroczenie przydzielonych zasobów i niezwłocznie przekazuje tę informację przełożonym.

4.5 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.

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

4.5.1 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 wyłączenia 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.

4.5.2 Urządzenia teletransmisyjne, routery CE (Customer Edge) umiejscowione w obiektach komisariatów 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.

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

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

4.5.3.1 Wymagania dla urządzeń WAN/MAN w technologii MPLS:

- a) budowa modułarna,
- b) możliwość przełączania w oparciu o standard MPLS i IP v4, IP v6,
- c) architektura elementu przełączającego oparta o w pełni nieblokowaną matrycę przełączającą,
- d) wymaga 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 jednocześnie 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,
 - EoMPLS
 - 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”.

4.5.3.2 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 ramach “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.

4.6 Systemy Łączności Telefonicznej

4.6.1 Sieci łączności telefonicznej

Policyjna Sieć Łączności Telefonicznej (PSLT) 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 (PSLT) jest połączona z sieciami publicznymi PSTN oraz sieciami resortów, służb i instytucji, do których ma odniesienie art. 4 ustawy z dnia 16 lipca 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 (PSLT) 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.

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

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

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

- a) wymagania dotyczące łączności 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 (sygn. 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 sieciami 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.

4.6.3 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, IVR itp.,
 - system rejestracji i taryfikacji połączeń, rejestrujący cały ruch telefoniczny i przechowyujący dane przez okres co najmniej 12 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,
 - system rejestracji treści korespondencji w zależności od potrzeb.
- 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 i grup zamkniętych,
 - 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 oraz IVR,
 - możliwość zdalnego wykonania podstawowych zmian konfiguracyjnych oraz nadzoru,
 - skalowalność rozwiązań umożliwiającą 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 połączenia do sieci LAN,
- skalowalność systemu umożliwiającą prostą rozbudowę,
- serwer musi realizować następujące funkcje telefoniczne,
 - o identyfikację numeru dla połączeń przychodzących,
 - o przenoszenie wywołań warunkowe oraz bezwarunkowe,
 - o parkowanie połączeń (możliwość „zawieszenia” połączenia przychodzącego, a następnie odebranie tego samego połączenia z innego aparatu w systemie),
 - o obsługę połączeń oczekujących – możliwość obsługi przez abonenta kilku połączeń jednocześnie (jedno aktywne, pozostałe zawieszone),
 - o obsługę klawiszy szybkiego wybierania,
 - o transferowanie połączeń,
 - o funkcję zamawiania połączeń,
 - o zestawianie telekonferencji,
 - o automatyczny wybór standardu kompresji głosu dla obsługiwanych połączeń,
 - o automatyczne zestawianie najtańszej drogi połączenia wychodzącego,
 - o automatyczne uaktualnianie oprogramowania telefonów IP z serwera przetwarzania połączeń,
 - o 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, IVR 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 wyposażań,
- posiadanie odpowiedniej ilości 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.

4.6.4 Przełączniki LAN

Wszystkie instalowane przełączniki Ethernet instalowane w sieci LAN w celu obsługi łączności telefonicznej, 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):

Własność	802.3af	802.3at	802.3bt	802.3bt
Maksymalna moc dostarczana przez urządzenie zasilające (PSE)	15,40 W	30,0 W	60 W	100 W
Zakres napięcia na urządzeniu zasilającym (PSE)	44,0–57,0 V[2]	50,0–57,0 V[2]	50,0–57,0 V	52,0–57,0 V
Prąd maksymalny I_{max}	350 mA	600 mA	600 mA	960 mA
Maksymalna rezystancja kabla	20 Ω	12.5 Ω	12.5 Ω	12.5 Ω

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

4.6.5 Urządzenia końcowe (terminale)

Wymaga się stosowanie następujących urządzeń końcowych (terminali) w Policijnej 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), serwery faksowe (faxserwery),
- 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.

4.6.6 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 SULTelP - 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.

4.7 Systemy radiokomunikacyjne

Jako docelowy do wdrożenia i eksploatacji w Policji planowany jest system TETRA. Przesłankami dla wprowadzenia standardu TETRA są jego cechy użytkowe i funkcjonalne, skalowalność, duża niezawodność eksploatacyjna oraz zabezpieczenia poufności przekazywanych danych. Rolę uzupełniającą do systemu TETRA w Policji mogą pełnić rozwiązania DMR tier II.

W Policji użytkowane są analogowe (EDACS, konwencjonalny) systemy łączności radiotelefonicznej. Jednostki organizacyjne Policji mają prawo użytkować te systemy, podejmując jednocześnie działania zmierzające do ich wycofania. Modernizacja i rozbudowa systemów lokalnych lub budowa nowych niestandardowych systemów lokalnych wymaga zgody Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji. Każdorazowej zgody wymaga również doposażenie istniejących systemów (innych niż TETRA i DMR tier II) w sprzęt abonencki.

4.7.1 TETRA

KWP/KSP mają prawo użytkować dotychczas eksploatowane systemy TETRA. Celem zapewnienia kompatybilności rozwiązań TETRA w skali całej Policji modernizacja i rozbudowa tych systemów wymaga zgody Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji. Zgody nie wymaga doposażanie istniejących systemów w sprzęt abonencki z uaktywnionym szyfrowaniem TEA2.

4.7.1.1 Wymagania ogólne:

- połączenia pomiędzy użytkownikami sieci w 95% przypadków, powinno być zestawione w czasie: $\leq 0,5$ s, a w pozostałych przypadkach w czasie < 2 s,
- czas uwalniania kanału komunikacyjnego po zakończeniu połączenia (czas podtrzymania) powinien być programowalny,
- system powinien dynamicznie przydzielać kanały komunikacyjne bez względu na rodzaj transmisji, głos lub dane pakietowe,
- system powinien umożliwiać jednoczesną transmisję głosu i danych pakietowych,
- przenoszenie trwającego połączenia pomiędzy sąsiednimi stacjami bazowymi nie powinno przerywać komunikacji i zmuszać użytkownika do ponownego zestawiania połączenia,
- dane lokalizacyjne stacji ruchomych powinny być przesyłane w kanale sterującym.

4.7.1.2 Połączenia grupowe:

- połączenia grupowe powinny być zestawiane przez dedykowaną dla służb cyfrową sieć radiokomunikacyjną,
- powinno być możliwe zestawienie połączenia do wszystkich użytkowników zarejestrowanych w danej grupie, bez względu na liczbę aktywnych użytkowników i ich rodzaj (radiotelefony, konsole dyspozytorskie) oraz liczbę stacji bazowych uczestniczących w realizacji połączenia,
- system powinien dynamicznie dla połączenia grupowego przydzielać kanały komunikacyjne tylko w tych stacjach bazowych, w których są zarejestrowani członkowie danej grupy,
- w każdej stacji bazowej, w której są zarejestrowani członkowie danej grupy, dla połączenia grupowego system powinien dynamicznie przydzielać tylko jeden kanał komunikacyjny,
- rejestracja do grupy rozmównej powinna odbywać się w sposób automatyczny,
- system powinien umożliwiać dostęp do połączeń grupowych tylko autoryzowanym użytkownikom,
- w trybie połączeń grupowych radiotelefon powinien automatycznie odbierać wszystkie wywołania skierowane do grupy, do której jest dołączony, bez konieczności wykonywania jakichkolwiek działań ze strony użytkownika,
- w trybie połączenia grupowego system powinien umożliwiać transmisję w tym samym czasie tylko jednemu użytkownikowi z danej grupy,
- zgłoszeniem żądania przydziału kanału komunikacyjnego do nadawania w komunikacji grupowej powinno być naciśnięcie przycisku PTT,
- możliwość połączeń grupowych na rozległym obszarze z możliwością zestawienia transmisji z użyciem wybranych stacji bazowych,
- system powinien przekazywać informację członkom grupy, jeżeli znajdują się oni poza zdefiniowanym obszarem działania grupy,
- system powinien realizować połączenia rozsiewcze do wszystkich użytkowników zarejestrowanych w wybranej stacji bazowej (Site Call) lub wybranych stacji bazowych (Multi-Site Call),
- system powinien umożliwiać opóźnione dołączenie użytkownika do połączenia grupowego,
- podczas trwania połączenia grupowego system powinien zapewnić prezentację identyfikatora strony nadającej pozostałym członkom grupy,
- system powinien przerwać połączenie grupowe w przypadku: upływu zdefiniowanego w systemie czasu podtrzymania kanału komunikacyjnego, upływu zdefiniowanego w systemie maksymalnego czasu trwania połączenia grupowego lub wyłączenia połączenia,

- w zadanym czasie przed planowanym przerwaniem połączenia, system powinien automatycznie powiadomić użytkownika o zbliżającym się momencie zakończenia komunikacji. Wymóg ten nie dotyczy wywłaszczania połączeń.

4.7.1.3 Połączenia indywidualne:

- połączenia indywidualne powinny być zestawiane przez dedykowaną dla służb cyfrową sieć radiokomunikacyjną,
- system powinien umożliwiać zestawianie połączeń indywidualnych, którymi są połączenia pomiędzy dwoma radiotelefonami, albo pomiędzy radiotelefonem a konsolą dyspozytorską,
- użytkownik, do którego jest skierowane wywołanie indywidualne, powinien mieć możliwość manualnej akceptacji tego wywołania przed zestawieniem połączenia (odbiór wywołania),
- system powinien umożliwić użytkownikowi wywoływanemu bezwarunkowo, lub wskutek spełnienia określonego warunku (zajęty, nie odpowiada, nieosiągalny) przekierowanie połączenia do innego użytkownika niż zdefiniowany przez użytkownika wywołującego,
- użytkownik, który nie odebrał przychodzącego wywołania, powinien być powiadomiony o niezrealizowanym połączeniu,
- wywoływanie skierowane do numeru zajętego, pomimo zajętości powinno być sygnalizowane,
- powinno być możliwe zakończenie połączenia indywidualnego:
 - w dowolnym momencie, przez jednego z uczestników, albo przez system,
 - na skutek upływu zdefiniowanego w systemie maksymalnego czasu trwania połączenia indywidualnego
 - wskutek wywłaszczenia połączenia.
- połączenia indywidualne powinny być realizowane w całej sieci, bez ograniczeń dotyczących obszaru,
- system powinien umożliwiać realizację połączeń indywidualnych w trybie dwukierunkowym oraz jednokierunkowym,
- system powinien umożliwiać identyfikację użytkowników uczestniczących w połączeniu indywidualnym,
- system powinien umożliwiać zdefiniowanie maksymalnego czasu trwania połączenia indywidualnego,
- w określonym czasie przed planowanym przerwaniem połączenia, system powinien automatycznie powiadomić użytkownika o zbliżającym się momencie zakończenia komunikacji. Wymóg ten nie dotyczy wywłaszczania połączeń,
- system powinien umożliwiać konfigurowanie praw użytkownika dostępnych w ramach usługi połączenia indywidualnego w tym, co najmniej ograniczeń realizacji połączeń z sieciami zewnętrznymi.

4.7.1.4 Połączenia alarmowe:

- połączenie alarmowe (połączenie ratunkowe) powinno być inicjowane za pomocą dedykowanego przycisku "Emergency",
- bez względu na to, w jakim trybie pracy jest radiotelefon, naciśnięcie dedykowanego przycisku "Emergency" powinno spowodować automatyczne przełączenie radiotelefonu w tryb połączenia alarmowego,
- w trybie połączeń alarmowych sygnał z mikrofonu powinien być nadawany automatycznie,

- naciśnięcie dedykowanego przycisku "Emergency" powinno spowodować automatyczne wysyłanie alarmu do zdefiniowanych użytkowników systemu,
- wywołanie alarmowe powinno mieć w systemie przypisany najwyższy priorytet,
- połączenie alarmowe nie może być wyłączone,
- system powinien natychmiast zestawiać połączenie alarmowe, a w przypadku braku wolnych zasobów wyłączać trwające połączenia,
- sygnalizacja przychodzącego połączenia alarmowego powinna zawierać, co najmniej identyfikator oraz lokalizację strony nadającej (lokalizacja nie dotyczy radiotelefonów bez funkcji GPS),
- system powinien zapewniać uprawnionym użytkownikom możliwość wyłączenia sygnalizacji połączenia alarmowego.

4.7.1.5 Połączenia z oraz do zewnętrznych sieci telekomunikacyjnych:

- system powinien realizować połączenia z oraz do resortowych ruchomych sieci radiokomunikacyjnych, w tym np.:
 - sieci analogowej pracującej w paśmie VHF,
 - sieci cyfrowych systemu DMR,
 - innych sieci systemu TETRA.
- system powinien realizować połączenia z oraz do resortowych stałych sieci telefonicznych,
- system powinien realizować połączenia z oraz do publicznych sieci ruchomych,
- system powinien realizować połączenia z oraz do publicznych stałych sieci telefonicznych.

4.7.1.6 Priorytety połączeń:

- system powinien umożliwiać przypisanie poziomów priorytetów dla:
 - użytkowników indywidualnych,
 - rodzajów połączeń głosowych: grupowych, indywidualnych, i alarmowych,
 - połączeń do sieci zewnętrznych,
 - transmisji danych pakietowych.
- poziom priorytetu powinien być podstawą pierwszeństwa obsługi w kolejce wywołań oczekujących oraz uprawnień do wyłączania połączeń,
- system powinien natychmiast, poza kolejnością, zestawiać połączenia alarmowe, a w przypadku braku wolnego kanału wyłączać dla potrzeb połączenia alarmowego istniejące połączenie,
- na żądanie uprzywilejowanych użytkowników z określonej listy system powinien zestawiać połączenia do wybranego użytkownika bez względu na jego zaangażowanie w trwającym połączeniu (wyłączenie użytkownika).

4.7.1.7 Kolejowanie wywołań:

- w przypadku próby zestawienia połączenia, gdy wymagane zasoby systemu są zajęte, system powinien obsługiwać kolejowanie połączeń,
- w przypadku połączeń grupowych, system powinien wywołać zwrotnie radiotelefon, którego wywołanie ze względu na brak wolnych zasobów zostało umieszczone w kolejce,
- wymaga się, aby system obsługiwał nie mniej niż 10 poziomów priorytetów,
- brak wolnych zasobów powinien być sygnalizowany wywołującemu,
- kolejowane połączenia powinny być obsługiwane w kolejności priorytetów,

- połączenia w kolejce o tym samym priorytecie powinny być obsługiwane według kolejności nadejścia.

4.7.1.8 Transmisja wiadomości statusowych:

- użytkownicy systemu powinni mieć możliwość nadawania i odbioru zakodowanych komunikatów o stanie pracy, tzw. wiadomości statusowych,
- wymaga się możliwości skonfigurowania i wykorzystywania w systemie, co najmniej 200 różnych wiadomości statusowych,
- system powinien umożliwiać przysyłanie wiadomości statusowych do wybranej grupy użytkowników albo rozsiewczo do zdefiniowanego obszaru,
- czas upływający od zainicjowania nadawania wiadomości statusowej z radiotelefonu lub konsoli dyspozytorskiej, do rozpoczęcia odbioru wiadomości w 95% przypadków nie powinien przekraczać 3 s., a w pozostałych przypadkach 6 s.,
- nadawanie i odbiór wiadomości statusowych powinno być możliwe podczas komunikacji głosowej,
- w przypadku, gdy wiadomość statusowa nie może być dostarczona do odbiorcy / odbiorców nadawca powinien otrzymać informację o niepowodzeniu dostarczenia.

4.7.1.9 Transmisja krótkich wiadomości tekstowych:

- użytkownicy systemu powinni mieć możliwość nadawania i odbioru krótkich wiadomości tekstowych o długości przynajmniej 255 bajtów,
- nadawanie i odbiór krótkich wiadomości tekstowych powinno być możliwe podczas komunikacji głosowej,
- opóźnienia transmisyjne usługi krótkich wiadomości tekstowych: całkowity czas przesłania wiadomości tekstowej o długości do 50 bajtów w 95% przypadków nie powinien przekraczać 5 s., w pozostałych przypadkach 10 s., całkowity czas przesłania wiadomości tekstowej o długości od 51 do 255 bajtów w 95% przypadków nie powinien przekraczać 6 s., w pozostałych przypadkach 12 s.,
- w przypadku, gdy krótka wiadomość tekstowa nie może być dostarczona do odbiorcy/odbiorców, nadawca powinien otrzymać informację o braku możliwości jej dostarczenia.

4.7.1.10 Transmisja danych pakietowych:

- system powinien umożliwiać przysyłanie danych pakietowych. Rozmiar przesyłanych danych pakietowych może być dowolny,
- brama po stronie infrastruktury systemu powinna wykorzystywać protokoły IP do przysyłania danych pakietowych między terminalami,
- opóźnienie przesyłu danych pakietowych o wielkości od 256 do 1500 bajtów, liczone od nadania pierwszego bitu datagramu IP z radiotelefonu do dostarczenia jego ostatniego bitu do bramy IP, przy założeniu, że transmisja danych z radiotelefonu odbywa się bez przerw, w 95% przypadków nie powinno przekroczyć 10 s., a w pozostałych przypadkach 20 s.,

- w przypadku, gdy dane pakietowe nie mogą być skutecznie przesłane, inicjujący transmisję powinien otrzymać informację o braku możliwości ich przesłania.

4.7.1.11 Organizacja łączności:

- system powinien umożliwiać dynamiczne tworzenie grup użytkowników zgodnie z aktualnymi potrzebami operacyjnymi poprzez zdalne dołączanie użytkowników do grupy lub odłączanie od grupy,
- system powinien umożliwiać zachowanie autonomii działania różnych organizacji poprzez wydzielenie w ramach zbudowanej sieci osobnych, wirtualnych podsieci,
- wymaga się, aby system mógł obsługiwać nie mniej niż 10 wirtualnych podsieci użytkowników, umożliwiając tworzenie rozbudowanych struktur hierarchicznych,
- system powinien umożliwiać nadawanie użytkownikom skróconych nazw, aliasów,
- adresowanie skróconymi numerami - wysyłanie do infrastruktury skróconego numeru zamiast pełnego identyfikatora,
- powinna być zapewniona możliwość bezpośredniej komunikacji pomiędzy radiotelefonami, bez udziału infrastruktury sieci,
- w trybie bezpośredniej komunikacji DMO powinny być realizowane, co najmniej następujące usługi:
 - połączenia grupowe,
 - połączenia indywidualne,
 - połączenia alarmowe,
 - przesyłanie statusów.
- w przypadku utraty komunikacji pomiędzy stacją bazową a stacjonarną infrastrukturą (węzłem sterującym) sieci, stacja bazowa powinna działać w trybie jednostrefowej lokalnej łączności trunkingowej,
- w trybie jednostrefowej lokalnej łączności trunkingowej stacja bazowa powinna realizować, co najmniej następujące usługi:
 - połączenia grupowe,
 - połączenia indywidualne,
 - połączenia alarmowe,
 - szyfrowanie transmisji radiowej z kluczem statycznym.
- wszyscy użytkownicy pozostający w zasięgu stacji bazowej powinni automatycznie otrzymywać informację o stanie sieci: trunking rozległy/trunking lokalny,
- użytkownik terminala powinien otrzymywać informacje o tym, że znajduje się poza zasięgiem stacji bazowej,
- system powinien umożliwiać zdalną zmianę konfiguracji infrastruktury sieci,
- system powinien umożliwiać:
 - monitorowanie ruchu w kanałach radiowych,
 - sprawdzenie rejestracji radiotelefonów,
 - raportowanie aktywności grup,
 - raportowanie aktywności indywidualnych użytkowników.
- radiotelefon powinien skanować grupy rozmówne, do których jest dołączony,
- system powinien umożliwiać zdefiniowanie, co najmniej 20 000 identyfikatorów grupowych,
- system powinien umożliwiać zdefiniowanie co najmniej 140 000 identyfikatorów indywidualnych.

4.7.1.12 Szybkie rozszerzenie zasięgu łączności:

- możliwość połączeń pomiędzy użytkownikami wykonującymi zadania w zasięgu sieci trunkingowej oraz poza nią w trybie łączności bezpośredniej z wykorzystaniem dedykowanego radiotelefonu spełniającego funkcje bramy (TMO/DMO Gateway),
- w połączeniach realizowanych z wykorzystaniem bramy (Gateway) powinny być dostępne, co najmniej następujące usługi:
 - połączenia grupowe,
 - połączenia alarmowe.
- użytkownicy uczestniczący w połączeniach realizowanych z wykorzystaniem bramy powinni uzyskać sygnalizację trybu pracy "Gateway",
- możliwość połączeń dla zamkniętej grupy użytkowników wykonujących zadania poza zasięgiem stacji sieci trunkingowej, wykorzystująca tryb łączności bezpośredniej z zastosowaniem dedykowanego radiotelefonu spełniającego funkcje stacji retransmisyjnej (DMO Repeater),
- w połączeniach realizowanych z wykorzystaniem stacji retransmisyjnej (DMO Repeater) powinny być dostępne, co najmniej następujące usługi:
 - połączenia grupowe,
 - połączenia indywidualne,
 - połączenia alarmowe.
- użytkownicy uczestniczący w połączeniach realizowanych z wykorzystaniem stacji retransmisyjnej powinni uzyskać sygnalizację trybu pracy "Repeater",
- radiotelefon pełniący funkcję przekaźnika oraz radiotelefony wykorzystujące tryb pracy „Repeater” powinny wspierać ten sam typ wymiany komunikacji w systemie TETRA,
- powinno być możliwe wykorzystanie mobilnej stacji bazowej w trybie jednostrefowej lokalnej łączności trunkingowej,
- powinno być możliwe przyłączenie do systemu i integracja ze stacjonarną infrastrukturą sieci mobilnej stacji bazowej.

4.7.1.13 Bezpieczeństwo sieci:

- system TETRA powinien wykorzystywać zharmonizowane zakresy częstotliwości przeznaczone w Europie dla służb bezpieczeństwa publicznego i ratownictwa: 380-385 MHz dla nadajników stacji ruchomych oraz 390-395 MHz dla nadajników stacji bazowych,
- system powinien realizować procedury autoryzacji radiotelefonów poprzez uwierzytelnienie inicjowane przez infrastrukturę sieci (SwMI). System powinien umożliwiać uwierzytelnienie infrastruktury sieci (SwMI),
- system powinien być wyposażony w centrum zarządzania kluczami do celów uwierzytelniania,
- wyposażenie systemu w mechanizmy weryfikacji uprawnień
- możliwość szyfrowania transmisji (głos, dane, sygnalizacja), realizowanej w interfejsie radiowym (MS-BS) za pomocą zmiennych kluczy szyfrujących (długość klucza szyfrującego min. 64 bity):
 - wspólny klucz szyfrujący-CCK,
 - grupowy klucz szyfrujący-GCK,
 - pochodny klucz szyfrujący-DCK,
 - statyczny klucz szyfrujący-SCK.
- system powinien być wyposażony w centrum dystrybucji kluczy,

- system powinien umożliwiać dynamiczną zmianę klucza szyfrującego drogą radiową (OTAR), co najmniej w zakresie klucza pochodnego (DCK - Derived Cipher Key),
- system powinien umożliwiać zdalne czasowe zablokowanie/odblokowanie obsługi radiotelefonu w sieci,
- system powinien umożliwiać zdalne, trwałe zablokowanie obsługi radiotelefonu w sieci,
- system powinien zawierać mechanizmy zabezpieczenia aplikacyjno-sprzętowego baz danych systemu,
- system musi spełniać wymogi ochrony antywirusowej,
- system powinien umożliwiać stosowanie szyfrowania głosu end-to-end (E2E) w relacjach radiotelefon-radiotelefon, oraz radiotelefon-konsola dyspozytorska za pomocą klucza o długości nie mniejszej od 128 bitów,
- system powinien umożliwiać szyfrowanie korespondencji radiowej z wykorzystaniem algorytmu TEA2. W okresie przejściowym (z uwagi na istniejące ośrodki TETRA wykorzystujące szyfrowanie TEA1) dopuszcza się możliwość wykorzystywania grup CLEAR. Okres przejściowy powinien zostać ograniczony do niezbędnego minimum,
- możliwość przekazywania informacji do użytkowników połączenia o rodzaju zestawianej transmisji (szyfrowana/nieszyfrowana).

4.7.1.14 Konsole dyspozytorskie:

- dostęp i konfigurowanie, w zakresie przyznanych uprawnień, do zasobów: grup rozmównych, radiotelefonów, interfejsów,
- konsole powinny działać w trybie połączeń głosowych oraz transmisji danych pakietowych,
- konsole powinny umożliwiać obsługę zgłoszeń alarmowych (Emergency) generowanych w systemie,
- konsole powinny umożliwiać monitorowanie aktywności członków grup,
- konsole powinny umożliwiać nadawanie do więcej niż jednej grupy rozmównych z zachowaniem separacji komunikacji pomiędzy grupami,
- konsole powinny umożliwiać zespalandzenie (łączenie) dwóch lub więcej grup rozmównych w jedną wirtualną grupę, która wykorzystuje jeden kanał komunikacyjny,
- konsole powinny umożliwiać zespalandzenie (przyłączenie) grupy systemu wykorzystującej kanał innej radiokomunikacyjnej sieci resortowej (analogowej, DMR, TETRA) do innej grupy/grup systemu,
- konsole powinny umożliwiać dyskretny nasłuch,
- konsole powinny umożliwiać natychmiastowe nadawanie z prawem wyłączenia połączeń,
- możliwość przekazywania informacji o stanie systemu i alarmach,
- możliwość używania konsol dyspozytorskich przewodowych i bezprzewodowych.

4.7.1.15 Podsystem zarządzania siecią:

- podsystem zarządzania siecią powinien być zgodny z modelem FCAPS (Fault, Configuration, Accounting, Performance, Security) i powinien obejmować zarządzanie: usterkami, konfiguracją, rozliczeniami, wydajnością oraz bezpieczeństwem,
- podsystem zarządzania usterkami powinien w czasie rzeczywistym oraz w formie komunikatów informować administratora systemu o nieprawidłowościach związanych z funkcjonowaniem sieci,

- podsystem powinien być skonfigurowany w taki sposób, aby umożliwić administratorowi zapoznanie się ze szczegółowym opisem błędu, który będzie dostępny po rozwinięciu komunikatu o awarii,
- szczegółowy opis błędu powinien zawierać:
 - jednoznaczną identyfikację problemu wraz z podaniem przyczyny jego wystąpienia,
 - algorytm postępowania dla administratora.
- podsystem zarządzania usterkami powinien umożliwiać przegląd historii alarmów danego rodzaju w okresie, co najmniej 90 dni,
- podsystem zarządzania konfiguracją powinien udostępniać szczegółowe informacje o nastawach i elementach konfiguracyjnych, które będą zawierać: charakterystykę elementu, który jest konfigurowany, jednoznaczną identyfikację nastawy konfiguracyjnej, graniczne wartości przedziału, w ramach, którego mogą być dokonywane zmiany nastaw konfiguracyjnych, opis wpływu określonej wartości nastawy konfiguracyjnej na konfigurowany element,
- podsystem zarządzania konfiguracją powinien umożliwiać utworzenie i archiwizowanie kopii zapasowej (backup) danych konfiguracyjnych systemu (rozumianych, jako dane zawierające również informacje dotyczące grup i użytkowników),
- podsystem zarządzania konfiguracją powinien umożliwiać odzyskiwanie danych konfiguracyjnych systemu z kopii zapasowej, tworzenie i odzyskiwanie danych konfiguracyjnych nie powinno powodować przerw w prawidłowej pracy systemu,
- podsystem zarządzania rozliczeniami powinien umożliwiać generowanie raportów o aktywności użytkowników w systemie za okres min. 365 dni. Konfiguracja podsystemu powinna umożliwiać, po wprowadzeniu numeru identyfikacyjnego radiotelefonu oraz zadanego okresu, uzyskanie następujących danych o aktywności użytkownika w systemie:
 - znacznik daty i czasu,
 - rodzaj połączenia (grupowe, indywidualne, telefoniczne, alarmowe, wysłanie statusu, wysłanie krótkich wiadomości tekstowych, głosowe, transmisja danych, afiliacja do systemu itp.),
 - status połączenia (rozpoczęte, zakończone, szyfrowane, nieszyfrowane, odrzucone, dopuszczone, kolejgowane itp.),
 - kierunek połączenia (radiotelefon – radiotelefon, radiotelefon - konsola, radiotelefon - grupa, radiotelefon - telefon itp.),
 - identyfikatory, aliasy, adresy IP itp. stron biorących udział w połączeniu,
 - czas trwania połączenia,
 - ilość przesłanych danych pakietowych,
 - identyfikatory stacji bazowych zaangażowanych w połączenie z jednoznacznym wskazaniem stacji, do której był zalogowany wywołujący.
- konfiguracja podsystemu powinna umożliwiać - po wprowadzeniu numeru identyfikacyjnego grupy oraz zadanego okresu, uzyskanie następujących danych o aktywności grupy rozmównej w systemie:
 - znacznik daty i czasu,
 - rodzaj połączenia (grupowe, telefoniczne, alarmowe, wysłanie statusu, wysłanie krótkich wiadomości tekstowych itp.),
 - status połączenia (rozpoczęte, zakończone, szyfrowane, nieszyfrowane, odrzucone, dopuszczone, kolejgowane itp.),
 - kierunek połączenia (konsola – grupa, radiotelefon – grupa, telefon – grupa itp.),
 - identyfikatory, aliasy, adresy IP itp. stron biorących udział w połączeniu,

- czas trwania połączenia,
- identyfikatory stacji bazowych zaangażowanych w połączenie z jednoznacznym wskazaniem stacji, do której był zalogowany wywołujący.
- konfiguracja podsystemu powinna umożliwiać - po wprowadzeniu numeru identyfikacyjnego radiotelefonu lub zakresu numerów identyfikacyjnych lub listy numerów identyfikacyjnych z możliwością jej importu z pliku utworzonego przynajmniej w jednym z popularnych formatów, takich jak .txt, .xls, .doc itp. - uzyskanie bieżących danych na temat użytkownika(ów):
 - bieżąca afiliacja do strefy lub jej brak,
 - bieżąca afiliacja do grupy lub jej brak,
 - ostatnie dane lokalizacyjne GPS (opcjonalnie).
- podstawowe dane z bazy użytkowników – identyfikator, alias, numer fabryczny, obecny użytkownik, status pracy w systemie (radiotelefon aktywny, wykluczony, zablokowany, przegrupowany, oczekujący na przegrupowanie lub zablokowanie, zaginiony itp.),
- procesy zarządzania wydajnością powinny określać zdolność systemu do obsługi generowanego ruchu poprzez charakterystykę efektywności zaspokajania potrzeb użytkowników przez system łączności,
- parametryzowanie wydajności systemu powinno odbywać się poprzez bieżące monitorowanie obciążenia stref oraz raportowanie zidentyfikowanych cech właściwych dla opisu przebiegu łączności,
- w skład powyższych cech powinny wchodzić:
 - całkowita liczba wywołań dla wskazanego obszaru, rozpatrywana jako sumaryczna liczba połączeń oraz liczba wywołań w jednostce czasu,
 - rodzaj transmisji (połączenia głosowe, transmisja danych),
 - czas trwania transmisji,
 - liczba i typ stanów niedostępności zasobów,
 - liczba stref uczestniczących w połączeniach,
 - zajętość kanałów komunikacyjnych w zadanym obszarze i jednostce czasu,
 - liczba aktywnych użytkowników oraz grup rozmównych w zadanym obszarze i jednostce czasu.
- podsystem powinien umożliwiać wgląd w historię parametrów wydajnościowych za okres min. 90 dni,
- we wszystkich podsystemach powinna być zapewniona możliwość raportowania przechowywanych danych wg zadanych parametrów czasu, zakresu i sposobu sortowania,
- raportowanie powinno zapewniać zarówno bezpośredni wydruk, jak również eksport w logicznie sformatowanej postaci do pliku w jednym, wybranym przez użytkownika formacie: tekstowym, oddzielonym tabulatorami lub innymi charakterystycznymi znakami, bazy SQL, MS Office, OpenOffice.

4.7.1.16 Łączność ziemia – powietrze:

- na etapie uzyskania pokrycia zasięgiem radiowym obszarów całych województw (zgodnie z odrębnymi wymaganiami dla zasięgów radiowych) w relacji do naziemnych urządzeń łączności radiowej TETRA. System powinien również zapewniać pokrycie dla dwukierunkowej łączności ze statkami powietrznymi (AGA) poruszającymi się z prędkością do 300 km/h na wysokości do 500 m ponad powierzchnią ziemi.
- na etapie uzyskania pokrycia zasięgiem radiowym obszarów całych województw (zgodnie z odrębnymi wymaganiami dla zasięgów radiowych) w relacji do naziemnych urządzeń łączności

radiowej TETRA wymaga się wykorzystanie dla potrzeb łączności AGA europejskich zharmonizowanych zakresów częstotliwości 384,800 – 385,000 MHz i 394,800 – 395,000 MHz. Radiotelefony przeznaczone do łączności AGA powinny automatycznie wybierać kanał sterujący/częstotliwość stacji bazowej AGA. Wymaga się, aby konfiguracja sieci uniemożliwiała rejestrację naziemnych stacji ruchomych w komórkach przeznaczonych do łączności AGA. Dopuszcza się, aby terminal łączności AGA wykorzystywał sieć łączności lądowej, gdy statek powietrzny znajduje się na ziemi. Przenoszenie trwającego połączenia AGA pomiędzy sąsiednimi stacjami bazowymi nie może powodować zrywania komunikacji. Usługi dostępne dla użytkowników radiotelefonów na statkach powietrznych powinny być takie same jak dla użytkowników radiotelefonów w pojazdach lądowych. W przypadku braku komunikacji stacji bazowej AGA z infrastrukturą sieci, stacja bazowa powinna wstrzymać nadawanie, aby umożliwić awaryjną komunikację terminali AGA za pośrednictwem sieci naziemnej.

4.7.1.17 Rejestracja oraz archiwizacja aktywności użytkowników:

- podsystem rejestracji i archiwizacji powinien zapewniać cyfrowy zapis korespondencji głosowej wraz ze znacznikami daty i godziny umożliwiającymi odsłuch, wyszukiwanie i katalogowanie nagrań.
- podsystem rejestracji i archiwizacji powinien umożliwiać kopiowanie nagrań na przenośne nośniki danych,
- scentralizowane zarządzanie rejestracją korespondencji z możliwością zdalnego dostępu i eksportu z poziomu lokalnych stanowisk odsłuchowych z możliwością nadawania uprawnień wynikających z użytkowania wirtualnych podsieci poszczególnych użytkowników oraz struktur hierarchicznych. Konsola dyspozytorska powinna posiadać możliwość odsłuchu, co najmniej ostatnich 30 minut własnej korespondencji zarejestrowanej lokalnie.

4.7.1.18 Współpraca z innymi rozwiązaniami teleinformatycznymi:

- wykonawca powinien udostępnić specyfikację interfejsów API,
- na etapie uzyskania pokrycia zasięgiem radiowym obszarów całych województw graniczących z państwami UE zostanie wystawiony interfejs umożliwiający współpracę z systemami łączności krajów sąsiednich w celu realizacji łączności transgranicznej.

4.7.1.19 Konsola dyspozytorska

a) wymagania ogólne:

- konsole dyspozytorskie muszą być urządzeniami przeznaczonymi do pracy ciągłej, zasilanymi z sieci energetycznej prądem przemiennym o napięciu 230V, wyposażonymi w:
 - klawiaturę,
 - mysz,
 - monitor LCD dotykowy o wielkości co najmniej 23 cale z możliwością regulacji kąta nachylenia (określonego w stopniach katowych) i wysokości położenia ekranu od powierzchni biurka,
 - mikrofon biurkowy z przyciskiem nadawania,
 - nożny przycisk nadawania,
 - co najmniej dwa zewnętrzne głośniki o mocy minimum 5W,

- 5 kpl. osobistych zestawów przewodowych nagłownych, mikrofonowo - słuchawkowych podłączanych do konsoli poprzez „szybkoszłączkę” wraz z przyciskiem nadawania,
- co najmniej jeden niewykorzystany port USB w wersji co najmniej 3.0 do podłączenia pamięci masowych.
- konsole dyspozytorskie muszą być połączone z infrastrukturą za pomocą sieci teletransmisyjnej z użyciem protokołu TCP/IP;
- system powinien mieć możliwość podłączenia Konsoli Dyspozytorskiej przez łącze satelitarne lub modem LTE.

b) wymagania funkcjonalne:

- konsole dyspozytorskie muszą działać co najmniej w trybie połączeń głosowych, transmisji danych pakietowych, krótkich wiadomości tekstowych, wiadomości statusowych; administrator konsoli dyspozytorskiej musi mieć dostęp i możliwość konfigurowania, w zakresie przyznanых uprawnień, do zasobów:
 - grup rozmównych,
 - terminali,
 - interfejsów.
- konsole dyspozytorskie muszą umożliwiać pracę w trybie ciągłym 24/7,
- konsole muszą umożliwiać obsługę zgłoszeń alarmowych (Emergency) generowanych w systemie,
- konsole dyspozytorskie muszą umożliwiać monitorowanie aktywności członków grup czyli podglądu aktualnie załogowanych na grupie użytkowników,
- konsole dyspozytorskie muszą przekazywać informację o wybranych alarmach generowanych w ramach systemu,
- konsole dyspozytorskie muszą posiadać GUI umożliwiający dyspozytorowi pełną obsługę i wizualizację stanów dedykowanych dla danej konfiguracji zasobów konsolowych. Interfejs GUI konsoli dyspozytorskiej musi być w języku polskim,
- konsola dyspozytorskiej powinna być wyposażona w urządzenie sumujące sygnał audio z konsoli i zewnętrznego aparatu telefonicznego, które zsumowany sygnał prześle do nagłownego zestawu mikrofono-słuchawkowego,
- możliwość nadawania przez administratora opcjonalnych uprawnień każdej z konsol dyspozytorskich do korzystania z zasobów systemu,
- możliwość niezależnej zmiany kanałów/grup dla każdego zasobu dostępnego w systemie z poziomu konsoli dyspozytorskiej,
- możliwość nadawania przez administratora opcjonalnych poziomów uprawnień każdemu z zasobów systemowych udostępnionych na danej konsoli, niezależnie dla każdej z konsol,
- konsole dyspozytorskie muszą posiadać możliwość tworzenia kont z uprawnieniami użytkowników ograniczających dostęp do zasobów konsoli,
- grupy rozmówne oraz dostępne zasoby innych systemów radiokomunikacyjnych obsługiwane przez konsolę muszą być przedstawiane graficznie jako okna wyświetlane na jej ekranie,
- do głośników musi być możliwość przypisania im źródła sygnału audio tak, aby jeden głośnik był przypisany do aktualnie wybranych grup/kanałów rozmównych (fonia wybrana), a drugi głośnik musi sumować audio pochodzące ze wszystkich innych grup/kanałów rozmównych (fonia niewybrana). Każdy z głośników musi posiadać wbudowaną niezależną regulację głośności,

- każdy z zasobów udostępniony na konsoli musi posiadać możliwość niezależnej, programowej regulacji głośności dla fonii wybranej i niewybranej z zapamiętaniem ostatnio ustawionego stanu,
- oprogramowanie dyspozytorskie musi zawierać okno wyświetlające historię połączeń odbywających się w ramach danej konsoli; historia połączeń musi obejmować co najmniej 200 ostatnich połączeń,
- konsola dyspozytorska musi mieć możliwość łączenia ze sobą dwóch lub więcej grup/kanałów rozmównych, aby mogły uczestniczyć w scalonym połączeniu grupowym,
- konsola dyspozytorska musi mieć możliwość łączenia dostępnych zasobów TETRA i innych systemów radiokomunikacyjnych, aby mogły uczestniczyć w scalonym połączeniu grupowym,
- połączenia grupowe muszą być inicjowane przez wybranie na wyświetlaczu graficznym grupy rozmownej i naciśnięcie przycisku nadawania,
- włączenie nadawania korespondencji musi być możliwe do realizacji za pomocą myszki komputerowej, włącznika nożnego, włącznika ręcznego lub poprzez bezpośredni dotyk na ekranie monitora,
- konsole dyspozytorskie muszą otrzymywać sygnał audio ze wszystkich grup rozmównych, do których są dołączone,
- dyspozytorzy konsol mają najwyższy priorytet w ramach połączenia grupowego i muszą mieć możliwość przerwania nadawania aktualnie nadającemu terminalowi,
- konsole dyspozytorskie muszą mieć możliwość wykonywania i odbierania połączeń indywidualnych do i od terminali,
- konsole dyspozytorskie muszą mieć możliwość wykonywania i odbierania połączeń telefonicznych z funkcjonalnością CLIP,
- dyspozytor musi mieć dostęp do listy aliasów/ISSI terminali umożliwiającej zainicjowanie połączenia indywidualnego,
- dyspozytor musi mieć możliwość zainicjowania wywłaszczającego priorytetowego połączenia indywidualnego, które poprzez wywłaszczenie otrzyma zasoby ruchowe i przerwie połączenie indywidualne lub telefoniczne niższego priorytetu, w które zaangażowania będzie strona wywoływana,
- konsola dyspozytorska musi zapewniać interfejs użytkownika do wysyłania i odbierania wiadomości tekstowych (SDS),
- konsola dyspozytorska musi umożliwiać rozsyłanie wiadomości tekstowych do wielu terminali jednocześnie,
- w momencie odebrania połączenia alarmowego, każda konsola dyspozytorska monitorująca daną grupę rozmówną musi zacząć emitować specyficzny sygnał dźwiękowy do momentu podjęcia działania przez dyspozytora;
- prezentowane na ekranie wpisy historii połączeń dla przychodzącej komunikacji alarmowej muszą być oznaczone w sposób wyróżniony. Gdy dyspozytor podejmie obsługę sytuacji alarmowej, wszystkie konsole dyspozytorskie monitorujące daną grupę rozmówną muszą otrzymać wizualną sygnalizację,
- z poziomu konsoli dyspozytorskiej dyspozytor musi mieć możliwość odsłuchu co najmniej ostatnich 12 godzin korespondencji prowadzonej na własnym stanowisku. Nagrania na liście nagrań muszą być oznaczone graficznym wyróżnikiem typu połączenia. Wyszukiwanie nagrań poprzez co najmniej przewijanie w przód i wstecz listy zarejestrowanych nagrań. Odtwarzanie nagrania z możliwością pauzy, przewijania do przodu i wstecz;
- konsole muszą posiadać wbudowany mechanizm uniemożliwiający pojawienie się sprzężeń akustycznych na sąsiadujących konsolach,

- przestrzeń robocza każdego dyspozytora konsoli musi być konfigurowalna przez administratora systemu. Administrator musi mieć także możliwość zdefiniowania kilku profili dyspozytorskich (obejmujących konkretną konfigurację konsoli) możliwych do pobrania przez dyspozytora,
- konsola Dyspozytorska musi zapewniać dostęp do zobrazowanych graficznie co najmniej 128 zasobów: TETRA, DMR, z jednoczesną obsługą co najmniej 128 sesji audio na jednej konsoli. Limity te muszą być niezależne dla każdej konsoli,
- konsola musi zapewniać tworzenie co najmniej 16 scaleń, w każdym scaleniu musi być możliwość umieszczenia co najmniej 10 zasobów. Limity te muszą być niezależne dla każdej konsoli,
- konsola musi zapewniać tworzenie co najmniej 3 multiwyborów, w każdym multiwyborze musi być możliwość umieszczenia co najmniej 20 zasobów. Ograniczenie sumarycznej liczby wszystkich zasobów w multiwyborach nie może być mniejsze niż 40,
- dostępne na konsolach dyspozytorskich zasoby grupowe, muszą być pozyskiwane poprzez bezpośrednie połączenie z systemem. Niedopuszczalne jest pozyskiwanie tych zasobów poprzez wykorzystywanie terminali,
- cała korespondencja prowadzona z wykorzystaniem konsoli dyspozytorskiej musi być rejestrowana w module rejestracji.

4.7.1.20 Radiotelefon noszony TETRA

a) wymagania ogólne:

- zgodność ze standardem ETSI TETRA,
- zakres częstotliwości pracy w trybie TMO min. 380 - 430 MHz,
- zakres częstotliwości pracy w trybie DMO min. 380 - 430 MHz,
- minimalny zakres temperatury pracy MS, anteny, akumulatora, klipsa, od -25°C do + 55°C,
- nadajnik klasy 3L (1,8W),
- kolorowy wyświetlacz,
- minimalna klasa ochrony obudowy przed wnikaniem pyłu i wody IP 65,
- pełna klawiatura alfanumeryczna.

b) wymagania funkcjonalne:

- praca w trybach TMO, DMO,
- transmisja danych pakietowych,
- wysyłanie, odbieranie krótkich wiadomości SDS,
- praca na dowolnej z co najmniej 800 zaprogramowanych grup rozmownych TMO,
- programowe definiowanie wyświetlanej nazwy grupy (minimum 12 znaków alfanumerycznych),
- programowy podział zaprogramowanych grup rozmownych na minimum 50 folderów po minimum 16 grup każdy, przy czym ta sama grupa może być przydzielona do dowolnej liczby folderów,
- programowe ograniczanie czasu nadawania,
- programowe i ręczne ustawienia grup rozmownych do pracy w skaningu ze zróżnicowanym priorytetem skanowania,
- tworzenie przynajmniej 20 różnych list skanowania po przynajmniej 16 pozycji każda, które będą uaktywniane stosownie do potrzeb użytkownika,
- wybór grup rozmownych z użyciem dedykowanego przełącznika obrotowego lub dedykowanych do tego celu przycisków,
- regulację głośności przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,

- realizację wywołań: alarmowych, grupowych, indywidualnych i telefonicznych,
- wysyłanie i odbieranie wiadomości statusowych,
- programowe definiowanie wyświetlanej nazwy grupy DMO (minimum 12 znaków alfanumerycznych),
- programowy podział zaprogramowanych grup DMO na foldery,
- programowe przypisanie dowolnej grupy DMO do dowolnej grupy TMO, z możliwością powtórzenia tego samego kanału DMO dla dowolnej ilości grup TMO,
- korzystanie z interfejsu użytkownika w języku polskim,
- włączenie trybu alarmowego dedykowanym przyciskiem,
- realizację połączeń telefonicznych w trybie duplex,
- realizację połączeń indywidualnych w trybie simpleks oraz w trybie duplex,
- programowe zdefiniowanie skróconych numerów wybierania ISSI,
- programowe i ręczne zdefiniowanie listy kontaktów radiowych i telefonicznych o pojemności przynajmniej 500 pozycji,
- ładowanie kluczy maskujących do terminala za pomocą sprzętu dostarczonego przez wykonawcę w ramach zamówienia,
- zabezpieczenie kluczy maskujących; klucze nie mogą być przechowywane w terminalu w sposób jawny a ich odczyt lub przepisanie pomiędzy dwoma terminalami musi być niemożliwe;
- przystosowanie do obsługi maskowania E2E,
- realizację funkcjonalności OTAR,
- użycie programowalnych przycisków funkcyjnych (min. 2), umieszczonych w sposób umożliwiający szybki i łatwy dostęp do uprzednio zdefiniowanych funkcji,
- pracę w klasach bezpieczeństwa SC1, SC2, SC3, SC3 (z i bez GCK),
- maskowanie korespondencji TETRA-TEA2. W okresie przejściowym dopuszcza się stosowanie maskowania TEA1,
- wysyłanie i odbieranie wiadomości statusowych,
- praca w trybie TMO/DMO Gateway, wg potrzeb,
- praca w trybie DMO Repeater, wg potrzeb.

4.7.1.21 Radiotelefon przewoźny TETRA

a) wymagania ogólne

- zgodność ze standardem ETSI TETRA,
- zakres częstotliwości pracy w trybie TMO przynajmniej 380 - 430 MHz,
- zakres częstotliwości pracy w trybie DMO przynajmniej 380 - 430 MHz,
- nadajnik klasy 2 (10W),
- czułość dynamiczna odbiornika nie gorsza niż -103dBm,
- wyświetlacz kolorowy o ilości kolorów nie mniejszej niż 65000 i rozdzielczości wyświetlacza nie mniejszej niż 320 x 240 pikseli,
- klasa ochrony minimum IP 54,
- pełna klawiatura alfanumeryczna,

b) wymagania funkcjonalne

- praca w trybach TMO, DMO,
- transmisja danych pakietowych,
- wysyłanie, odbieranie krótkich wiadomości SDS,

- praca na dowolnej z co najmniej 800 zaprogramowanych grup rozmownych TMO,
- programowe definiowanie wyświetlanej nazwy grupy (minimum 12 znaków alfanumerycznych),
- programowy podział zaprogramowanych grup rozmownych na minimum 50 folderów po minimum 16 grup każdy, przy czym ta sama grupa może być przydzielona do dowolnej liczby folderów,
- programowe ograniczanie czasu nadawania,
- programowe i ręczne ustawienia grup rozmownych do pracy w skaningu ze zróżnicowanym priorytetem skanowania,
- tworzenie przynajmniej 20 różnych list skanowania po przynajmniej 16 pozycji każda, które będą uaktywniane stosownie do potrzeb użytkownika,
- wybór grup rozmownych z użyciem dedykowanego przełącznika obrotowego lub dedykowanych do tego celu przycisków,
- regulację głośności przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- realizację wywołań: alarmowych, grupowych, indywidualnych i telefonicznych,
- wysyłanie i odbieranie wiadomości statusowych,
- programowe definiowanie wyświetlanej nazwy grupy DMO (minimum 12 znaków alfanumerycznych),
- programowy podział zaprogramowanych grup DMO na foldery,
- programowe przypisanie dowolnej grupy DMO do dowolnej grupy TMO, z możliwością powtórzenia tego samego kanału DMO dla dowolnej ilości grup TMO,
- korzystanie z interfejsu użytkownika w języku polskim,
- włączenie trybu alarmowego dedykowanym przyciskiem,
- realizację połączeń telefonicznych w trybie duplex,
- realizację połączeń indywidualnych w trybie simpleks oraz w trybie duplex,
- programowe zdefiniowanie skróconych numerów wybierania ISSI,
- programowe i ręczne zdefiniowanie listy kontaktów radiowych i telefonicznych o pojemności przynajmniej 500 pozycji,
- ładowanie kluczy maskujących do terminala za pomocą sprzętu dostarczonego przez wykonawcę w ramach zamówienia,
- zabezpieczenie kluczy maskujących; klucze nie mogą być przechowywane w terminalu w sposób jawny a ich odczyt lub przepisanie pomiędzy dwoma terminalami musi być niemożliwe;
- przystosowanie do obsługi maskowania E2E,
- realizację funkcjonalności OTAR,
- użycie programowalnych przycisków funkcyjnych (min. 2), umieszczonych w sposób umożliwiający szybki i łatwy dostęp do uprzednio zdefiniowanych funkcji,
- pracę w klasach bezpieczeństwa SC1, SC2, SC3, SC3 (z i bez GCK),
- maskowanie korespondencji TETRA-TEA2. W okresie przejściowym dopuszcza się stosowanie maskowania TEA1,
- wysyłanie i odbieranie wiadomości statusowych,
- praca w trybie TMO/DMO Gateway, wg potrzeb,
- praca w trybie DMO Repeater, wg potrzeb.

c) wymagania sprzętowe i ukompletowanie

- ukompletowanie MS musi umożliwiać montaż rozdzielny,
- moduł nadawczo-odbiorczy-N/O,
- panel sterowania,
- przewód łączący panel sterowania z modulem N/O,

- przewód zasilający z zabezpieczeniem od strony akumulatora,
- mikrofon zewnętrzny dedykowany do MS z przyciskiem nadawania PTT i zaczepem,
- głośnik o mocy minimum 4W,
- uaktywniony odbiornik GPS,
- antena dachowa zintegrowana z anteną GPS z przewodem,
- mikrofon i przycisk PTT, wg potrzeb.

d) wymagania dla instalacji antenowej

- $WFS \leq 1,5$ w wymaganym zakresie częstotliwości,
- antena dookólna o wzmacnieniu ≥ 0 dBi,
- dopuszczalna moc maksymalna nie mniej niż 20W,
- polaryzacja pionowa.

4.7.1.22 Radiotelefon biurkowy TETRA

a) wymagania ogólne:

wymagania ogólne takie same jak dla radiotelefonu przewoźnego.

b) wymagania funkcjonalne:

- wymagania funkcjonalne takie same jak dla radiotelefonu przewoźnego.

c) wymagania sprzętowe:

- wbudowany głośnik w podstawie lub module wyświetlacza,
- mikrofon biurkowy z przyciskiem PTT,
- nożny przycisk nadawania,
- przewód zasilający DC
- zasilacz sieciowy 230V AC do pracy buforowej z akumulatorem – czas podtrzymania co najmniej 8h (w trybie pracy 5/5/90),

d) wymagania dla instalacji antenowej:

- antena dookólna - zależnie od projektu lokalizacyjnego, wymaga się użycie anten o wzmacnieniu ≥ 3 dBd,
- $WFS \leq 1,5$ w wymaganym zakresie częstotliwości,
- dopuszczalna moc maksymalna nie mniej niż 20W,
- polaryzacja pionowa,

4.7.1.23 Radiotelefon biurkowy TETRA ze sterowaniem

a) wymagania ogólne:

- połączenie modułu biurkowego i modułu N/O, realizowane z użyciem interfejsu sieciowego TCP/IP RJ-45, bez konieczności połączenia z zewnętrzną siecią
- pozostałe parametry techniczne ogólne takie same jak dla radiotelefonu przewoźnego.

b) wymagania funkcjonalne:

- wymagania funkcjonalne takie same jak dla radiotelefonu biurkowego.

c) wymagania sprzętowe:

- moduł biurkowy z wbudowanym głośnikiem:

- mikrofon biurkowy z przyciskiem PTT,
- nożny przycisk nadawania,
- przewód zasilający DC
- moduł N/O musi stanowić zwartą konstrukcję wyposażoną zgodnie z rozwiązaniem przyjętym przez wykonawcę,

d) wymagania dla instalacji antenowej:

- wymagania dla instalacji antenowej takie same jak dla terminala biurkowego.

4.7.2 DMR

W wybranych lokalizacjach eksploatowany jest system analogowo-cyfrowy DMR, który posiada również możliwości koniecznego do wycofania systemu łączności analogowej. Rozwiązania DMR pełnią w Policji jedynie rolę uzupełniającą w stosunku do systemu TETRA. Rozwiązania DMR mogą być wdrażane jedynie w przypadku braku możliwości lub znacznych utrudnień we wdrażaniu systemu TETRA przy każdorazowym uzyskaniu zgody od Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji.

4.7.2.1 Stacja retransmisyjna DMR

a) ogólne cechy użytkowe:

- praca w standardach: cyfrowym ETSI TS 102 361 oraz analogowym; w trybach simpleks/duosimpleks, duplex
- złącze akcesoriów na obudowie umożliwiające podłączanie dodatkowych urządzeń,
- złącze umożliwiające programowanie stacji oraz transmisję danych zgodną ze standardem USB,
- programowalny adres IP,
- przypisany adres sprzętowy (MAC adres),
- zabezpieczenie hasłem przed odczytem parametrów konfiguracyjnych ze stacji retransmisyjnej,
- obsługa transmisji maskowanych i jawnych,
- zabezpieczenie przepięciowe i przeciw odwrotnemu podłączeniu biegunów zasilania,
- automatyczne ładowanie „on-line” baterii akumulatorów zasilania rezerwowego,
- automatyczne, bezzwłoczne przełączenie z zasilania sieciowego na rezerwowe i odwrotnie, zapewniające ciągłą pracę,
- automatyczne zabezpieczenie baterii przed nadmiernym rozładowaniem.

b) parametry techniczne

- minimalny zakres częstotliwości pracy 148 +174 MHz,
- maksymalna dopuszczalna odchyłka częstotliwości kanału ± 2 ppm,
- czułość analogowa odbiornika lepsza niż 0,4 μ V dla SINAD 20 dB oraz 0,3 μ V dla SINAD 12 dB,

- kodowa blokada szumów (CTCSS) wybierana programowo na dowolnym kanale analogowym z możliwością zaprogramowania dowolnego kodu z zakresu 67÷255 Hz (programowana ze skokiem 0,1 Hz),
- retransmisja tonów CTCSS,
- czułość cyfrowa 5% BER/0,3 μ V,
- modulacja na kanale analogowym: częstotliwości (11K0F3E),
- modulacja na kanale cyfrowym: 2 szczelinowa TDMA (7K60FXD dane, 7K60FXW dane i głos),
- odporność na intermodulacje ≥ 70 dB,
- tłumienie emisji niepożądanych ≥ 70 dB,
- selektywność sąsiedniokanałowa ≥ 60 dB dla kanału 12,5 kHz,
- programowalny odstęp sąsiedniokanałowy 12,5 kHz,
- praca na dowolnym z co najmniej 16 zaprogramowanych kanałów,
- praca z dużą lub małą mocą fali nośnej nadajnika programowana w zakresie 1-25 W,
- programowe ograniczenie czasu nadawania w granicach od 15 do 480 s ze skokiem 15 s,
- protokół cyfrowy zgodny z ETSI TS102 361,
- zasilanie sieciowe 230 V \pm 10 %, 50 Hz,
- minimalny zakres temperatury pracy od -30°C do +60°C.

c) wymagania uzupełniające

- metody pomiarów i parametry radiowe nie ujęte w niniejszych wymaganiach muszą być zgodne z normami: ETSI EN 300 086, ETSI EN 300 113, ETSI EN 102 361-2,
- wymagania dotyczące kompatybilności elektromagnetycznej muszą być zgodne z normami: ETSI EN 301 489-1 i ETSI EN 301 489-5,
- wymagania odnośnie bezpieczeństwa urządzeń nadawczych muszą być zgodne z normą EN 60950-1.

4.7.2.2 Radiotelefon przewoźny DMR

a) ogólne cechy użytkowe

- praca w standardach: cyfrowym ETSI TS 102 361 oraz analogowym; w trybach simpleks/duosimpleks,
- możliwość zaprogramowania min. 250 kanałów z możliwością podziału na strefy,
- czytelny wyświetlacz z matrycą punktową i podświetlaniem (min. 2 wiersze), umożliwiający wizualizację odbieranych i wysyłanych wywołań oraz poziomu sygnału w trybie cyfrowym,
- programowanie wyświetlanej nazwy kanału – min. 14 znaków,
- praca z dużą lub małą mocą fali nośnej nadajnika, programowana indywidualnie dla każdego kanału,
- programowe ograniczanie czasu nadawania,
- możliwość skanowania kanałów analogowych z kanału cyfrowego oraz użytkowników, grup i kanałów cyfrowych z kanału analogowego,
- możliwość wysyłania i odbierania wiadomości tekstowych,

- wizualna sygnalizacja (np. diodowa) stanów pracy radiotelefonu, w tym: wywołań, skaningu i stanów monitorowania,
- wbudowany odbiornik GPS,
- wywołanie indywidualne, grupowe, alarmowe oraz okólnikowe (wszystkich) w trybie cyfrowym z identyfikacją na wyświetlaczu abonenta wywołującego i sygnalizacją akustyczną (z możliwością wyłączenia sygnalizacji akustycznej),
- programowalny adres IP radiotelefonu,
- radiotelefon musi posiadać poniższe funkcje sygnalizacji:
 - o zdalne sprawdzenie obecności radiotelefonu w sieci,
 - o zdalny monitoring,
 - o zdalne zablokowanie radiotelefonu,
 - o zdalne odblokowanie radiotelefonu.
- kodowa blokada szumów CTCSS wybierana programowo na dowolnym kanale analogowym,
- możliwość maskowania korespondencji w trybie cyfrowym,
- możliwość utworzenia min. 16 kluczy kodowych i przypisywania ich do kanałów,
- możliwość pracy w systemie cyfrowym z wieloma urządzeniami retransmisyjnymi pracującymi na tej samej parze częstotliwości, z możliwością rozróżnienia urządzeń retransmisyjnych,
- sterowanie MENU dedykowanymi do tego celu przyciskami, oraz dodatkowo min. 4 programowalne przyciski,
- wybór kanałów – przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- regulacja głośności przełącznikiem obrotowym lub dedykowanymi do tego celu przyciskami,
- złącze akcesoryjne - umożliwiające programowanie radiotelefonu i transmisję danych zgodną ze standardem USB, podłączenie dodatkowego głośnika i mikrofonu, przycisku nadawania, itp.,
- zabezpieczenie przepięciowe i przed odwrotnym podłączeniem biegunów zasilania,
- gniazdo antenowe VHF typ BNC, gniazdo do anteny zewnętrznej GPS,
- wbudowany wewnętrzny głośnik,
- możliwość programowego tworzenia listy kontaktów (książki adresowej)
 - wywołań indywidualnych w trybie cyfrowym,
- menu radiotelefonu w języku polskim.

b) parametry techniczne:

- pasmo częstotliwości pracy 148÷174 MHz,
- modulacja na kanale analogowym: częstotliwości (11K0F3E),
- modulacja na kanale cyfrowym: 2 szczelinowa TDMA (7K60FDX dane, 7K60FXB dane i głos),
- odstęp międzykanałowy - 12,5 kHz,
- zasilanie stałoprądowe 13,2 V $\pm 20\%$ minus na masie z zabezpieczeniem przepięciowym i przed odwrotnym podłączeniem biegunów zasilania,
- moc wyjściowa fali nośnej nadajnika programowana w całym zakresie częstotliwości od 1 W do 25 W (tylko w trybie serwisowym),

- możliwość ustawienia dwóch poziomów mocy (moc niska, moc wysoka) na dowolnym kanale,
- maksymalna dopuszczalna dewiacja częstotliwości $\pm 2,5$ kHz, dla odstępu 12,5 kHz,
- stabilność częstotliwości ± 2 ppm,
- charakterystyka pasma akustycznego (+1, -3 dB),
- łączne zniekształcenia modulacji $\leq 5\%$, przy 1 kHz, dewiacja 60% wartości maksymalnej,
- odstęp od zakłóceń min. 40 dB,
- moc emitowana na kanałach sąsiednich ≤ 60 dB dla odstępu 12,5 kHz,
- wokoder cyfrowy,
- protokół cyfrowy zgodny z ETSI TS102 361,
- czułość analogowa nie gorsza niż $0,35 \mu\text{V}$ przy SINAD wynoszącym 12 dB,
- czułość cyfrowa 5% BER/ $0,3 \mu\text{V}$,
- współczynnik zawartości harmoniczných $\leq 5\%$, przy 1 kHz, dewiacja 60% wartości maksymalnej,
- charakterystyka pasma akustycznego (+1, -3 dB),
- selektywność sąsiedniokanałowa min. 60 dB dla odstępu 12,5 kHz,
- tłumienie sygnałów niepożądanych ≥ 70 dB dla odstępu 12,5 kHz,
- moc wyjściowa akustyczna dla głośnika wewnętrznego minimum 3 W,
- przydzwiski i szумы nie więcej niż -40 dB dla odstępu 12,5 kHz.

c) środowisko i klimatyczne warunki pracy

- minimalny zakres temperatury pracy N/O $-25^{\circ} \div +55^{\circ}\text{C}$,
- minimalny zakres temperatury pracy anteny samochodowej $-30^{\circ} \div +60^{\circ}\text{C}$,
- klasa odporności na warunki środowiskowe IP 54,
- odporność na przepięcia (ESD) zgodnie z normą IEC 801-2 KV.

d) wymagania uzupełniające

- metody pomiarów i parametry radiowe nie ujęte w niniejszych wymaganiach muszą być zgodne z normami: ETSI EN 300 086, ETSI EN 300 113, ETSI EN 102 361-2,
- wymagania dotyczące kompatybilności elektromagnetycznej muszą być zgodne z normami: ETSI EN 301 489-1 i ETSI EN 301 489-5,
- wymagania odnośnie bezpieczeństwa urządzeń nadawczych muszą być zgodne z normą EN 60950-1.

4.7.2.3 Radiotelefon noszony DMR

a) ogólne cechy użytkowe

- praca w standardach: cyfrowym ETSI TS 102 361 oraz analogowym, w trybach simpleks/duosimpleks,
- możliwość zaprogramowania min. 250 kanałów z możliwością podziału na strefy,
- czytelny wyświetlacz z matrycą punktową i podświetlaniem (min. 2 wiersze), umożliwiający wizualizację odbieranych i wysyłanych wywołań, poziomu sygnału w trybie cyfrowym, stanu naładowania baterii,

- programowanie wyświetlanej nazwy kanału – min. 16 znaków alfanumerycznych,
- praca z dużą lub małą mocą fali nośnej nadajnika, programowana indywidualnie dla każdego kanału,
- programowe ograniczanie czasu nadawania,
- możliwość skanowania kanałów analogowych z kanału cyfrowego oraz użytkowników, grup i kanałów cyfrowych z kanału analogowego,
- możliwość wysyłania i odbierania wiadomości tekstowych,
- wizualna sygnalizacja (np. diodowa) stanów pracy radiotelefonu, w tym: wywołań, skaningu i stanów monitora,
- wbudowany odbiornik GPS,
- wywołanie indywidualne, grupowe, alarmowe oraz okólnikowe (wszystkich) w trybie cyfrowym z identyfikacją na wyświetlaczu abonenta wywołującego i sygnalizacją akustyczną (z możliwością wyłączenia sygnalizacji akustycznej),
- programowalny adres IP radiotelefonu,
- dedykowany łatwo dostępny przycisk sygnału alarmowego.
- radiotelefon musi posiadać poniższe funkcje sygnalizacji :
 - o zdalne sprawdzenie obecności radiotelefonu w sieci,
 - o zdalny monitoring,
 - o zdalne zablokowanie radiotelefonu,
 - o zdalne odblokowanie radiotelefonu.
- kodowa blokada szumów CTCSS wybierana programowo na dowolnym kanale analogowym,
- możliwość maskowania korespondencji w trybie cyfrowym,
- możliwość utworzenia min. 16 kluczy kodowych i przypisywania ich do kanałów,
- sterowanie MENU dedykowanymi do tego celu przyciskami oraz dodatkowo min. 3 programowalne przyciski,
- wybór kanałów – przełącznikiem obrotowym,
- regulacja głośności potencjometrem obrotowym lub dedykowanymi do tego celu przyciskami,
- złącze akcesoryjne: umożliwiające programowanie radiotelefonu i transmisję danych zgodną ze standardem USB, podłączenie dodatkowego mikrofonogłośnika z przyciskiem nadawania itp.,
- 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,
- pełna klawiatura numeryczna,
- wbudowany głośnik,
- menu radiotelefonu w języku polskim.

b) parametry techniczne

- pasmo częstotliwości pracy 148÷174 MHz,
- modulacja na kanale analogowym: częstotliwości (11K0F3E),
- modulacja na kanale cyfrowym: 2 szczelinowa TDMA (7K60FDX dane, 7K60FXE dane i głos),

- odstęp międzykanałowy-12,5/25 kHz,
- maksymalna moc nadajnika 5 W, z możliwością ustawienia dwóch poziomów mocy: poziom niski 1W, poziom wysoki 5 W, programowana w całym zakresie częstotliwości,
- maksymalna dopuszczalna dewiacja częstotliwości $\pm 2,5$ kHz (dla odstępów 12,5 kHz),
- stabilność częstotliwości ± 2 ppm,
- charakterystyka pasma akustycznego (+1,-3 dB),
- łączne zniekształcenia modulacji $\leq 5\%$, przy 1 kHz, dewiacja 60% wartości maksymalnej,
- odstęp od zakłóceń - 40 dB dla odstępów 12,5 kHz,
- moc emitowana na kanałach sąsiednich ≤ 60 dB dla odstępów 12,5 kHz,
- wokoder cyfrowy,
- protokół cyfrowy zgodny z ETSI-TS102 361,
- czułość analogowa nie gorsza niż $0,30 \mu V$ przy SINAD wynoszącym 12 dB,
- czułość cyfrowa 5% BER/ $0,3 \mu V$,
- współczynnik zawartości harmonicznych $\leq 5 \%$, przy 1 kHz, dewiacja 60% wartości maksymalnej i mocy akustycznej 0,5 W,
- charakterystyka pasma akustycznego (+1, -3 dB),
- selektywność sąsiedniokanałowa min. 60 dB dla odstępów 12,5 kHz,
- tłumienie sygnałów niepożądanych ≥ 70 dB dla odstępów 12,5 kHz,
- przydźwięki i szумы nie więcej niż -40 dB dla odstępów 12,5 kHz,
- moc wyjściowa akustyczna dla głośnika wewnętrznego minimum 0,5 W.

c) środowisko i klimatyczne warunki pracy

- minimalny zakres temperatury pracy radiotelefonu $-20^{\circ} \div +60^{\circ} C$ ($-30^{\circ} \div +60^{\circ} C$),
- odporność obudowy na działanie wody na poziomie określonym normą IEC 60529 IP57.

d) wymagania uzupełniające

- metody pomiarów i parametry radiowe nie ujęte w niniejszych wymaganiach muszą być zgodne z normami: ETSI EN 300 086, ETSI EN 300 113, ETSI EN 102 361-2,
- wymagania dotyczące kompatybilności elektromagnetycznej muszą być zgodne z normami: ETSI EN 301 489-1 i ETSI EN 301 489-5,
- wymagania odnośnie bezpieczeństwa urządzeń nadawczych muszą być zgodne z normą EN 60950-1.

4.7.3 System łączności satelitarnej

Usługi w zakresie łączności satelitarnej dla Policji realizowane są za pośrednictwem systemu INMARSAT, który uznaje się wiodącym systemem łączności satelitarnej w Policji, z zastrzeżeniem polegającym na możliwości stosowania innego systemu, zaakceptowanego przez Dyrektora BLi Komendy Głównej Policji.

4.8 Terminale mobilne

4.8.1 Mobilny Terminal Noszony (MTN)

a) wymagania użytkowe:

- procesor z funkcjonalnością skalowania częstotliwości jego pracy, dostosowujący wydajność do aplikacji i obciążenia w celu zwiększenia wydajności i energooszczędności, wielozadaniowy, zapewniający długi czas pracy na baterii,
- pamięć RAM min. 2GB,
- system operacyjny Android w wersji min. 8.0 bądź system operacyjny Microsoft Windows 10 Mobile IoT Enterprise, lub równoważny, w polskiej wersji językowej wraz z bezterminową licencją, dokumentacja w języku polskim,
- dokumentacja w języku polskim,
- zasilacz sieciowy AC (230V 50Hz),
- dwa wymienne akumulatory ładowalne, każdy zapewniający minimum 12 godzin ciągłej pracy, przy włączonym przez 2h ekranie przy jasności 500 NIT's, włączonym GPS, włączonej transmisji danych w standardzie min. LTE, urządzenie wysyła pakiety danych co minimum 15 sekund, 50 odczytów danych z dokumentów za pomocą wbudowanego czytnika,
- 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 min. USB i funkcjonalnością ładowania baterii oraz synchronizowania go z komputerem typu desktop lub laptop
- wymaga się, aby waga urządzenia nie przekraczała 450g,
- wymaga się, aby wymiary nie były większe niż 166 mm x 90 mm x 31 mm,
- kolorowy ekran dotykowy o rozdzielczości minimum 1024x720 pixeli, przekątna ekranu nie mniejsza, niż 4,7",
- ilość kolorów co najmniej 16 mln., możliwość regulacji natężenia podświetlania ekranu, podświetlanie równomierne na całej powierzchni ekranu.
- czytelność ekranu gwarantowana w przypadku intensywnego nasłonecznienia (min. 500NIT's),
- opcjonalny rysik chowane
- slot na kartę SD (dopuszczalny Mini, Micro) obsługujący karty o pojemności min do 64GB,
- przestrzeń na dane min. 32 GB,
- klawiatura wirtualna (ekranowa),
- slot standardowej karty miniSIM/microSIM,
- wbudowany głośnik, wbudowany mikrofon,
- wbudowany optyczny czytnik kodów jedno i dwu wymiarowych wraz z aplikacją/bibliotekami umożliwiającymi 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/ WCDMA/HSDPA/ HSUPA/HSPA+/LTE/LTE+/5G bez blokady typu sim-lock, umożliwiający pracę w sieci każdego krajowego operatora telefonii komórkowej,
- 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 pod wskazany adres sieciowy APN, jak również udostępnienie informacji o położeniu terminala na potrzeby aplikacji pracujących pod kontrolą systemu operacyjnego zainstalowanego w MTN,
- dane o lokalizacji muszą być przekazywane przez moduł GPS poprzez narzędzie (aplikację) następnie do systemów centralnych Policji zgodnie z wykorzystywanym formatem. Terminal musi realizować powyższe funkcjonalności samodzielnie bez udziału operatora.
- urządzenie powinno spełniać normy MIL-STD-810G, w zakresie odporności na: wysoką temperaturę, niską temperaturę, zmiany temperatur - szok temperaturowy, wilgotność powietrza, wibracje, upadek
- znak CE potwierdzający spełnienie zasadniczych wymagań określonych w przepisach wykonawczych do ustawy o systemie oceny zgodności z dnia 30 sierpnia 2004 r. (Dz. U. 2002 r. Nr 166, poz. 1360),

b) pozostałe wymagania:

- Wbudowany czytnik kart RFID, komunikacja na częstotliwości 13,56 MHz, wspierane standardy: ISO/IEC 14443-4 Typ A & B, MIFARE (Classic 1K and 4K, DESFire, MIFARE Plus), NFC forum (tag type 1, 2, 3, 4)
- Wbudowana kamera tylna min. 8 Mpix, wyposażona w lampę doświetlającą LED
- Możliwość wykonywania połączeń głosowych w sieci GSM
- uwierzytelnienie użytkowników w zakresie dostępu do aplikacji KM SWD musi odbywać się poprzez wykorzystywany w Policji serwer uwierzytelniający BTUU,
- oprogramowanie/biblioteka musi umożliwiać przeprowadzenie uwierzytelnienia i autoryzacji użytkownika w BTUU na podstawie hasła użytkownika do konta w LDAP oraz dostęp do jawnych systemów informatycznych w sieci PSTD poprzez dedykowaną aplikację KM SWD,
- mechanizm uwierzytelnienia i autoryzacji musi zapewniać jednoznaczną identyfikację użytkownika, - certyfikaty urządzenia, CUID, SSL muszą znajdować się w obszarze pamięci chronionej,
- terminal musi umożliwiać nawiązanie bezpiecznej sesji SSL/TLS,
- proces uwierzytelnienia zgodny z BTUU z wykorzystaniem serwera Proxy,
- czas logowania do systemu operacyjnego terminala z wykorzystaniem oprogramowania uwierzytelniającego nie może wynosić więcej niż 1 minuta.

4.8.2 Mobilny Terminal Przewoźny (MTP)

a) wymagania użytkowe:

- procesor z funkcjonalności skalowania częstotliwości jego pracy, dostosowujący wydajność do aplikacji i obciążenia w celu zwiększenia wydajności i energooszczędności, wielozadaniowy, zapewniający długi czas pracy na baterii, wydajność w testach Pass Mark, CPU Benchmark na poziomie min. 3000 pkt
- pamięć RAM min. 2GB,
- system operacyjny Microsoft Windows 10 bądź równoważny lub Android w wersji min. 8.0, w polskiej wersji językowej wraz z bezterminową licencją, dokumentacja w języku polskim,
- dokumentacja w języku polskim,
- zasilacz sieciowy AC (230V 50Hz),
- 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,
- akumulator o mocy nie mniejszej niż 30Wh
- wymaga się, aby waga urządzenia nie przekraczała 1500g,
- wymaga się, aby wymiary nie były większe niż 300 mm x 200 mm x 30 mm,
- kolorowy ekran dotykowy o rozdzielczości minimum 1280x768 pixeli, przekątna ekranu nie mniejsza, niż 9,8", jasność nie mniejsza niż 350 NIT's,
- ilość kolorów co najmniej 16 mln., możliwość regulacji natężenia podświetlania ekranu, podświetlanie równomierne na całej powierzchni ekranu.
- opcjonalny rysik
- slot na kartę SD (dopuszczalny Mini, Micro),
- przestrzeń na dane min. 32 GB, SSD/eMMC,
- klawiatura wirtualna (ekranowa),
- slot standardowej karty miniSIM/microSIM,
- wbudowany głośnik, wbudowany mikrofon,
- wbudowany modem min. GPRS/EDGE/ WCDMA/HSDPA/ HSUPA/HSPA+/LTE/LTE+/5G bez blokady typu sim-lock, umożliwiający pracę w sieci każdego krajowego operatora telefonii komórkowej,
- 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 pod wskazany adres sieciowy APN, jak również udostępnienie informacji o położeniu terminala na potrzeby aplikacji pracujących pod kontrolą systemu operacyjnego zainstalowanego w MTN,
- 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.
- znak CE potwierdzający że spełnienie zasadniczych wymagań określonych w przepisach wykonawczych do ustawy o systemie oceny zgodności z dnia 30 sierpnia 2004 r. (Dz. U. 2002 r. Nr 166, poz. 1360),

b) pozostałe wymagania:

- Wbudowana kamera tylna min. 8 Mpix, wyposażona w lampę doświetlającą LED
- uwierzytelnienie użytkowników w zakresie dostępu do aplikacji KM SWD musi odbywać się poprzez wykorzystywany w Policji serwer uwierzytelniający BTUU,
- oprogramowanie/biblioteka musi umożliwiać przeprowadzenie uwierzytelnienia i autoryzacji użytkownika w BTUU na podstawie hasła użytkownika do konta w LDAP oraz dostęp do jawnych systemów informatycznych w sieci PSTD poprzez dedykowaną aplikację KM SWD,
- mechanizm uwierzytelnienia i autoryzacji musi zapewniać jednoznaczną identyfikację użytkownika, - certyfikaty urządzenia, CUID, SSL muszą znajdować się w obszarze pamięci chronionej,
- terminal musi umożliwiać nawiązanie bezpiecznej sesji SSL/TLS,
- proces uwierzytelnienia zgodny z BTUU z wykorzystaniem serwera Proxy,
- czas logowania do systemu operacyjnego terminala z wykorzystaniem oprogramowania uwierzytelniającego nie może wynosić więcej niż 1 minuta.
- System operacyjny umożliwiający uruchamianie aplikacji napisanych w technologii Universal Windows Platform (UWP) oraz umożliwiający uruchomienie i działanie aplikacji Klienta Mobilnego SWD, działająca w trybie modern UI, napisanej w technologii Universal Windows Platform (UWP)
- wbudowany port USB min. 2.0
- Temperatury pracy: +5°C - +35°C
- Temperatury przechowywania: -10°C do +55 °C

4.9 Inne systemy

4.9.1 System monitoringu wizyjnego

4.9.1.1 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) bądź obiektyw ze stałą ogniskową,
- szybka głowica (obrot 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.

4.9.1.2 Sieć transmisyjna dedykowana na potrzeby monitoringu

W celu zapewnienia właściwych parametrów transmisyjnych, odporności na zakłócenia i niezawodności systemu, transmisję sygnałów wizyjnych i telemetrycznych wymaga 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.

4.9.1.3 Stanowisko nadzoru i rejestracji

Wymaga 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.

4.9.2 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 radiowej korespondencji analogowej i DMR,
- 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,
- rejestracja korespondencji w standardzie TETRA odbywa się wg. wymagań dla tego systemu.

4.9.3 Policyjny System Wideokonferencyjny (PSW)

PSW jest platformą komunikacji multimedialnej opartą na własnej infrastrukturze serwerowej i grupowych terminalach wideokonferencyjnych funkcjonujących w dedykowanej podsieci IP, wydzielonej w ramach infrastruktury OST 112.

PSW musi posiadać bezpieczny styk z siecią Internet umożliwiający realizację połączeń z terminalami policyjnymi funkcjonującymi w sieci Internet (mobilne terminale wideokonferencyjne) jak i użytkownikami spoza Policji.

System musi być zintegrowany z resortowym systemem łączności telefonicznej oraz systemem telefonii IP w sieci OST 112.

Elementy infrastruktury serwerowej jak i terminale powinny należeć do Policji.

Dopuszcza się podłączanie do PSW terminali i wideokonferencyjnych systemów pozapolicyjnych należących do organów administracji państwowej z zastosowaniem bezpiecznego punktu styku.

System musi:

- umożliwiać zabezpieczenie przed nieuprawnionym dostępem do urządzeń połączeń i zarejestrowanych danych w celu zabezpieczenia przed zmianą konfiguracji i utratą poufności i integralności,
- umożliwiać rozbudowę bez konieczności wymiany istniejących elementów systemu,
- umożliwiać zestawienie połączeń wideokonferencyjnych wraz z przesyłaniem treści z systemami wideokonferencyjnymi instytucji zewnętrznych obsługujących standardy SIP i H323.

4.9.3.1 Wymagania minimalne dla PSW.

Dokument do użytku służbowego

- a) system powinien być spójny i posiadać wbudowane funkcje w zakresie:
 - centralnego zarządzania serwerami, terminalami, użytkownikami, połączeniami,
 - wykrywania oraz diagnozowania błędów i awarii,
 - aktualizacji oprogramowania,
 - zabezpieczania i odtwarzania konfiguracji serwerów oraz terminali,
 - monitorowania bieżących parametrów połączeń i statusu terminali i serwerów,
 - planowania wideokonferencji,
 - rejestracji i udostępniania nagrań,
 - streamingu do sieci wewnętrznej oraz do sieci Internet.
- b) możliwość zastosowania terminali sprzętowych jak i dedykowanego oprogramowania na platformy PC lub urządzenia mobilne,
- c) urządzenia systemu muszą być dostosowane do zasilania napięciem – 230V, 50 Hz.

4.9.3.2 Minimalne wymagane techniczno-użytkowe:

- a) obsługa połączeń wielopunktowych i punkt-punkt ,
- b) jednoczesna obsługa połączeń wideokonferencyjnych w oparciu o protokoły H.320, H.323 i SIP,
- c) możliwość dołączenia do wideokonferencji telefonów w trybie audio,
- d) możliwość dołączenia do wideokonferencji telefonów IP w trybie audio-wideo,
- e) wsparcie dla WebRTC,
- f) obsługa standardów kodowania wideo: H.261, H.263, H.263++, H.264 AVC/SVC,
- g) obsługa standardów kodowania audio: G.711, G.722, G.722.1, ,
- h) obsługa H.239 i BFCP, również w połączeniach kaskadowych,
- i) wsparcie dla IPv4, IPv6,
- j) wsparcie dla IP QoS,
- k) wsparcie dla H.460 NAT/Firewall Traversal (STUNT/TURN/ICE),
- l) obsługa połączeń wideokonferencyjnych w jakości wideo HD 720p 30, Full HD 1080p 60,
- m) transkodowanie w czasie rzeczywistym pomiędzy protokołami audio, protokołami wideo, protokołami sieciowymi, rozdzielczością obrazu,
- n) możliwość konfiguracji wirtualnych pokoi wideokonferencyjnych z zabezpieczeniem przed nieuprawnionym dostępem kodem PIN,
- o) możliwość niezależnego nagrywania minimum 20 wideokonferencji w jakości minimum HD 720p 30 każda,
- p) możliwość integracji z zewnętrznym systemem pamięci masowej,
- q) IVR z funkcją zapowiedzi głosowych rozpoczęcia/zakończenia nagrywania, oraz możliwością dodawania własnych zapowiedzi,
- r) centralna książka adresowa,
- s) integracja z LDAP,
- t) edycja i wyświetlanie komunikatów tekstowych.
- u) funkcje poprawy jakości obrazu w przypadku pogorszenia parametrów sieci transmisyjnej,
- v) zarządzanie serwerami przez http/https przy wykorzystaniu przeglądarki internetowej,
- w) obsługa połączeń wideokonferencyjnych oraz połączeń głosowych z/do sieci ISDN,
- x) konfiguracja systemu musi umożliwiać logiczne wydzielenie grup z możliwością przypisania do nich zasobów sprzętowych (terminale) i licencyjnych na połączenia. Każda z grup powinna posiadać możliwość odrębnego administrowania oraz swobodę dysponowania przypisanymi

zasobami. Administrator całego systemu powinien mieć możliwość zarządzania zasobami wszystkich grup.

4.9.3.3 Elementy składowe terminali sprzętowych:

- a) kodek sprzętowy,
- b) pilot zdalnego sterowania lub inne urządzenie zapewniające zdalne bezprzewodowe sterowanie funkcjami,
- c) monitor/telewizor ze stojakiem lub wieszakiem lub inne urządzenie wyświetlające obraz,
- d) kamera lub zestaw kamer z systemem śledzenia i kadrowania osoby mówiącej,
- e) minimum 2 mikrofony,
- f) niezbędne okablowanie,
- g) terminale sprzętowe powinny być wyposażone w interfejsy sygnałowe audio-wideo stosownie do wymagań użytkowników w zależności od możliwych do wykorzystania innych źródeł sygnałów audio-wideo niż kamera systemowa.
- h) dopuszcza się wyposażenie dodatkowe w postaci terminali w postaci tablic interaktywnych, itp. lub stosowanie terminali specjalnych, np. o podwyższonej odporności na warunki atmosferyczne.

4.9.3.4 Wymagania minimalne dla terminala wideokonferencyjnego

- a) Obsługa połączeń wideo przez sieć IP zgodnie ze standardem H323 i SIP,
- b) nawiązywanie połączeń wideokonferencyjnych z poziomu terminala,
- c) wsparcie dla WebRTC,
- d) obsługa standardów kodowania wideo: H.261, H.263, H.263++, H.264 AVC/SVC,
- e) obsługa standardów kodowania audio: G.711; G.722; G.722.1,,
funkcja redukcji echa,
- f) obsługa H.239 i BFCP, również w połączeniach kaskadowych,
- g) wsparcie dla IPv4, IPv6,
- h) wsparcie dla IP QoS,
- i) wsparcie dla H.460 NAT/Firewall Traversal (STUNT/TURN/ICE),
- j) obsługa połączeń wideokonferencyjnych w jakości wideo HD 720p 30, Full HD 1080p 60,
- k) obsługa formatów 4:3, 16:9,
- l) zabezpieczenia hasłem dostępu do terminala,
- m) zdalna aktualizacja oprogramowania,
- n) ekranowe pełne menu użytkownika w języku polskim,
- o) zarządzanie i konfiguracja terminala przez http/https przy wykorzystaniu przeglądarki internetowej,
- p) zdalne sterowanie funkcjami terminala z pilota lub innego bezprzewodowego urządzenia (np. regulacja siły głosu, nawiązywanie połączeń, sterowanie obiektywem kamery, wyciszenie mikrofonu, włączanie i wyłączanie prezentacji),
- q) podłączenie zewnętrznego źródła obrazu przez dedykowany interfejs fizyczny,
- r) wykrywanie i śledzenie osoby mówiącej (uzależnione od dodatkowego wyposażenia).

Rodzaj i wyposażenie terminali powinno być dobierane do potrzeb użytkownika oraz warunków otoczenia, w którym będą funkcjonowały, w tym wielkości i rozkładu pomieszczeń. W szczególności należy uwzględnić ilość niezbędnych interfejsów audio-wideo, ilość i rodzaj kamer

systemowych, ilość i rodzaj urządzeń wizualizujących oraz wielkość pomieszczeń, przy zachowaniu racjonalnego gospodarowania środkami finansowymi.

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 ukończenie tych urządzeń, muszą pozostać w miejscu ich użytkowania, pod nadzorem użytkownika końcowego lub wyznaczonego służbowego punktu serwisowego.

5.1 Stanowiska dostępne sieci PSTD

Stanowiska dostępne, które służą dostępowi do centralnych systemów Policji, muszą zawierać elementy pozwalające na niezaprzeczalną identyfikację użytkownika przez BTUU za pomocą mechanizmów PKI.

5.1.1 Ogólne wymagania bezpieczeństwa stanowiska dostępowego:

- a) dostęp do BIOS/UEFI musi być zabezpieczony hasłem,
- b) BIOS/UEFI powinien uniemożliwić nieautoryzowane uruchomienie systemu operacyjnego z urządzenia innego, niż wskazano w jego ustawieniach,
- c) sekwencję startową w BIOS/UEFI należy ustawić, tak aby system startował tylko i wyłącznie z dysku twardego, zawierającego system operacyjny, w celu uniemożliwienia startu z innego napędu (wymaga się włączenie opcji SecureBoot). Jednocześnie należy wyłączyć możliwość przeprowadzenia rozruchu komputera przy użyciu innych urządzeń (np. poprzez kartę sieciową, napęd optyczny, port USB itd.),
- d) użytkownik stanowiska dostępowego powinien korzystać z konta z ograniczonymi uprawnieniami, założonego przez administratora lokalnego (nie dotyczy stanowisk wykorzystywanych przez administratorów),
- e) hasła użytkowników muszą składać się przynajmniej z 10 znaków i spełniać wymagania co do złożoności (angielskie duże znaki, małe znaki, niealfanumeryczne, cyfry), maksymalnego okresu ważności - 90 dni, historii haseł - 5 pamiętanych haseł, próg blokady konta - 5 nieudanych prób zalogowania,
- f) stanowisko dostępne musi mieć uaktywniony, zabezpieczony hasłem wygaszacz ekranu, uruchamiany automatycznie po max. 30 minutach bezczynności,
- g) wszystkie partycje dysku należy sformatować w systemie plików NTFS lub równoważnym zapewniającym podobne funkcjonalności,
- h) 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,
- i) zabrania się podłączania Stanowisk Dostępowych do sieci Internet. W przypadku konieczności przeklasyfikowania Stanowiska Dostępowego na SSR, przed podłączeniem takiego stanowiska do sieci Internet należy usunąć wszystkie dane

zapisane na jego dyskach wraz z informacjami o strukturze nośnika danych (w sposób uniemożliwiający odzyskanie danych) oraz dokonać reinstalacji systemu operacyjnego,

- j) przy konfiguracji systemu operacyjnego należy stosować zasady prowadzenia inspekcji oraz ustawień dzienników zdarzeń określonych w Rozdziale 9 *Ogólne zasady konfiguracji sprzętu komputerowego wykorzystywanego w jednostkach Policji (komputery stacjonarne, komputery przenośne)*,
- k) **Szyfrowanie funkcją BitLocker informatycznych nośników danych na stanowiskach dostępowych.** W celu zabezpieczenia informacji kopiowanych na informatyczne nośniki danych włącza się w konsoli gpedit.msc ustawienie „Odmawiaj dostępu do zapisu do dysków wymiennych niechronionych funkcją BitLocker” (Konfiguracja komputera\ Szablony administracyjne\ Składniki systemu Windows\ Szyfrowanie dysków funkcją BitLocker\ Wymienne dyski danych\ Odmawiaj dostępu do zapisu do dysków wymiennych niechronionych funkcją BitLocker\ Włączone).

Naczelnik właściwy ds. łączności/informatyki może w uzasadnionych przypadkach, podjąć decyzję o dopuszczeniu, innych rozwiązań informatycznych zapewniających odpowiedni poziom bezpieczeństwa szyfrowania informacji kopiowanych na informatyczne nośniki danych.

- l) **Ewidencjonowanie podłączanych informatycznych nośników danych w systemie operacyjnym stanowiska komputerowego.** W celu rejestracji numerów seryjnych informatycznych nośników danych podłączanych do stanowiska komputerowego należy „Włączyć” dziennik DriveFrameworks-UserMode (Podgląd zdarzeń/ Dziennik aplikacji i usług/ Microsoft/ Windows/ DriveFrameworks-UserMode/ Działaj) w ustawieniach systemu operacyjnego.

Rejestracja numerów seryjnych informatycznych nośników danych podłączanych do stanowiska komputerowego może być realizowana przy zastosowaniu innych rozwiązań informatycznych rekomendowanych przez komórki właściwe do spraw łączności i informatyki w jednostkach organizacyjnych Policji.

5.1.2 Rodzaje stanowisk dostępowych:

- a) standardowy komputer dostępowy:
 - oprogramowanie identyfikujące użytkownika,
 - elektroniczny czytnik kart mikroprocesorowych
- b) dedykowany i specjalizowany komputer dla dostępu do obszaru informacji niejawnych, zawierający:
 - oprogramowanie identyfikujące sprzęt i użytkownika,
 - elektroniczny czytnik kart mikroprocesorowych,
- c) mobilny Terminal:
 - Przewoźny (MTP),
 - Noszony (MTN).

W lokalizacjach, w których nie istnieje możliwość zapewnienia stałego łącza sieciowego, umożliwiającego dostęp do centralnych systemów Policji, dopuszcza się użytkowanie stanowisk dostępowych, wykorzystujących mobilny dostęp do sieci PSTD przy zastosowaniu kart SIM. Rozwiązanie to może funkcjonować jedynie tymczasowo. Zgodę na uruchomienie i dopuszczenie do eksploatacji takiego stanowiska, wydaje Dyrektor Biura Łączności i Informatyki KGP na czas określony. Stanowisko musi zawierać następujące elementy:

- oprogramowanie identyfikujące użytkownika,
- elektroniczny czytnik kart mikroprocesorowych lub identyfikatora cyfrowego,
- modem lub router umożliwiający transmisję danych przez sieć GSM (z czytnikiem SIM) z wykorzystaniem dedykowanego APN Policji (stanowiącego element bramy SMDB znajdującej się w BLiI KGP),
- oprogramowanie umożliwiające zestawienie szyfrowanej transmisji danych z wykorzystaniem tunelu VPN od stanowiska dostępowego do urządzenia brzegowego w SMDB.

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 BLiI KGP, a za ich publikację odpowiada Naczelnik Wydziału właściwego do spraw utrzymania systemów TI BLiI 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 opisaniem w rozdziale „Oprogramowanie”, w tym dozwolone pakiety oprogramowania biurowego,
- b) stanowiska dostępne muszą być objęte systemem ochrony antywirusowej,
- c) zgodę na instalację innego oprogramowania, niezbędnego dla realizacji zadań służbowych może wydać Dyrektor BLiI 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) 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 BLiI 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.
- b) na komputerach przenośnych z zastrzeżeniem wskazanym w rozdziale 5.1.3 może być zainstalowane oprogramowanie zakupione przez BLiI KGP, komendę wojewódzką Policji / Komendę Stołeczną Policji lub szkołę Policji oraz oprogramowanie dodatkowe na nieodpłatnej licencji, pozwalającej na jego używanie przez podległe jednostki Policji.

5.3 Sprzęt peryferyjny, urządzenia wielofunkcyjne

5.3.1 Urządzenia wielofunkcyjne winny być eksploatowane i skonfigurowane, zgodnie z następującymi wymaganiami:

- 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 (jeżeli interfejs urządzenia pozwala na wprowadzenie np. znaków specjalnych);
- urządzeniom eksploatowanym w sieci, należy przypisywać statyczne adresy IP, dopuszcza się również adresowanie z wykorzystaniem protokołu DHCP (ang. Dynamic Host Configuration Protocol);
- 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 nie może być udostępniana;

- 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;
- w urządzeniu wielofunkcyjnym, które powróciło z naprawy w serwisie zewnętrznym, należy przywrócić ustawienia fabryczne („twardy reset”), a następnie ponownie skonfigurować urządzenie, zgodnie z wymaganiami i potrzebami w miejscu eksploatacji. W ten sam sposób należy postępować z urządzeniami zastępczymi, wydаныmi przez serwis zewnętrzny na czas naprawy. Za wykonanie wyżej wymienionych czynności odpowiadają komórki organizacyjne właściwe w zakresie informatyki i łączności.

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 niniejszym dokumencie, 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 ich odzyskanie.

5.4.2 Użytkowanie prywatnego sprzętu TI podczas realizacji zadań służbowych.

Zabrania się funkcjonariuszom oraz pracownikom Policji, używania prywatnego sprzętu TI (np. komputerów przenośnych, drukarek, aktywnych urządzeń sieciowych), a także prywatnych elektronicznych nośników danych oraz oprogramowania, w celu realizacji zadań służbowych.

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 elektronicznych nośnikach wchodzących w ukończenie urządzeń kontrahenta, zostaną usunięte w sposób uniemożliwiający ich odczytanie),
- b) komputery przenośne oraz wszelkie elektroniczne nośniki danych, 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 elektronicznych nośnikach danych,

- c) dostęp przedstawicieli firm zewnętrznych do systemów policyjnych może odbywać się wyłącznie przy współudziale osoby odpowiedzialnej z Policji,
- d) zdalny dostęp 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. W przypadku przedstawicieli firm zewnętrznych, 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) jakiegokolwiek odstępstwa od powyższych zasad wymagają uzyskania zgody Dyrektora BLiI KGP lub kierownika komórki organizacyjnej jednostki organizacyjnej Policji właściwej do spraw łączności i informatyki.

5.4.4 Użytkowanie sprzętu przekazanego na potrzeby jednostek organizacyjnych Policji

- a) sprzęt TI przekazany na potrzeby jednostki organizacyjnej Policji, na podstawie darowizn, umów przekazania sprzętu, itp., od podmiotów zewnętrznych, musi spełniać wymagania przedstawione w niniejszym dokumencie, w zależności od rodzaju i przeznaczenia urządzeń.
- b) zabrania się funkcjonariuszom oraz pracownikom Policji, wykorzystywania sprzętu przekazanego przez podmioty, bez ich uprzedniego sprawdzenia i skonfigurowania zgodnie z wymaganiami przez administratora technicznego/ lokalnego.
- c) jakiegokolwiek odstępstwa od powyższych zasad wymagają uzyskania pisemnej zgody kierownika komórki organizacyjnej jednostki organizacyjnej Policji właściwej do spraw łączności i informatyki.

Rozdział 6 Wymagania w zakresie oprogramowania stanowisk dostępowych.

6.1 Oprogramowanie stanowiska dostępowego.

Oprogramowanie instalowane na stanowisku dostępowym służące do uwierzytelniania użytkowników w systemach centralnych Policji, w oparciu o spersonalizowaną kryptograficzną kartę mikroprocesorową zawierającą dwa komplety danych w postaci klucza prywatnego i certyfikatu, musi gwarantować spełnienie następujących warunków:

- zarządzanie kontami użytkowników realizuje administrator,
- 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.

6.2 Oprogramowanie systemów operacyjnych

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

- 1) oprogramowanie MS Windows w polskiej wersji językowej, **lub równoważne**, wersje posiadające wsparcie producenta (z wykluczeniem wersji do tzw. zastosowań domowych).
- 2) oprogramowanie na licencji typu „Open Source”, oparte o otwarty kod źródłowy, z rodziny Linux i Unix (wersje posiadające wsparcie techniczne):
- 3) Oprogramowanie „inne” (komercyjne, kupowane na indywidualne potrzeby wynikające z charakteru realizowanych zadań):
 - Apple Mac OS (preinstalowane na komputerach Mac i MacBook), wersje posiadające wsparcie producenta,

6.3 Oprogramowanie biurowe

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

Wykaz standardowych programów obecnie wykorzystywanych w Policji:

- 1) Edytory tekstowe (format domyślny zapisu danych - „.doc”):
 - OpenOffice/LibreOffice Writer,
 - MS Office Word.
- 2) Arkusze kalkulacyjne (format domyślny zapisu - „.xls”):
 - OpenOffice/LibreOffice Calc,
 - MS Office Excel.
- 3) Programy do tworzenia prezentacji (format domyślny zapisu danych - „.ppt”):
 - OpenOffice/LibreOffice 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:
 - OpenOffice/LibreOffice Base
 - 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 (wersje posiadające wsparcie producenta),
 - Internet Explorer/Microsoft Edge,
 - Mozilla Firefox,
 - Opera,
 - Google Chrome,
- 2) Klienci poczty e-mail:
 - Lotus Notes,
 - MS Outlook Express,
 - MS Outlook,
 - Poczta systemu Windows,
 - Mozilla Thunderbird
 - lub inne aktualnie wdrożone w Policji

6.5 Oprogramowanie pozostałe

- 1) Wtyczki i rozszerzenia:
 - ActiveX,
 - Java,
 - Silverlight,
 - lub inne, niezbędne do prawidłowego działania przeglądarek internetowych.
- 2) Programy do nagrywania nośników optycznych:
 - Nero OEM,
 - InfraRecorder, AnyBurn,

- wbudowane oprogramowanie systemowe,
 - lub inne do zastosowań komercyjnych.
- 3) Programy do archiwizacji danych:
- WinRAR,
 - lub inne do zastosowań komercyjnych.
- 4) Oprogramowanie inne niż wymienione w pkt 1) do 3), dostosowane do szczególnych potrzeb wynikających z charakteru realizowanych zadań, np. oprogramowanie Apple Mac OS, najnowsze, stabilne wersje, 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 wraz z aktualizowaną bazą antywirusową.
- 6) **Sterowniki i niezbędne oprogramowanie.** Na Samodzielnych Stanowiskach Roboczych oraz stanowiskach dostępowych musi zostać zainstalowane niezbędne oprogramowanie oraz sterowniki w najnowszej wersji.
- 7) **Oprogramowanie narzędziowe.** Zaleca się administratorom wykorzystywanie oprogramowania do zarządzania środowiskiem stacji roboczych, umożliwiającym zdalne instalowanie poprawek systemowych i aplikacyjnych oraz innych niezbędnych narzędzi.

Rozdział 7 Generalne zasady korzystania ze służbowego sprzętu komputerowego

1. Komputery stacjonarne lub przenośne wydawane są w celu realizacji zadań służbowych.
2. Użytkownik zobowiązany jest do ochrony i nieudostępniania informacji przechowywanych na elektronicznych nośnikach danych osobom do tego nieuprawnionym. Komputery wydawane Użytkownikom są chronione hasłami dostępowymi (BIOS/UEFI, konto administratora). Hasła te są znane tylko i wyłącznie uprawnionym funkcjonariuszom oraz pracownikom Policji.
3. Użytkownik musi posiadać zgodę od przełożonego lub wyznaczonego przez niego pracownika danej komórki organizacyjnej na korzystanie ze sprzętu informatycznego poza miejscem pracy lub pełnienia służby w jednostce organizacyjnej Policji.
4. Każdy komputer posiada konto użytkownika zabezpieczone hasłem. Hasło to składa się z min. 10 znaków i musi zawierać: duże i małe litery, cyfry oraz 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).
5. Użytkownik zobowiązany jest zmienić swoje hasło przy pierwszym logowaniu do systemu.
6. Użytkownik komputera przenośnego zabezpiecza przetwarzane za jego pomocą informacje zapisując je na nośnikach (dysk twardy, pendrive itp.) w postaci zaszyfrowanej. Należy korzystać z funkcji "BitLocker" zintegrowanej z systemami operacyjnymi Windows, lub stosować oprogramowania rekomendowane przez komórki właściwe do spraw łączności i

informatyki w jednostkach organizacyjnych Policji. Wsparcie użytkowników w zakresie posługiwania się tego typu oprogramowaniem winny świadczyć komórki właściwe do spraw łączności i informatyki.

7. 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.
8. Użytkownik jest zobowiązany 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.
9. Zabrania się Użytkownikowi instalowania programów nieposiadających wykupionej licencji lub wykupionych praw użytkowania (wyjątkiem jest darmowe oprogramowanie dopuszczone do użytku w Policji – instaluje administrator).
10. Niedozwolone jest przechowywanie na dyskach twardych komputera oraz innych elektronicznych nośnikach danych, nielegalnych kopii plików zawierających treści, które objęte są prawami autorskimi, treści niezgodnych z prawem oraz nie związanych z wykonywanymi obowiązkami służbowymi.
11. Zabronione jest pozostawianie komputera bez nadzoru, podczas pracy z uruchomionymi programami/aplikacjami. Wymagane jest co najmniej zablokowanie komputera wygaszaczem ekranu z hasłem.
12. Użytkownik zobowiązany jest do korzystania z wygaszacza ekranu z włączoną opcją zabezpieczenia hasłem. Hasło nie może być udostępniane nikomu. Hasło składa się z min. 10 znaków i musi zawierać: duże i małe litery, cyfry oraz znak specjalny (jeżeli umożliwia to wygaszacz ekranu). Czas, po którym uaktywnia się wygaszacz, nie może być dłuższy niż 30 minut.
13. 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. Decyzja może zostać wydana jedynie na czas określony.
14. 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.
15. Zasady korzystania ze służbowego sprzętu komputerowego powinny być komunikowane użytkownikom tego sprzętu. Fakt zapoznania się z tymi zasadami powinien być potwierdzony podpisem użytkownika.
16. Użytkownik jest zobowiązany do należytej dbałości o powierzony mu sprzęt.
17. Konta użytkowników zwolnionych/przeniesionych do innej jednostki/komórki organizacyjnej Policji, są blokowane przez administratora technicznego (po uzyskaniu informacji od bezpośredniego przełożonego użytkownika) na okres 6 miesięcy po tym okresie konto zostaje usunięte z systemu operacyjnego. Konta użytkowników, zawieszonych w czynnościach służbowych/ delegowanych do innej jednostki/ komórki organizacyjnej Policji, są blokowane na okres zawieszenia/ delegowania. W uzasadnionych przypadkach dostęp do

kont i danych, osób zwolnionych/ zawieszonych/delegowanych/przeniesionych mogą uzyskać bezpośredni przełożeni, w porozumieniu z kierownikiem komórki właściwej do spraw łączności i informatyki.

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/UEFI; 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.
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:
 - a. hasła ochrony BIOS/UEFI komputerów;
 - hasła powinny mieć maksymalną długość na jaką pozwala wersja BIOS/UEFI (nie mniej niż 15);
 - dla osób realizujących zadania Administratora i Użytkownika winny być różne;
 - hasła przechowywane w miejscu, które jest zabezpieczone przed dostępem osób trzecich,
 - b. hasła do systemu operacyjnego komputera;
 - dla konta administracyjnego systemu hasło powinno zawierać nie mniej niż 15 (nie więcej niż 64) znaków alfanumerycznych w tym litery duże i małe, cyfry oraz znaki specjalne (takie jak @#!+-%). Zaleca się ustawianie haseł

dłuższych, budowanych w oparciu o całe zdanie. Hasło nie może zawierać w sobie imion, dat urodzenia, nazw jednostek/komórek organizacyjnych Policji, popularnych nazw własnych. Hasła nie można przechowywać w czytelnej formie w bezpośrednim otoczeniu komputera. Wymaga się zmiany hasła przynajmniej raz na 180 dni. W przypadku podejrzenia kompromitacji hasła, należy niezwłocznie je zmienić.

- dla konta użytkownika systemu hasło powinno zawierać nie mniej niż 14 znaków alfanumerycznych w tym litery duże i małe, cyfry oraz znaki specjalne (takie jak @#!+-%). Zaleca się ustawianie hasła dłuższych, budowanych w oparciu o całe zdanie. Hasło nie może zawierać w sobie imion, dat urodzenia, nazw jednostek/komórek organizacyjnych Policji, popularnych nazw własnych. Hasła nie można przechowywać w czytelnej formie w bezpośrednim otoczeniu komputera. Wymaga się zmiany hasła, przynajmniej raz na 180 dni. W przypadku podejrzenia kompromitacji hasła, należy niezwłocznie je zmienić.

c. hasła do systemów baz danych;

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

d. hasła do aplikacji;

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

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

- tak jak w punkcie b, dopuszczając 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. Zaleca się wykorzystywanie menedżera hasła, zabezpieczonego hasłem zawierającym nie mniej niż 15 znaków, zgodnie z lit. b), tiret pierwszy.
10. Zaleca się metodę uwierzytelniania dwuskładnikowego do logowania.
11. Zabrania się wykorzystywania oferowanych przez standardowe oprogramowanie mechanizmów umożliwiających zapamiętywanie hasła.
12. 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.
13. 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, jak również powiadomić bezpośredniego przełożonego.

14. 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, sprzęt typu NAS (Network Attached Storage))

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

9.1 Konfiguracja BIOS/UEFI (Setup)

1. Jeżeli BIOS/UEFI posiada funkcję monitorowania otwarcia obudowy, należy tę funkcję włączyć.
2. Jeżeli BIOS/UEFI posiada funkcję uaktywnienia hasła na włączenie komputera, należy tę funkcję włączyć.
3. Dostęp do ustawień BIOS/UEFI powinien być zabezpieczony hasłem o maksymalnej liczbie znaków na jakie pozwala wersja BIOS/UEFI (nie więcej niż 13). Hasła należy ustawić na wszystkich kontach dostępu do BIOS/UEFI.
4. Hasło musi zawierać małe i duże litery, cyfry i znaki specjalne (!@#\$, itp., jeżeli BIOS/UEFI to umożliwia).
5. Hasło do BIOS/UEFI Administrator przechowuje w sposób uniemożliwiający jego ujawnienie, w zamkniętej kopercie u swojego przełożonego lub w miejscu przez niego wskazanym.
6. Sekwencję startową w BIOS/UEFI 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/UEFI jest możliwa tylko i wyłącznie przez uprawnionego Administratora, po podaniu hasła zabezpieczającego, chroniącego BIOS/UEFI komputera.
8. Obudowa komputera powinna zostać fizycznie zabezpieczona (np. poprzez założenie mini-zamka, plomby, naklejenie naklejki, gilosa) w celu uniemożliwienia bądź wykrycia ewentualnych prób ingerencji.
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 lub inne, należy przeprowadzić tę czynność zgodnie z poniższymi wytycznymi:

1. Należy podjąć próbę odzyskania danych użytkownika;
2. Należy sformatować wszystkie partycje dysku w systemie plików NTFS dla środowiska Windows, lub innym właściwym dla danego systemu operacyjnego;
3. Jako hasło dostępu do konta Administratora należy wpisać 13 znakowe hasło o odpowiedniej złożoności (małe i duże litery, cyfry, oraz 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 10 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. Dane przetwarzane na komputerach przenośnych winny być szyfrowane. W tym celu należy korzystać z funkcji "BitLocker", wbudowanej w systemy operacyjne Windows, bądź stosować inne rozwiązania rekomendowane przez komórki właściwe do spraw łączności i informatyki. Administratorzy zapewniają niezbędne wsparcie Użytkownikom w tym zakresie.
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 BLiI 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 BLiI 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 – 180 dni;
2. Minimalny okres ważności hasła – 1 dzień;
3. Minimalna długość hasła – 14 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	<i>TAK</i>	<i>TAK</i>	Lokalnie lub zdalnie. Przy logowaniu do domeny
zarządzania kontami	<i>TAK</i>	<i>TAK</i>	Tworzenie, zmiana, usunięcie konta użytkownika lub grupy, zmiana nazwy, włączenie/wyłączenie konta użytkownika i zmiana hasła.
Dostępu do usługi katalogowej	<i>NIE</i>	<i>NIE</i>	Nie ma wpływu na nic w stacjach roboczych i member Server
zdarzeń logowania	<i>TAK</i>	<i>TAK</i>	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	<i>NIE</i>	<i>TAK</i>	Dostęp do plików, katalogów, drukarek
zmian zasad	<i>TAK</i>	<i>TAK</i>	Zmiany na prawa Użytkownika lub polityka audytu lub opcje zabezpieczeń użytkownika (opcje hasła)
użycia uprawnień	<i>NIE</i>	<i>TAK</i>	Działania Użytkownika, prawa Użytkownika (zmiana czasu, Administrator przejmuje uprawnienia)
śledzenia procesów	<i>NIE</i>	<i>NIE</i>	Śledzenie programu aktywacji
zdarzeń systemowych	<i>TAK</i>	<i>TAK</i>	Zamykanie lub restart dla stacji komputerowych lokalnych

9.3.4 Ustawienia dzienników zdarzeń

Ustawienia Dziennika Zdarzeń	Wartość Ustawiona
------------------------------	-------------------

Maksymalny rozmiar dziennika aplikacji	20480KB
Maksymalny rozmiar dziennika bezpieczeństwa	20480KB
Maksymalny rozmiar dziennika systemowego	20480KB
Archiwizuj dziennik po zapelnieniu, nie zastepuj zdarzen	

9.3.5 Szyfrowanie funkcją BitLocker informatycznych nośników danych.

W celu zabezpieczenia informacji kopiowanych na informatyczne nośniki danych włącza się w konsoli gpedit.msc ustawienie „Odmawiaj dostępu do zapisu do dysków wymiennych niechronionych funkcją BitLocker” (Konfiguracja komputera\ Szablony administracyjne\ Składniki systemu Windows\ Szyfrowanie dysków funkcją BitLocker\ Wymienne dyski danych\ Odmawiaj dostępu do zapisu do dysków wymiennych niechronionych funkcją BitLocker\ Włączone).

Naczelnik właściwy ds. łączności/informatyki może w uzasadnionych przypadkach, podjąć decyzję o dopuszczeniu, innych rozwiązań informatycznych zapewniających odpowiedni poziom bezpieczeństwa szyfrowania informacji kopiowanych na informatyczne nośniki danych.

9.3.6 Ewidencjonowanie podłączanych informatycznych nośników danych w systemie operacyjnym stanowiska komputerowego

W celu rejestracji numerów seryjnych informatycznych nośników danych podłączanych do stanowiska komputerowego należy „Włączyć” dziennik DriveFrameworks-UserMode (Podgląd zdarzeń/ Dziennik aplikacji i usług/ Microsoft/ Windows/ DriveFrameworks-UserMode/ Działa) w ustawieniach systemu operacyjnego.

Rejestracja numerów seryjnych informatycznych nośników danych podłączanych do stanowiska komputerowego może być realizowana przy zastosowaniu innych rozwiązań informatycznych

9.4 Konfiguracja sprzętu typu NAS (Network Attache Storage)

Administratorzy odpowiedzialni za konfigurację sprzętu typu NAS, powinni kierować się następującymi zasadami/wymaganiami:

- a) zabezpieczenie dostępu do zasobu,
 - użytkownicy zasobu powinni korzystać z indywidualnych kont z ograniczonymi uprawnieniami,
 - hasła użytkowników powinny zostać utworzone zgodnie z rozdz. 8 pt. „Ogólna polityka haseł”,
 - logowanie do zasobu przez przeglądarkę internetową powinno odbywać się za pośrednictwem bezpiecznego połączenia HTTPS, zaleca się (jeżeli oprogramowanie

urządzenia to umożliwia) zastosowanie uwierzytelniania dwuskładnikowego (np. Google Authenticator).

- b) należy zablokować wszystkich kont wbudowanych w system (admin, gość, itp.) – jeżeli oprogramowanie urządzenia posiada taką funkcję,
- c) należy wyłączyć zbędne/nie używane usługi/porty np. Telnet, SSH itp.,
- d) należy na bieżąco aktualizować oprogramowanie sprzętowe (firmware),
- e) należy systematycznie wykonywać kopie zapasowe/kopie migawkowe (snapshot) danych znajdujących się na urządzeniu,
- f) instalacja oprogramowania antywirusowego oraz jego aktualizacja powinna odbywać się minimum raz na kwartał – (ręczna aktualizacja baz sygnatur wirusów),
- g) w celu zapewnienia rozliczalności należy rozszerzyć zakres zbieranych logów systemowych w ustawieniach NAS (id/login użytkownika, data i godzina, czy logowanie zakończyło się sukcesem, do jakiego pliku uzyskano dostęp, jaka czynność została wykonana na pliku) oraz prowadzić ich systematyczną archiwizację (minimum raz na kwartał w pliku np. „Kwartał.Rok.csv”),
- h) w celu zapewnienia poufności zaleca się zastosować szyfrowanie całych wolumenów,
- i) jeżeli urządzenie NAS nie spełnia ww. wymogów należy przeprowadzić szacowanie ryzyka.

Rozdział 10 Zadania Lokalnych Administratorów

Zadania lokalnych administratorów wykonują policjanci/pracownicy komórek łączności i informatyki oraz policjanci/pracownicy komórek organizacyjnych Policji, zgodnie z zakresami obowiązków.

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, uwzględniających wersję programu antywirusowego, adresy IP, lokalizację sprzętu, numery inwentarzowe i seryjne urządzeń oraz dane użytkowników.
12. Zgrywanie danych użytkowników sprzętu, w celu przeinstalowania systemu operacyjnego lub migracji na inny sprzęt.

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 нефunkcjonalnych 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 Wprowadzanie zmian do dokumentu

1. Wnioski o wprowadzenie zmian do niniejszego dokumentu, wraz z uzasadnieniem, należy kierować w formie pisemnej do Dyrektora BŁiI KGP.
2. Dyrektor BŁiI KGP akceptuje bądź odrzuca proponowane zmiany.
3. Zmiany w dokumencie podlegają zatwierdzeniu przez Komendanta Głównego Policji.