Warszawa, dnia środa, 18 lutego 2026 r.

Poz. 26

ZARZĄDZENIE NR 5
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 14 lutego 2026 r.

w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji

Na podstawie art. 7 ust. 1 pkt 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636, 718 i 1366) zarządza się, co następuje:

Rozdział 1
Przepisy ogólne

§ 1. Zarządzenie określa:

1) zasady działania BTUU, w tym jego przeznaczenie, strukturę, sposób administrowania oraz korzystania z zasobów;

2) tryb nadawania uprawnień do dostępu do BTUU;

3) tryb przydzielania oraz postępowania z kartami mikroprocesorowymi, wykorzystywanymi w celu identyfikacji i uwierzytelniania użytkowników podczas logowania się do systemów teleinformatycznych Policji;

4) sposób uwierzytelniania użytkowników Mobilnych Terminali Noszonych oraz Mobilnych Terminali Przewoźnych;

5) tryb nadawania, modyfikowania, cofania oraz ewidencjowania uprawnień do dostępu do Aplikacji do Zarządzania Uprawnieniami oraz do przetwarzania informacji, w tym danych osobowych, w Aplikacji do Zarządzania Uprawnieniami;

6) tryb przyznawania użytkownikom Aplikacji do Zarządzania Uprawnieniami poziomów dostępu do tej aplikacji.

§ 2. Użyte w zarządzeniu określenia i skróty oznaczają:

1) administrator lokalny – policjanta albo pracownika Policji odpowiadającego za prawidłowe funkcjonowanie, eksploatację i zabezpieczenie komponentów systemów łączności oraz informatyki wymagających działań administracyjnych i eksploatacyjnych użytkowanych w jednostce organizacyjnej Policji lub jej komórce organizacyjnej wyznaczonego przez kierownika tej jednostki organizacyjnej Policji lub jej komórki organizacyjnej zgodnie z „Wymaganiami dotyczącymi standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie informatyki i łączności” zatwierdzonymi przez Zastępcę Komendanta Głównego Policji;

2) AP w Szczytnie – Akademię Policji w Szczytnie;

3) AZU – Aplikację do Zarządzania Uprawnieniami;

4) BOA – Centralny Pododdział Kontrterrorystyczny Policji „BOA”;

5) BSWP – Biuro Spraw Wewnętrznych Policji;

6) BTUU – Bezpieczny Tryb Uwierzytelniania Użytkownika;

7) CBŚP – Centralne Biuro Śledcze Policji;

8) CBZC – Centralne Biuro Zwalczania Cyberprzestępczości;

9) certyfikat – zestaw podpisanych cyfrowo danych służących do potwierdzenia tożsamości użytkownika;

10) CLKP – Centralne Laboratorium Kryminalistyczne Policji;

11) dezaktywacja użytkownika – umieszczenie w BTUU informacji o unieważnieniu certyfikatów z KM;

12) hasło – hasło wykorzystywane do autoryzacji użytkowników MTN lub MTP;

13) hasło robocze – tymczasowe, pierwsze hasło nadawane użytkownikowi w BTUU;

14) identyfikator kadrowy – identyfikator kadrowy, o którym mowa w rozdziale 8 zarządzenia nr 53 Komendanta Głównego Policji z dnia 4 grudnia 2023 r. w sprawie Systemu Wspomagania Obsługi Policji (Dz. Urz. KGP poz. 101 oraz z 2025 r. poz. 32);

15) inspektor ds. rejestracji – osobę upoważnioną do wykonywania w PR KGP lub PR czynności polegających na aktywacji, dezaktywacji, recertyfikacji i odblokowaniu KM;

16) KGP – Komendę Główną Policji;

17) KM – kartę mikroprocesorową, umożliwiającą identyfikację i uwierzytelnienie użytkownika poprzez BTUU w systemach teleinformatycznych Policji;

18) KSIP – Krajowy System Informacyjny Policji, o którym mowa w art. 21nb ustawy o Policji;

19) MTN – Mobilny Terminal Noszony, będący komputerem przenośnym komunikującym się z systemami teleinformatycznymi dostępnymi poprzez PSTD z wykorzystaniem bezprzewodowej transmisji danych;

20) MTP – Mobilny Terminal Przewoźny, będący komputerem zainstalowanym w pojeździe, komunikującym się z systemami teleinformatycznymi dostępnymi poprzez PSTD z wykorzystaniem bezprzewodowej transmisji danych;

21) podmioty pozapolicyjne – podmioty pozapolicyjne w rozumieniu § 2 pkt 32 zarządzenia nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji (Dz. Urz. KGP poz. 114, z późn. zm.[1)]);

22) PR – Punkt Rejestracji zlokalizowany w komendzie wojewódzkiej (Stołecznej) Policji, realizujący w szczególności czynności związane z aktywacją, dezaktywacją, recertyfikacją i odblokowaniem KM dla użytkowników pełniących służbę lub zatrudnionych w komendzie wojewódzkiej (Stołecznej) Policji oraz w podległych jej jednostkach organizacyjnych Policji;

23) PR KGP – Punkt Rejestracji zlokalizowany w KGP, realizujący w szczególności czynności związane z aktywacją, dezaktywacją, recertyfikacją i odblokowaniem KM w komórkach organizacyjnych KGP oraz w przypadku użytkowników pełniących służbę lub zatrudnionych w BSWP, BOA, CBŚP, CBZC, CLKP, AP w Szczytnie, szkołach policyjnych oraz w podmiotach pozapolicyjnych;

24) PSTD – wirtualną sieć prywatną VPN, działającą 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 bezpieczny dostęp do systemów teleinformatycznych Policji;

25) recertyfikacja – wygenerowanie i osadzenie na KM certyfikatu na kolejny okres ważności;

26) SWD Policji – System Wspomagania Dowodzenia Policji, o którym mowa w art. 20e ustawy o Policji;

27) system teleinformatyczny Policji – system, zbiór danych lub zestaw zbiorów danych, w którym przetwarza się informacje, w tym dane osobowe, w celu realizacji przez Policję zadań ustawowych, w szczególności:

[1)] Zmiany wymienionego zarządzenia zostały ogłoszone w Dz. Urz. KGP z 2019 r. poz. 120, z 2021 r. poz. 100, z 2022 r. poz. 163, 223 i 232, z 2023 r. poz. 83, z 2024 r. poz. 17 oraz z 2025 r. poz. 70.

a) SWD Policji,

b) elektroniczny zbiór danych dotyczący sprawców wykroczeń, o którym mowa w art. 20f ust. 4 ustawy o Policji,

c) zbiór danych zawierający informacje o wynikach analizy kwasu deoksyrybonukleinowego (DNA), o którym mowa w art. 21a ustawy o Policji,

d) KSIP,

e) systemy, zbiory danych lub zestawy zbiorów danych utworzone na podstawie art. 20 ust. 1g ustawy o Policji;

28) ustawa o Policji – ustawę z dnia 6 kwietnia 1990 r. o Policji;

29) uwierzytelnianie na MTN lub MTP – uwierzytelnianie użytkowników aplikacji Klienta Mobilnego SWD Policji przy pomocy identyfikatora kadrowego;

30) użytkownik – osobę posiadającą uprawnienie do przetwarzania informacji, w tym danych osobowych, w systemach teleinformatycznych Policji z wykorzystaniem KM lub uwierzytelniania na MTN lub MTP;

31) wniosek AZU – wniosek o nadanie, modyfikację lub cofnięcie uprawnień do dostępu do AZU oraz do przetwarzania informacji, w tym danych osobowych, w AZU;

32) WUSIPiK BŁiI KGP – Wydział Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki KGP.

Rozdział 2
Zasady działania BTUU oraz nadawanie uprawnień do dostępu do BTUU

§ 3. 1. BTUU stanowi centralny policyjny system autoryzacji i uwierzytelniania użytkowników, umożliwiający im dostęp do zasobów informacyjnych systemów teleinformatycznych Policji.

2. BTUU składa się z podsystemów pełniących wyspecjalizowane zadania, które wspólnie zapewniają możliwość bezpiecznego, kontrolowanego dostępu użytkowników do systemów teleinformatycznych Policji.

3. W BTUU przetwarza się następujące dane osobowe policjantów i pracowników Policji oraz funkcjonariuszy i pracowników podmiotów pozapolicyjnych posiadających uprawnienie do przetwarzania informacji za pomocą aplikacji do Sprawdzeń i Rejestracji w KSIP dla Podmiotów Pozapolicyjnych, o którym mowa w § 12 ust. 9 zarządzenia nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji:

1) nazwisko i imię;

2) identyfikator kadrowy;

3) numer PESEL;

4) jednostka organizacyjna pełnienia służby lub wykonywania pracy;

5) adres email;

6) informacje o nadanych uprawnieniach i certyfikatach.

4. Dane osobowe przetwarzane w BTUU wykorzystuje się podczas generowania certyfikatu do KM.

5. Zadania administratora, w imieniu Komendanta Głównego Policji, w odniesieniu do informacji, w tym danych osobowych, przetwarzanych w BTUU wykonuje kierownik komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki.

§ 4. 1. Uprawnienia dostępu do BTUU, poprzez przydzielenie odpowiedniej roli administracyjnej, nadaje centralny administrator BTUU, wyznaczony przez kierownika komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki.

2. Nadanie uprawnień dostępu do BTUU następuje na podstawie wniosku zatwierdzonego przez bezpośredniego przełożonego użytkownika. Wniosek sporządza się w dwóch egzemplarzach, a następnie przekazuje do akceptacji do komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki. Pierwszy egzemplarz zaakceptowanego wniosku przechowuje się w komórce organizacyjnej KGP właściwej w sprawach łączności i informatyki. Drugi egzemplarz zaakceptowanego wniosku odsyła się do nadawcy.

3. Do usunięcia uprawnień dostępu do systemu BTUU przepisy ust. 1 i 2 stosuje się odpowiednio.

4. Wzór wniosku o nadanie lub usunięcie uprawnień dostępu do BTUU określa załącznik nr 1 do zarządzenia.

Rozdział 3
Tryb postępowania z kartami mikroprocesorowymi (KM)

§ 5. 1. Aktywacji KM dokonuje się na podstawie wniosku, którego wzór określa załącznik nr 2 do zarządzenia, podpisanego przez:

1) kierownika jednostki organizacyjnej Policji lub jej komórki organizacyjnej – w przypadku wniosków dotyczących użytkowników pełniących służbę lub zatrudnionych w KGP, BSWP, BOA, CBŚP, CBZC, CLKP, AP w Szczytnie, szkołach policyjnych oraz podmiotach pozapolicyjnych;

2) kierownika jednostki organizacyjnej Policji – w przypadku wniosków dotyczących użytkowników pełniących służbę lub zatrudnionych w komendzie wojewódzkiej (Stołecznej) Policji oraz w podległych jej jednostkach organizacyjnych Policji.

2. Wniosek sporządza się w dwóch egzemplarzach, a następnie przekazuje do zatwierdzenia przez:

1) inspektora ds. rejestracji w PR KGP – w przypadku użytkowników, o których mowa w ust. 1 pkt 1;

2) inspektora ds. rejestracji w PR – w przypadku użytkowników, o których mowa w ust. 1 pkt 2.

3. Aktywacji KM dokonuje odpowiednio inspektor ds. rejestracji w PR KGP lub inspektor ds. rejestracji w PR, przez zapisanie w BTUU i w pamięci KM danych niezbędnych do logowania w systemach teleinformatycznych Policji.

4. Aktywowaną KM z kodem PIN oraz z jednym egzemplarzem zatwierdzonego wniosku przekazuje się, w dwóch oddzielnych kopertach, do jednostki organizacyjnej Policji lub jej komórki organizacyjnej, w której użytkownik pełni służbę lub jest zatrudniony. W jednej kopercie umieszcza się zatwierdzony wniosek wraz z KM, natomiast w drugiej kopercie kod PIN w formie koperty utajnionej uniemożliwiającej jego odczytanie przez osobę nieuprawnioną. Użytkownik potwierdza na wniosku własnoręcznym podpisem odebranie aktywowanej KM wraz z kodem PIN.

5. Pierwszy egzemplarz zatwierdzonego wniosku przechowuje się we właściwym PR lub PR KGP. Drugi egzemplarz zatwierdzonego wniosku przechowuje się w jednostce organizacyjnej Policji lub jej komórce organizacyjnej, w której użytkownik pełni służbę lub jest zatrudniony.

6. Ewidencję otrzymanych KM prowadzi się w jednostkach organizacyjnych Policji, w których pełnią służbę lub są zatrudnieni użytkownicy KM.

7. Wzór wniosku o aktywację, dezaktywację, odblokowanie, recertyfikację lub zdalną recertyfikację KM określa załącznik nr 2 do zarządzenia.

§ 6. 1. Recertyfikacji KM dokonuje się na podstawie wniosku, którego wzór określa załącznik nr 2 do zarządzenia, nie wcześniej niż na 30 dni kalendarzowych przed upływem jej ważności.

2. Do wniosku o recertyfikację dołącza się podlegającą recertyfikacji KM.

3. Recertyfikacji KM można dokonać również z wykorzystaniem oprogramowania do zdalnej recertyfikacji KM. W takim przypadku dopuszcza się sporządzenie wniosku w jednym egzemplarzu i przesłanie go drogą elektroniczną do właściwego inspektora ds. rejestracji. Do wniosku nie dołącza się podlegającej recertyfikacji KM.

4. Do recertyfikacji KM przepisy § 5 stosuje się odpowiednio.

§ 7. 1. Dezaktywacji KM dokonuje się na podstawie wniosku, którego wzór określa załącznik nr 2 do zarządzenia.

2. Dezaktywacja KM następuje w przypadku:

1) zmiany danych osobowych użytkownika;

2) zwolnienia ze służby użytkownika lub rozwiązania albo wygaśnięcia stosunku pracy użytkownika;

3) przeniesienia użytkownika do pełnienia służby lub świadczenia pracy w innej jednostce organizacyjnej Policji lub jej komórce organizacyjnej;

4) zmiany zakresu obowiązków użytkownika, polegającej na zaprzestaniu wykonywania przez niego zadań wymagających dostępu do systemów teleinformatycznych Policji;

5) podjęcia decyzji o dezaktywacji KM przez kierownika jednostki organizacyjnej Policji lub jej komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik;

6) utraty lub uszkodzenia KM w stopniu uniemożliwiającym dalsze użytkowanie;

7) likwidacji jednostki organizacyjnej Policji lub jej komórki organizacyjnej, w której użytkownik pełnił służbę lub był zatrudniony.

3. W przypadku utraty KM do wniosku o dezaktywację KM dołącza się notatkę służbową podpisaną przez właściwego przełożonego.

4. Do dezaktywacji KM przepisy § 5 stosuje się odpowiednio.

§ 8. 1. Zablokowanie uprawnień w trybie awaryjnym następuje w przypadku utraty przez użytkownika aktywowanej KM.

2. Użytkownik pełniący służbę lub zatrudniony:

1) w KGP, BSWP, BOA, CBŚP, CBZC, CLKP, AP w Szczytnie, szkole policyjnej lub w podmiocie pozapolicyjnym – niezwłocznie powiadamia o utracie aktywowanej KM dyżurnego Sekcji do Spraw Obsługi Całodobowej WUSIPiK BŁiI KGP,

2) w jednostce organizacyjnej Policji niewymienionej w pkt 1 – niezwłocznie powiadamia o utracie aktywowanej KM dyżurnego właściwej terytorialnie jednostki organizacyjnej Policji

– poprzez przesłanie wniosku o zablokowanie uprawnień w trybie awaryjnym, którego wzór określa załącznik nr 3 do zarządzenia.

3. Wniosek o zablokowanie uprawnień w trybie awaryjnym przekazuje się do realizacji:

1) w dni wolne od służby lub pracy oraz w dni robocze, poza obowiązującym w danej jednostce organizacyjnej Policji czasem służby lub pracy – dyżurnemu Sekcji do Spraw Obsługi Całodobowej WUSIPiK BŁiI KGP;

2) w dni robocze, w obowiązującym w danej jednostce organizacyjnej Policji czasie służby lub pracy – kierownikowi właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej (Stołecznej) Policji właściwej do spraw łączności i informatyki.

4. Dyżurny, o którym mowa w ust. 3 pkt 1, lub kierownik, o którym mowa w ust. 3 pkt 2, na podstawie otrzymanego wniosku o zablokowanie uprawnień w trybie awaryjnym, niezwłocznie blokuje uprawnienia do systemów teleinformatycznych Policji, do których w procesie autoryzacji wykorzystywana jest KM, oraz informuje właściwego inspektora ds. rejestracji o odebraniu uprawnień użytkownikowi.

5. Użytkownik utraconej aktywowanej KM powiadamia o jej utracie również bezpośredniego przełożonego, w formie notatki służbowej opisującej okoliczności zdarzenia.

6. Czynności określone w ust. 4 mogą być wykonywane również przez pełniących całodobowe dyżury dyżurnych komórek organizacyjnych jednostek organizacyjnych Policji właściwych do spraw łączności i informatyki.

§ 9. 1. KM ulega automatycznemu zablokowaniu w przypadku trzykrotnego wprowadzenia błędnego kodu PIN.

2. W przypadku zablokowania KM użytkownik składa wniosek o odblokowanie KM, którego wzór określa załącznik nr 2 do zarządzenia, do którego dołącza się zablokowaną KM.

3. Do odblokowania KM przepisy § 5 stosuje się odpowiednio.

§ 10. 1. Użytkownik:

1) wykorzystuje KM wyłącznie do realizacji zadań służbowych;

2) użytkuje i przechowuje KM w sposób uniemożliwiający wykorzystanie przez osobę nieuprawnioną;

3) nie ujawnia kodu PIN;

4) chroni KM przed zniszczeniem lub utratą;

5) niezwłocznie zwraca KM, w przypadku:

a) uszkodzenia,

b) odnalezienia utraconej KM,

c) określonym w § 7 ust. 1 pkt 1-5 i 7.

2. W przypadkach, o których mowa w ust. 1 pkt 5, KM zwraca się kierownikowi jednostki organizacyjnej Policji lub jej komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik, a następnie przesyła się ją odpowiednio do PR KGP lub do właściwego miejscowo PR. Zwrócone i nieuszkodzone KM mogą być ponownie aktywowane.

3. KGP oraz komendy wojewódzkie (Stołeczna) Policji organizują przechowywanie nieaktywnych KM we własnym zakresie.

4. PR KGP lub administrator lokalny zapewnia fizyczne zniszczenie uszkodzonych KM zgodnie z przepisami zarządzenia nr 26 Komendanta Głównego Policji z dnia 19 lutego 2018 r. w sprawie metod i form brakowania dokumentacji niearchiwalnej w Policji (Dz. Urz. KGP poz. 24, z 2019 r. poz. 76, z 2022 r. poz. 87 oraz z 2023 r. poz. 59).

Rozdział 4
Sposób uwierzytelniania użytkowników MTN oraz MTP

§ 11. Dostęp do systemów teleinformatycznych Policji z MTN lub MTP jest możliwy dla użytkowników, którzy:

1) posiadają uprawnienia umożliwiające dokonywanie sprawdzeń w Systemie Poszukiwawczym Policji w rozumieniu § 2 pkt 49 zarządzenia nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji;

2) mają przypisany w SWD Policji identyfikator MTN lub MTP tożsamy z urządzeniem;

3) na MTN lub MTP nie mają możliwości zmiany identyfikatora;

4) został dla nich utworzony patrol w SWD Policji;

5) logują się w określonym w SWD Policji dniu i godzinach.

§ 12. Przy korzystaniu z MTN lub MTP zabrania się dokonywania instalacji oprogramowania, uruchomiania połączeń z publicznymi sieciami telekomunikacyjnymi zapewniającymi dostęp do Internetu oraz przenoszenia danych.

§ 13. 1. Użytkownik MTN lub MTP otrzymuje hasło robocze, które zmienia przy uwierzytelnieniu na MTN lub MTP.

2. Hasło robocze nadaje się, odblokowuje się i resetuje się na podstawie wniosku zatwierdzonego przez kierownika jednostki organizacyjnej Policji lub jej komórki organizacyjnej, w której użytkownik pełni służbę lub jest zatrudniony. Wniosek sporządza się w dwóch egzemplarzach i przekazuje się do realizacji:

1) dyżurnemu Sekcji do Spraw Obsługi Całodobowej WUSIPiK BŁiI KGP – w przypadku użytkowników pełniących służbę lub zatrudnionych w KGP, BSWP, BOA, CBŚP, CBZC, CLKP, AP w Szczytnie oraz szkołach policyjnych;

2) administratorowi lokalnemu właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej (Stołecznej) Policji właściwej do spraw łączności i informatyki – w przypadku pozostałych użytkowników.

3. W dni wolne od służby lub pracy oraz w dni robocze poza obowiązującym w danej jednostce organizacyjnej Policji czasem służby lub pracy wniosek przekazuje się do pełniących całodobowe dyżury dyżurnych komórek organizacyjnych jednostek organizacyjnych Policji właściwych do spraw łączności i informatyki.

4. W przypadku braku możliwości nadania, odblokowania lub zresetowania hasła w danej jednostce organizacyjnej Policji czynność tę wykonuje dyżurny Sekcji do Spraw Obsługi Całodobowej WUSIPiK BŁiI KGP.

5. Wzór wniosku o nadanie, odblokowanie lub zresetowanie hasła roboczego użytkownika MTN lub MTP określa załącznik nr 4 do zarządzenia.

§ 14. 1. W przypadku utraty MTN lub MTP użytkownik:

1) pełniący służbę lub zatrudniony w KGP, BSWP, BOA, CBŚP, CBZC, CLKP, AP w Szczytnie lub szkole policyjnej niezwłocznie powiadamia o utracie MTN lub MTP dyżurnego Sekcji do Spraw Obsługi Całodobowej WUSIPiK BŁiI KGP, poprzez przesłanie wniosku o:

   a) nadanie, odblokowanie lub zresetowanie hasła roboczego użytkownika MTN lub MTP,

   b) oznaczenie MTN lub MTP jako utraconego i zablokowanie karty SIM w trybie awaryjnym, którego wzór określa załącznik nr 5 do zarządzenia;

2) inny, niż wymieniony w pkt 1 – niezwłocznie powiadamia o utracie MTN lub MTP dyżurnego pełniącej całodobowy dyżur komórki organizacyjnej jednostki organizacyjnej Policji właściwej do spraw łączności i informatyki.

2. Dyżurny, o którym mowa w ust. 1 pkt 1, na podstawie otrzymanych wniosków niezwłocznie usuwa dane z MTN lub MTP, blokuje kartę SIM w trybie awaryjnym oraz resetuje hasło użytkownika MTN lub MTP, poprzez nadanie nowego hasła roboczego.

3. Dyżurny, o którym mowa w ust. 1 pkt 2, niezwłocznie sporządza oba wnioski, o których mowa w ust. 1 pkt 1. Wnioski przekazuje się:

1) w dni wolne od służby lub pracy oraz w dni robocze poza obowiązującym w danej jednostce organizacyjnej Policji lub jej komórce organizacyjnej czasem służby lub pracy – dyżurnemu Sekcji do Spraw Obsługi Całodobowej WUSIPiK BŁiI KGP;

2) w dni robocze, w obowiązującym w danej jednostce organizacyjnej Policji lub jej komórce organizacyjnej czasie służby lub pracy – kierownikowi właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej (Stołecznej) Policji właściwej do spraw łączności i informatyki.

4. Dyżurny lub kierownik, o których mowa w ust. 3, na podstawie otrzymanych wniosków, niezwłocznie usuwa dane z MTN lub MTP, blokuje kartę SIM w trybie awaryjnym oraz resetuje hasło użytkownika MTN lub MTP, poprzez nadanie nowego hasła roboczego.

5. Czynności określone w ust. 2 mogą być wykonywane również przez pełniących całodobowe dyżury dyżurnych komórek organizacyjnych jednostek organizacyjnych Policji właściwych do spraw łączności i informatyki.

6. Użytkownik utraconego MTN lub MTP powiadamia o jego utracie również bezpośredniego przełożonego, w formie notatki służbowej opisującej okoliczności zdarzenia.

§ 15. Użytkownik MTN lub MTP:

1) wykorzystuje MTN lub MTP wyłącznie do realizacji zadań służbowych;

2) użytkuje hasło do MTN lub MTP w sposób uniemożliwiający wykorzystanie przez osobę nieuprawnioną;

3) nie ujawnia hasła do MTN lub MTP;

4) niezwłocznie zmienia hasło do MTN lub MTP w przypadku podejrzenia lub stwierdzenia jego ujawnienia;

5) chroni MTN lub MTP przed zniszczeniem lub utratą;

6) regularnie, nie rzadziej niż raz na 30 dni, zmienia hasło do MTN lub MTP.

Rozdział 5
Procedura nadawania, modyfikacji, cofania oraz ewidencjowania uprawnień do dostępu do AZU oraz do przetwarzania informacji, w tym danych osobowych w AZU, oraz przyznawania użytkownikom poziomów dostępu do AZU

§ 16. AZU jest narzędziem elektronicznym wspierającym realizację procesów związanych z nadawaniem, zmianą lub cofnięciem uprawnień użytkowników do przetwarzania informacji w systemach teleinformatycznych Policji w PSTD.

§ 17. AZU jest narzędziem do sterowania procesem i logiką wprowadzania oraz zatwierdzania wniosków o nadanie, zmianę oraz cofnięcie uprawnień do przetwarzania informacji w systemach teleinformatycznych Policji, zgodnie z procedurą nadawania, zmiany oraz cofania uprawnień do przetwarzania informacji w tych systemach określoną w przepisach regulujących ich funkcjonowanie.

§ 18. 1. W AZU rejestruje się każdą operację związaną z nadaniem, zmianą lub cofnięciem uprawnień do przetwarzania informacji w systemach teleinformatycznych Policji.

2. W AZU przetwarza się następujące dane osobowe użytkownika:

1) imię i nazwisko;

2) numer PESEL;

3) identyfikator kadrowy;

4) nazwę jednostki organizacyjnej Policji, w której pełni służbę lub jest zatrudniony użytkownik.

3. Informacje, o których mowa w ust. 2 pkt 3 i 4, są pobierane przez AZU z Systemu Wspomagania Obsługi Policji, o którym mowa w zarządzeniu nr 53 Komendanta Głównego Policji z dnia 4 grudnia 2023 r. w sprawie Systemu Wspomagania Obsługi Policji.

4. Zadania administratora, w imieniu Komendanta Głównego Policji, w odniesieniu do informacji, w tym danych osobowych, przetwarzanych w AZU wykonuje kierownik komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki.

§ 19. 1. Zakres uprawnień dostępu do AZU jest uzależniony od roli i obowiązków użytkownika.

2. Administratorem centralnym AZU jest policjant lub pracownik Policji wyznaczony przez kierownika komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki, który:

1) utrzymuje aktualność słowników AZU i parametrów konfiguracyjnych AZU na poziomie centralnym;

2) zakłada konta administratorów jednostek w AZU oraz konfiguruje administratorom jednostek w AZU pracę na rzecz jednostek organizacyjnych Policji, w zakresie właściwości terytorialnej;

3) ma dostęp do wszystkich jednostek organizacyjnych Policji wprowadzających wnioski AZU oraz wszystkich funkcjonalności AZU;

4) zarządza użytkownikami AZU na poziomie centralnym.

3. Administratorem jednostki w AZU jest policjant lub pracownik Policji wyznaczony przez kierownika jednostki organizacyjnej Policji do zarządzania użytkownikami w danej jednostce organizacyjnej Policji. Ma on możliwość obsługiwania kilku jednostek organizacyjnych Policji w przypadku skonfigurowania mu pracy na rzecz tych jednostek przez administratora centralnego AZU.

4. Zatwierdzającym w AZU jest policjant lub pracownik Policji zatwierdzający wnioski składane przez użytkowników z podległych jednostek organizacyjnych Policji w zakresie dostępu do systemów teleinformatycznych Policji, na podstawie przepisów regulujących ich funkcjonowanie.

5. Weryfikującym w AZU jest policjant lub pracownik Policji, który weryfikuje pod względem merytorycznym zakres wnioskowanych uprawnień dla użytkownika w zakresie dostępu do systemów teleinformatycznych Policji.

6. Przełożonym w AZU jest policjant lub pracownik Policji występujący o nadanie, zmianę lub cofnięcie uprawnień użytkowników w zakresie dostępu do systemów teleinformatycznych Policji na podstawie przepisów regulujących ich funkcjonowanie.

7. Wprowadzającym w AZU jest policjant lub pracownik Policji uprawniony przez administratora jednostki w AZU do generowania i wprowadzania do AZU wniosków w zakresie dostępu do systemów teleinformatycznych Policji składanych przez użytkowników z podległych jednostek organizacyjnych Policji.

8. Archiwizatorem w AZU jest policjant lub pracownik Policji zarządzający danymi archiwalnymi AZU.

9. Recenzentem w AZU jest policjant lub pracownik Policji, który ma dostęp do ewidencji wniosków oraz historii nadanych, zmienionych i cofniętych uprawnień dostępu do systemów teleinformatycznych Policji, zgodnie z przepisami regulującymi ich funkcjonowanie.

10. Audytorem w AZU jest policjant lub pracownik Policji odpowiadający za monitorowanie w AZU aktywności użytkowników oraz rejestrowanie i śledzenie operacji wykonywanych na danych.

11. Wykonującym w AZU jest policjant lub pracownik Policji uprawniony przez administratora jednostki w AZU do nadawania uprawnień użytkownikom z podległych jednostek organizacyjnych Policji po weryfikacji poprawności złożonego i zatwierdzonego wniosku.

12. Potwierdzającym wykonanie w AZU jest policjant lub pracownik Policji potwierdzający wykonanie operacji nadania, modyfikacji lub cofnięcia uprawnień dostępu do systemów teleinformatycznych Policji, zgodnie z przepisami regulującymi ich funkcjonowanie.

13. Uprawnienia wynikające z ról w aplikacji AZU można łączyć. Użytkownik może pełnić więcej niż jedną rolę w AZU.

§ 20. Kierownik komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki wyznacza administratora centralnego AZU.

§ 21. Kierownicy komórek organizacyjnych KGP, komendanci wojewódzcy (Stołeczny) Policji, Komendant BSWP, Komendant CBŚP, Komendant CBZC, dowódca BOA, Dyrektor CLKP, Komendant-Rektor AP w Szczytnie oraz komendanci szkół policyjnych lub ich zastępcy wyznaczają w podległych jednostkach organizacyjnych Policji lub komórkach organizacyjnych KGP:

1) administratora jednostki w AZU;

2) zatwierdzającego w AZU;

3) weryfikującego w AZU;

4) recenzenta w AZU;

5) audytora w AZU;

6) wykonującego w AZU;

7) potwierdzającego wykonanie w AZU.

§ 22. Kierownik jednostki organizacyjnej Policji lub komórki organizacyjnej, w której pełni służbę policjant lub jest zatrudniony pracownik Policji, będący użytkownikiem, wyznacza:

1) wprowadzającego w AZU;

2) archiwizatora w AZU.

§ 23. 1. Uprawnienia do przetwarzania informacji, w tym danych osobowych, w AZU nadaje się na pisemny wniosek kierownika jednostki organizacyjnej Policji lub jej komórki organizacyjnej, w której pełni służbę policjant lub jest zatrudniony pracownik Policji, którego wniosek dotyczy.

2. Wniosek AZU przysyła się w dwóch egzemplarzach do:

1) administratora centralnego AZU – w przypadku policjantów lub pracowników Policji, którzy zostali wyznaczeni do pełnienia roli administratora jednostki w AZU;

2) właściwego terytorialnie administratora jednostki w AZU – w przypadku policjantów i pracowników Policji, którzy zostali wyznaczeni do pełnienia roli:

   a) zatwierdzającego w AZU,

   b) weryfikującego w AZU,

   c) przełożonego w AZU,

d) wprowadzającego w AZU,

e) archiwizatora w AZU,

f) recenzenta w AZU,

g) audytora w AZU,

h) wykonującego w AZU,

i) potwierdzającego wykonanie w AZU.

3. Wniosek AZU, zweryfikowany przez administratora centralnego AZU lub administratora jednostki w AZU, podlega niezwłocznej realizacji. Wnioski niezrealizowane z powodu braków formalnych zwraca się wnioskodawcy.

4. Wzór wniosku AZU określa załącznik nr 6 do zarządzenia.

§ 24. 1. Kierownicy jednostek organizacyjnych Policji i kierownicy komórek organizacyjnych, o których mowa w § 22 i § 23:

1) dokonują na bieżąco weryfikacji nadanych uprawnień do dostępu do AZU oraz do przetwarzania informacji, w tym danych osobowych, w AZU w zakresie zgodności posiadanych uprawnień z realizowanymi zadaniami służbowymi oraz zgodności faktycznego zakresu przetwarzania informacji, w tym danych osobowych, w AZU z uprawnieniami wynikającymi z pełnionej roli w AZU;

2) składają wniosek o odpowiednią modyfikację zakresu nadanych uprawnień do dostępu do AZU oraz do przetwarzania informacji, w tym danych osobowych, w AZU, jeżeli nastąpi zmiana zakresu lub rodzaju czynności służbowych realizowanych przez uprawnionego policjanta lub pracownika Policji;

3) składają wniosek AZU o cofnięcie nadanych uprawnień do dostępu do AZU oraz do przetwarzania informacji, w tym danych osobowych, w AZU, jeżeli uprawniony policjant lub pracownik Policji:

a) został zawieszony w czynnościach służbowych lub w pełnieniu obowiązków,

b) został przeniesiony do pełnienia służby lub wykonywania pracy w innej jednostce organizacyjnej Policji lub jej komórce organizacyjnej,

c) zmarł;

4) składają wniosek AZU o cofniecie uprawnień do dostępu do AZU oraz do przetwarzania informacji, w tym danych osobowych, w AZU przed podpisaniem karty obiegowej w związku ze zwolnieniem policjanta ze służby lub rozwiązaniem umowy o pracę z pracownikiem Policji.

Rozdział 6
Przepisy przejściowe i końcowe

§ 25. Karty mikroprocesorowe z ważnymi certyfikatami przydzielone na podstawie przepisów zarządzenia uchylanego w § 28 zachowują swoją ważność do czasu wystąpienia okoliczności określonych w § 6 i § 7, jednak nie dłużej niż przez 24 miesiące od dnia wejścia w życie niniejszego zarządzenia.

§ 26. Wycofuje się stosowanie kart typu microSD z wbudowanym kryptoprocesorem (KSD) przyznawanych na podstawie przepisów zarządzenia uchylanego w § 28.

§ 27. 1. Wnioski złożone z wykorzystaniem wzorów określonych w załącznikach nr 1 i 3-5 do zarządzenia uchylanego w § 28 i nierozpatrzone przed dniem wejścia w życie niniejszego zarządzenia zachowują ważność do czasu złożenia wniosków z wykorzystaniem wzorów określonych w załącznikach nr 2-4 i 6 do niniejszego zarządzenia, jednak nie dłużej niż przez 12 miesięcy od dnia jego wejścia w życie.

2. Upoważnienia nadane z wykorzystaniem wzoru określonego w załączniku nr 6 do zarządzenia uchylanego w § 28 zachowują ważność do czasu nadania uprawnień z wykorzystaniem wzoru określonego w załączniku nr 6 do niniejszego zarządzenia, jednak nie dłużej niż przez 12 miesięcy od dnia jego wejścia w życie.

§ 28. Traci moc zarządzenie nr 29 Komendanta Głównego Policji z dnia 11 sierpnia 2017 r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych (Dz. Urz. KGP poz. 61, z 2021 r. poz. 38 oraz z 2022 r. poz. 136).

§ 29. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Komendant Główny Policji
z up. I Zastępca Komendanta Głównego Policji

nadinsp. Roman KUSTER

Załączniki do zarządzenia nr 5
Komendanta Głównego Policji
z dnia 14 lutego 2026 r.

Załącznik nr 1

WZÓR

Miejscowość, …… data ……..…… r.

…….

Pieczęć nagłówkowa jednostki organizacyjnej Policji

Egz. Nr……

AKCEPTUJĘ

(Naczelnik WOSI BŁiI KGP lub osoba upoważniona)

Naczelnik
Wydziału Ochrony Systemów Informatycznych
Komendy Głównej Policji

Wniosek o nadanie/usunięcie[1] uprawnień dostępu do BTUU

ID KADRA	PESEL	IMIĘ I NAZWISKO
Jednostka organizacyjna Policji i jej komórka organizacyjna miejsca pracy lub służby użytkownika		

……..…….……..…….

pieczęć i podpis bezpośredniego przełożonego użytkownika

……..……

Sporządził: imię, nazwisko, nr tel.

Data nadania lub usunięcia uprawnień oraz podpis centralnego administratora BTUU

Wyk. w 2 egz.
Egz. nr 1 – centralny administrator BTUU
Egz. nr 2 – nadawca po nadaniu lub usunięciu uprawnień

[1] Niepotrzebne skreślić.

Załącznik nr 2

WZÓR

ZATWIERDZAM
……. …….
(miejscowość, data)

Egz. …….
L. dz. .....

Adresat:
Inspektor ds. rejestracji w PR/PR KGP[1]
……....
Nadawca:
…….....

Wniosek o aktywację/dezaktywację/odblokowanie/recertyfikację/zdalną recertyfikację[1] KM

Lp.	Imię i nazwisko użytkownika	Rodzaj czynności do wykonania[2]	Numer KM[3]	Identyfikacyjny numer kadrowy użytkownika Numer PESEL użytkownika ……..	Nazwa jednostki organizacyjnej Policji i jej komórki organizacyjnej[4]	Numer telefonu sporządzającego wniosek

Załączniki:
……
Uzasadnienie:
……
……

…….……
pieczęć i podpis kierownika jednostki organizacyjnej Policji lub komórki organizacyjnej
(lub osoby przez niego upoważnionej)

Uwagi:
……..…….

[1] Niepotrzebne skreślić.

[2] Wstawić: A – w przypadku aktywacji, D – w przypadku dezaktywacji, R – w przypadku recertyfikacji, RZ – w przypadku recertyfikacji zdalnej, O – w przypadku odblokowania.

[3] W przypadku aktywacji KM rubrykę wypełnia inspektor ds. rejestracji, w pozostałych przypadkach – podmiot wnioskujący.

Data realizacji	Imię, nazwisko i podpis osoby realizującej wniosek

Potwierdzam odbiór KM wraz z kodem PIN.

Jednocześnie oświadczam, że zapoznałem/am[1] się z treścią zarządzenia nr …… Komendanta Głównego Policji z dnia …… *w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji.*

Nr KM	Imię, nazwisko i podpis wydającego	Data odbioru i czytelny podpis użytkownika

Załącznik nr 3

WZÓR

.....

(miejscowość, data)

Sekcja do Spraw Obsługi Całodobowej

Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych

Biura Łączności i Informatyki Komendy Głównej Policji/

Kierownik komórki organizacyjnej Komendy Wojewódzkiej Policji w ……/Komendy Stołecznej Policji[1)] właściwej do spraw łączności i informatyki

Wniosek

o zablokowanie uprawnień użytkowników KM w trybie awaryjnym

Lp.	Imię i nazwisko użytkownika	Identyfikator kadrowy użytkownika Numer PESEL użytkownika

.....

(imię, nazwisko i podpis zgłaszającego: dyżurnego właściwej terytorialnie jednostki organizacyjnej Policji lub użytkownika)

Uwagi:

.....

.....

.....

[1)] Niepotrzebne skreślić

Załącznik nr 4

WZÓR

ZATWIERDZAM
L.dz. .....

.....
(miejscowość, data)

Egz. Nr .....

Adresat:
.....
Nadawca:
.....

Wniosek o nadanie/odblokowanie/zresetowanie[1] hasła roboczego użytkownika MTN/MTP[1]

Lp.	Rodzaj czynności do wykonania[2]	Imię i nazwisko użytkownika[3]	Identyfikator kadrowy użytkownika Numer PESEL użytkownika	Nazwa jednostki organizacyjnej Policji
1.				

Załączniki:
Uzasadnienie:
.....

.....
(pieczęć i podpis kierownika jednostki organizacyjnej Policji lub jej komórki organizacyjnej)

Uwagi: .....

Data realizacji	Imię i nazwisko osoby realizującej wniosek

Oświadczam, że zapoznałam/zapoznałem[1)] się z treścią zarządzenia nr ..... Komendanta Głównego Policji z dnia ..... r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji

Lp.	Imię, nazwisko i podpis realizującego wniosek	Data i czytelny podpis użytkownika

1 Niepotrzebne skreślić.

2 Wstawić: N – w przypadku nadania, Z – w przypadku zresetowania, O – w przypadku odblokowania.

3 Po myślniku wstawić: F – w przypadku funkcjonariusza, P – w przypadku pracownika lub I – w przypadku innej uprawnionej osoby.

Załącznik nr 5

WZÓR

….....

(miejscowość, data)

Sekcja do Spraw Obsługi Całodobowej

Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych

Biura Łączności i Informatyki Komendy Głównej Policji/

kierownik komórki organizacyjnej Komendy Wojewódzkiej Policji

w ...../Komendy Stołecznej Policji[1)]

właściwej do spraw łączności i informatyki

Wniosek

o oznaczenie MTN lub MTP jako utraconego i zablokowanie karty SIM w trybie awaryjnym

Imię, nazwisko oraz identyfikator kadrowy użytkownika zgłaszającego utratę MTN lub MTP	
CUID SWD Policji	
Dokładna data i godzina utraty MTN lub MTP	

.....

(imię, nazwisko i podpis zgłaszającego: dyżurnego właściwej terytorialnie jednostki organizacyjnej Policji lub użytkownika)

Uwagi:

.....

.....

.....

[1)] Niepotrzebne skreślić.

Wypełnia administrator lokalny właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej Policji lub Komendy Stołecznej Policji właściwej do spraw łączności i informatyki lub policjant albo pracownik Sekcji Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji:

IMEI MTN lub MTP	
Nr seryjny MTN lub MTP	
Nr karty SIM do zablokowania	
Imię, nazwisko i podpis dokonującego oznaczenia MTN lub MTP jako utraconego i przesłanie do MTN lub MTP konfiguracji inicjującej czyszczenie danych na urządzeniu	
Data i godzina oznaczenia MTN lub MTP jako utraconego i przesłania do MTN lub MTP konfiguracji inicjującej czyszczenie danych na urządzeniu	
Imię, nazwisko i podpis dokonującego zablokowania karty SIM	
Data i godzina zablokowania karty SIM	

Załącznik nr 6

WZÓR

L.dz. ……..

WNIOSEK O NADANIE, MODYFIKACJĘ LUB COFNIĘCIE

uprawnienia do dostępu do AZU oraz przetwarzania informacji, w tym danych osobowych w AZU

1. Wnoszę o nadanie/modyfikację/cofnięcie* niżej wymienionemu policjantowi/pracownikowi Policji* uprawnienia do dostępu do AZU oraz do przetwarzania informacji, w tym danych osobowych w AZU

2.

☐ **NADANIE**	☐ **COFNIĘCIE**	☐ **MODYFIKACJA**

Powód modyfikacji

……..

3. Dane osoby, której udzielane jest uprawnienie

ID	**Nazwisko**	**Imię**	**e-mail**

4. Wnioskowana rola

Lp.	**Nazwa roli**	**Dostęp**	**Brak dostępu**	**Praca na rzecz jednostki**
1	Administrator jednostki w AZU			
2	Archiwizator w AZU			
3	Audytor w AZU			
4	Przełożony w AZU			

5	Potwierdzający wykonanie w AZU			
6	Recenzent w AZU			
7	Wykonujący w AZU			
8	Wprowadzający w AZU			
9	Zatwierdzający w AZU			
10	Weryfikujący w AZU			

Oznaczyć **KRZYŻYKIEM** „**X**” pola odpowiadające wnioskowanej roli. Pozostałe pola oznaczyć znakiem „ **–** ”. Wszystkie pola muszą być wypełnione. **W przypadku COFNIĘCIA uprawnienia pól <u>nie wypełnia się</u>.**

.....

(wnioskujący: pieczęć, podpis i data)

.....

(podpis i pieczęć nadającego/modyfikującego/cofającego* uprawnienie, data)

OŚWIADCZENIE**

Ja, niżej podpisany/a, zobowiązuję się do zapewnienia bezpieczeństwa informacji oraz danych osobowych przetwarzanych w AZU, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem.

_____

* - niepotrzebne skreślić

** - oświadczenie podpisuje się **tylko w przypadku nadawania lub modyfikacji** uprawnień