Warszawa, dnia 11 września 2017 r.

Poz. 61

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

Na podstawie art. 7 ust. 1 pkt 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2016 r. poz. 1782, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Zarządzenie określa tryb przydzielania oraz postępowania z kartami mikroprocesorowymi, wykorzystywanymi w celu identyfikacji i uwierzytelniania użytkowników podczas logowania się do części jawnej systemów teleinformatycznych Policji oraz sposób uwierzytelniania użytkowników Mobilnych Terminali Noszonych typu 2, zwanych dalej „MTN typu 2".

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) administrator centralny – dyrektora Biura Łączności i Informatyki Komendy Głównej Policji;
2) administrator lokalny – kierownika właściwej do spraw łączności i informatyki, komórki organizacyjnej komendy wojewódzkiej Policji lub Komendy Stołecznej Policji;
3) aktywacja – umieszczenie w bazie danych systemu BTUU informacji o certyfikacie klucza publicznego wygenerowanym na KM lub KSD;
4) BTUU – bezpieczny tryb uwierzytelnienia użytkowników, stanowiący system umożliwiający identyfikację, uwierzytelnianie i autoryzację użytkowników zasobów informacyjnych systemów teleinformatycznych Policji;
5) certyfikat – zestaw podpisanych cyfrowo danych;
6) CUID – identyfikator SWD mobilnego terminala noszonego;
7) dezaktywacja – umieszczenie w bazie danych BTUU informacji o unieważnieniu certyfikatów z KM lub KSD;
8) hasło – hasło w systemie OIM – hasło poczty Cryptomail – hasło wykorzystywane do autoryzacji użytkowników MTN typu 2;
9) hasło „robocze" – tymczasowe, pierwsze hasło nadawane użytkownikowi w LDAP, podlegające zmianie przy pierwszej autoryzacji z MTN typu 2, zgodne z polityką autoryzacji BTUU;
10) identyfikator kadrowy – indywidualny numer identyfikacyjny nadany policjantowi lub pracownikowi Policji przez komórkę organizacyjną Policji właściwą do spraw osobowych;

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2016 r. poz. 1948 i 1955 oraz z 2017 r. poz. 60, 244, 708, 768, 1086 i 1321.

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

12) karta SIM – moduł identyfikacji abonenta, pełniący rolę klucza dostępowego do sieci komórkowej;

13) KM – kartę mikroprocesorową, umożliwiającą identyfikację i uwierzytelnienie użytkownika;

14) kod PIN – przydzielony użytkownikowi kod, przypisany do KM lub KSD;

15) KSD – kartę typu microSD z wbudowanym kryptoprocesorem, umożliwiającą identyfikację i uwierzytelnienie użytkownika mobilnego terminala noszonego;

16) LDAP – Lightweight Directory Access Protocol – protokół przeznaczony do korzystania z usług katalogowych;

17) MTN typu 2 – urządzenia, które do uwierzytelniania nie wykorzystują KM i KSD, korzystające z nowej metody uwierzytelniania użytkowników na urządzeniach opartej o identyfikator i hasło z LDAP;

18) MDM – mobile device management – system zarządzający MTN typu 2;

19) OIM – Oracle Identity Manager – narzędzie do obsługi kont użytkowników;

20) odblokowanie – odblokowanie kodu PIN przypisanego do KM;

21) PKI – Infrastrukturę Klucza Publicznego, stanowiącą system organizacyjno-informatyczny, w którego skład wchodzą urzędy certyfikacyjne, urzędy (punkty) rejestracyjne, użytkownicy certyfikatów klucza publicznego (subskrybenci – użytkownicy systemów teleinformatycznych Policji), oprogramowanie i sprzęt;

22) PR – zlokalizowany w komendzie wojewódzkiej Policji lub Komendzie Stołecznej Policji punkt rejestracji, stanowiący element systemu PKI, realizujący czynności związane z aktywacją, dezaktywacją, recertyfikacją i odblokowaniem KM lub KSD dla użytkowników pełniących służbę lub zatrudnionych w komendzie wojewódzkiej Policji lub Komendzie Stołecznej Policji oraz w podległych jednostkach organizacyjnych Policji;

23) PR KGP – zlokalizowany w Komendzie Głównej Policji punkt rejestracji realizujący czynności związane z aktywacją, dezaktywacją, recertyfikacją i odblokowaniem KM lub KSD dla użytkowników pełniących służbę lub zatrudnionych w Komendzie Głównej Policji, Centralnym Biurze Śledczym Policji, Centralnym Laboratorium Kryminalistycznym Policji, Wyższej Szkole Policji w Szczytnie oraz szkołach policyjnych;

24) recertyfikacja – wygenerowanie na KM lub KSD certyfikatu na kolejny okres ważności;

25) SPP – System Poszukiwawczy Policji;

26) SWD – System Wspomagania Dowodzenia Policji;

27) uwierzytelnianie na MTN typu 2 – uwierzytelnianie użytkowników aplikacji Klienta Mobilnego SWD przy pomocy identyfikatora i hasła z LDAP;

28) użytkownik – funkcjonariusza lub pracownika Policji autoryzowanego do przetwarzania danych w systemach teleinformatycznych Policji z wykorzystaniem KM lub KSD lub uwierzytelniania na MTN typu 2 albo inną osobę uprawnioną w tym zakresie na podstawie odrębnych przepisów;

29) zablokowanie – automatyczne zablokowanie KM lub KSD po trzykrotnym, błędnym wprowadzeniu kodu PIN;

30) zresetowanie hasła – ustawienie nowego hasła „roboczego”, zgodnego z polityką autoryzacji BTUU, realizowane na wniosek, w szczególności w przypadku blokady lub podejrzenia lub stwierdzenia jego ujawnienia.

§ 3. Nadzór nad funkcjonowaniem BTUU sprawują:

1) administrator centralny – w Komendzie Głównej Policji;

2) administratorzy lokalni – w komendach wojewódzkich Policji i Komendzie Stołecznej Policji.

§ 4. 1. Aktywacji KM i KSD dokonuje inspektor ds. rejestracji, poprzez zapisanie w BTUU i pamięci KM lub KSD danych niezbędnych do bezpiecznego logowania w jawnych systemach teleinformatycznych Policji – na podstawie wniosku:

1) kierownika właściwej komórki organizacyjnej – w przypadku wniosków dotyczących policjantów pełniących służbę lub pracowników Policji zatrudnionych w Komendzie Głównej Policji, Centralnym Biurze Śledczym Policji, komendach wojewódzkich Policji, Komendzie Stołecznej Policji, Centralnym Laboratorium Kryminalistycznym Policji, Wyższej Szkole Policji w Szczytnie oraz szkołach policyjnych;

2) kierownika właściwej jednostki organizacyjnej Policji – w przypadku wniosków dotyczących policjantów pełniących służbę lub pracowników Policji zatrudnionych w komendach powiatowych (miejskich, rejonowych) Policji, komisariatach Policji i komisariatach specjalistycznych Policji.

2. Wniosek o aktywację KM lub KSD sporządza się w dwóch jednobrzmiących egzemplarzach, według wzoru określonego w załączniku nr 1 do zarządzenia w przypadku aktywacji KM lub według wzoru określonego w załączniku nr 2 do zarządzenia w przypadku aktywacji KSD, a następnie przekazuje do zatwierdzenia przez:

1) kierownika komórki organizacyjnej Biura Łączności i Informatyki Komendy Głównej Policji spełniającej funkcje PR KGP – w przypadku użytkowników pełniących służbę lub zatrudnionych w Komendzie Głównej Policji, Centralnym Biurze Śledczym Policji, Centralnym Laboratorium Kryminalistycznym Policji, Wyższej Szkole Policji w Szczytnie oraz w szkołach policyjnych;

2) właściwego administratora lokalnego – w przypadku pozostałych użytkowników.

3. Kierownik lub administrator lokalny, o których mowa w ust. 2, przekazuje wniosek o aktywację do PR lub PR KGP w celu realizacji.

§ 5. 1. Po aktywacji KM lub KSD, jeden egzemplarz odpowiednio uzupełnionego wniosku o aktywację przekazuje się zwrotnie kierownikowi komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik KM lub KSD, wraz z KM lub KSD oraz kodem PIN, umieszczonym w oddzielnej kopercie zamkniętej w sposób uniemożliwiający odczytanie kodu PIN przez osobę nieuprawnioną. Drugi egzemplarz wniosku o aktywację przechowuje się we właściwym PR lub PR KGP.

2. KM oraz kod PIN są przekazywane użytkownikowi przez kierownika komórki organizacyjnej, w której użytkownik pełni służbę lub jest zatrudniony.

3. Użytkownik potwierdza na wniosku o aktywację własnoręcznym podpisem odebranie KM wraz z kodem PIN.

4. KSD instaluje się w mobilnym terminalu noszonym pozostającym na stanie ewidencyjnym komórki organizacyjnej, o której mowa w ust. 1. Kody PIN do KSD są przekazywane użytkownikom mobilnych terminali noszonych przez kierowników komórek organizacyjnych, w których użytkownicy pełnią służbę lub są zatrudnieni. Odbiór kodu PIN użytkownik potwierdza własnoręcznym podpisem na wniosku o aktywację.

5. Egzemplarz wniosku o aktywację z potwierdzeniem odbioru KM wraz z kodem PIN lub kodu PIN do KSD jest przechowywany w komórce organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik KM lub KSD.

6. W komórkach organizacyjnych, w których pełnią służbę lub są zatrudnieni użytkownicy KM lub KSD, prowadzi się ewidencję otrzymanych KM i KSD.

§ 6. 1. Do recertyfikacji stosuje się odpowiednio § 4 i 5.

2. Do wniosku o recertyfikację należy dołączyć podlegającą recertyfikacji KM lub KSD.

3. Wniosek o recertyfikację należy przesłać do właściwego PR lub PR KGP nie później niż 30 dni przed terminem wygaśnięcia ważności certyfikatu.

§ 7. 1. KM lub KSD podlegają dezaktywacji 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 komórce lub jednostce organizacyjnej Policji;

4) zmiany zakresu obowiązków, polegającej na zaprzestaniu wykonywania zadań wymagających dostępu do informacji jawnych przetwarzanych w systemach teleinformatycznych Policji;

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

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

7) likwidacji jednostki lub komórki organizacyjnej Policji, w której użytkownik pełni służbę lub jest zatrudniony.

2. W przypadku dezaktywacji z powodu utraty KM lub KSD stosuje się odpowiednio § 4 i § 8 – z tym, że wniosek o dezaktywację sporządza się w jednym egzemplarzu.

3. Wnioski o dezaktywację są przechowywane we właściwym PR lub PR KGP.

§ 8. 1. W przypadku utraty aktywowanej KM lub KSD użytkownik:

1) pełniący służbę lub zatrudniony w Komendzie Głównej Policji, Centralnym Biurze Śledczym Policji, Centralnym Laboratorium Kryminalistycznym Policji, Wyższej Szkole Policji w Szczytnie i w szkole policyjnej – jest obowiązany niezwłocznie powiadomić o utracie dyżurnego Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji, poprzez przesłanie faksem wniosku o zablokowanie uprawnień użytkownika (użytkowników) w trybie awaryjnym, sporządzonego według wzoru określonego w załączniku nr 3 do zarządzenia;

2) inny niż wymieniony w pkt 1 – jest obowiązany niezwłocznie powiadomić o utracie dyżurnego właściwej terytorialnie jednostki organizacyjnej Policji.

2. Dyżurny, o którym mowa w ust. 1 pkt 2, jest obowiązany niezwłocznie sporządzić wniosek o zablokowanie uprawnień użytkownika (użytkowników) w trybie awaryjnym, według wzoru określonego w załączniku nr 3 do zarządzenia.

3. Wniosek, o którym mowa w ust. 2, przekazuje się:

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 Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji – faksem na numer w policyjnej sieci telekomunikacyjnej 72 159 02;

2) w dni robocze, w obowiązującym w danej jednostce organizacyjnej Policji, czasie służby lub pracy – kierownikowi właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej Policji lub Komendy Stołecznej Policji 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, niezwłocznie podejmuje czynności powodujące zablokowanie uprawnień w trybie awaryjnym i przekazuje informację o zablokowaniu operatorowi właściwego terytorialnie PR lub PR KGP, w celu dezaktywacji certyfikatu użytkownika utraconej KM lub KSD.

5. Czynności określone w ust. 4, mogą być wykonywane przez pełniących całodobowe dyżury dyżurnych komórek organizacyjnych Policji właściwych do spraw łączności i informatyki, do których kieruje się wnioski o zablokowanie uprawnień.

6. Użytkownik utraconej KM lub KSD, powiadamia o ich utracie również bezpośredniego przełożonego, notatką służbową opisującą okoliczności zdarzenia.

§ 9. 1. W przypadku trzykrotnego wprowadzenia błędnego kodu PIN, KM lub KSD jest automatycznie blokowana.

2. W przypadku określonym w ust. 1, odblokowanie KM lub KSD następuje na podstawie wniosku o odblokowanie, sporządzonego według wzoru określonego odpowiednio w załączniku nr 1 lub 2 do zarządzenia.

3. Do wniosku o odblokowanie KM lub KSD należy dołączyć zablokowaną KM lub KSD.

§ 10. 1. Użytkownik jest obowiązany do:

1) wykorzystywania KM lub KSD wyłącznie do realizacji zadań służbowych;

2) użytkowania i przechowywania KM lub KSD w sposób uniemożliwiający wykorzystanie przez osobę nieuprawnioną;

3) nieujawniania kodu PIN;

4) ochrony KM lub KSD przed zniszczeniem lub utratą;

5) niezwłocznego zwrotu KM lub KSD:

a) uszkodzonej,

b) uprzednio utraconej a następnie odnalezionej,

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

2. W przypadkach, o których mowa w ust. 1 pkt 5, KM lub KSD powinna być zwrócona kierownikowi komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik tej KM lub KSD, a następnie przesłana kierownikowi komórki organizacyjnej Biura Łączności i Informatyki Komendy Głównej Policji spełniającej funkcję PR KGP lub właściwemu administratorowi lokalnemu. Zwrócone i nieuszkodzone KM lub KSD mogą być ponownie aktywowane.

3. Kierownik lub administrator, o których mowa w ust. 2, jest obowiązany spowodować fizyczne zniszczenie uszkodzonych KM lub KSD, co powinno być udokumentowane protokołem zniszczenia wskazującym rodzaje i numery seryjne zniszczonych KM lub KSD.

§ 11. Komenda Główna Policji, komendy wojewódzkie Policji oraz Komenda Stołeczna Policji, każda we własnym zakresie, organizują przechowywanie nieaktywnych KM i KSD.

§ 12. 1. Każdemu użytkownikowi MTN typu 2, należy nadać hasło „robocze” w LDAP w polu „userpassword”.

2. Hasło „robocze” nadaje się lub resetuje na podstawie wniosku sporządzonego według wzoru określonego w załączniku nr 5 do zarządzenia. Wniosek o nadanie hasła „roboczego” sporządzony w dwóch jednobrzmiących egzemplarzach, zatwierdzony przez kierownika komórki organizacyjnej, w której pełni służbę lub jest zatrudniony użytkownik, przekazuje się do realizacji do administratora lokalnego właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej Policji lub Komendy Stołecznej Policji do spraw łączności i informatyki lub dyżurnego Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji.

3. W dni wolne od służby lub pracy oraz w dni robocze poza obowiązującym, w danej jednostce organizacyjnej Policji, czasem służby lub pracy, wniosek, o którym mowa w ust. 2, przekazuje się do pełniących całodobowe dyżury dyżurnych komórek organizacyjnych Policji właściwych do spraw łączności i informatyki.

4. W przypadku braku możliwości nadania lub zresetowania hasła w danej jednostce organizacyjnej Policji – czynność tę wykonuje dyżurny Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji.

5. Hasło „robocze” użytkownikowi nadaje i przekazuje, w sposób zapewniający poufność, administrator lokalny właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej Policji lub Komendy Stołecznej Policji do spraw łączności i informatyki, a dla pełniących służbę lub zatrudnionych w Komendzie Głównej Policji, Wyższej Szkole Policji w Szczytnie i w szkole policyjnej, pełniący dyżur pracownik Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji.

6. Hasło „robocze” może zostać nadane lub hasło może zostać zresetowane na podstawie wniosku, według wzoru określonego w załączniku nr 5 do zarządzenia:

1) w dni robocze, w obowiązującym w danej jednostce organizacyjnej Policji, czasie służby lub pracy – przez administratora lokalnego właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej Policji lub Komendy Stołecznej Policji do spraw łączności i informatyki, a w Komendzie Głównej Policji przez dyżurnego Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji;

2) w dni wolne od służby lub pracy oraz w dni robocze poza obowiązującym w danej jednostce organizacyjnej Policji, czasem pracy lub służby – przez pełniących całodobowe dyżury dyżurnych komórek organizacyjnych Policji właściwych do spraw łączności i informatyki.

7. Po otrzymaniu hasła „roboczego”, użytkownik obowiązany jest do jego niezwłocznej zmiany. Czynność powinien wykonać na MTN typu 2 niezwłocznie po jego pobraniu do służby. Użytkownik samodzielnie określa kolejne hasło podczas pierwszego logowania do aplikacji.

§ 13. 1. W przypadku utraty MTN typu 2 użytkownik:

1) pełniący służbę lub zatrudniony w Komendzie Głównej Policji, Wyższej Szkole Policji w Szczytnie lub w szkole policyjnej – jest obowiązany niezwłocznie powiadomić o utracie dyżurnego Sekcji do Spraw Obsługi Całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji, poprzez przesłanie faksem „wniosku o oznaczenie w systemie MDM urządzenia jako utracone i przesłanie do urządzenia konfiguracji inicjującej czyszczenie danych na urządzeniu i zgłoszenie do operatora świadczącego usługi transmisji danych zablokowania karty SIM w trybie awaryjnym”, sporządzonego według wzoru określonego w załączniku nr 4 do zarządzenia oraz „wniosek o zresetowanie hasła użytkownika MTN typu 2”, sporządzony według wzoru określonego w załączniku nr 5 do zarządzenia;

2) inny, niż wymieniony w pkt 1 – jest obowiązany niezwłocznie powiadomić o utracie dyżurnego całodobowych komórek organizacyjnych Policji właściwych do spraw łączności i informatyki.

2. Dyżurny, o którym mowa w ust. 1 pkt 1, na podstawie otrzymanego wniosku, niezwłocznie podejmuje czynności powodujące inicjację czyszczenia danych na urządzeniu, a następnie zablokowanie karty SIM w trybie awaryjnym, jak również dokonuje zresetowania hasła użytkownika MTN typu 2, poprzez nadanie nowego hasła „roboczego”.

3. Dyżurny, o którym mowa w ust. 1 pkt 2, jest obowiązany niezwłocznie sporządzić „wniosek o oznaczenie w systemie MDM urządzenia jako utracone i przesłanie do urządzenia konfiguracji inicjującej czyszczenie danych na urządzeniu i zgłoszenie do operatora świadczącego usługi transmisji danych zablokowania karty SIM w trybie awaryjnym” oraz „wniosek o zresetowanie hasła użytkownika MTN typu 2”, według wzorów określonych odpowiednio w załącznikach 4 i 5 do zarządzenia.

4. Wnioski, o których mowa w ust. 3, przekazuje się:

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 Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji – faksem na numer w policyjnej sieci telekomunikacyjnej 72 159 02;

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

5. Dyżurny lub kierownik, o których mowa w ust. 4, na podstawie otrzymanego wniosku, niezwłocznie podejmuje czynności powodujące inicjację czyszczenia danych na urządzeniu, a następnie zablokowanie karty SIM w trybie awaryjnym, jak również dokonuje zresetowania hasła użytkownika MTN typu 2, poprzez nadanie nowego hasła „roboczego”.

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

7. Użytkownik utraconego MTN typu 2, powiadamia o jego utracie również bezpośredniego przełożonego, notatką służbową opisującą okoliczności zdarzenia.

§ 14. Użytkownik MTN typu 2 jest obowiązany do:

1) wykorzystywania go wyłącznie do realizacji zadań służbowych;

2) użytkowania hasła w sposób uniemożliwiający wykorzystanie przez osobę nieuprawnioną;

3) nieujawniania hasła;

4) niezwłocznej zmiany hasła w przypadku podejrzenia lub stwierdzenia jego ujawnienia;

5) ochrony go przed zniszczeniem lub utratą;

6) regularnej zmiany hasła, nie rzadziej niż raz na 30 dni.

§ 15. 1. Hasło użytkownika MTN typu 2 musi składać się z minimum 8 znaków, a maksymalnie 20 znaków.

2. Hasło, o którym mowa w ust. 1, nie może zawierać polskich znaków diakrytycznych. Wybierając hasła użytkownicy powinni kierować się ich jakością oraz:

1) łatwością do zapamiętania i trudnością do odgadnięcia;

2) odstępstwem od prostych skojarzeń i informacji dotyczących użytkownika, w szczególności imienia, nazwiska, nr telefonu lub konta, daty urodzenia, miejsca pracy, identyfikatora kadrowego;

3) wykorzystaniem cyfr, dużych i małych liter, zgodnie z przyjętą polityką autoryzacji BTUU;

4) unikaniem kolejności występowania znaków wynikających z układu na klawiaturze;

5) cykliczną zmianą powtarzania się kolejności poszczególnych znaków.

§ 16. Z MTN typu 2, dostęp do systemów informatycznych możliwy jest dla użytkowników, którzy:

1) mają uprawnienia umożliwiające dokonywanie sprawdzeń w SPP;

2) mają przypisany w SWD terminal o numerze CUID tożsamym z urządzeniem;

3) na urządzeniu nie mają możliwości zmiany numeru CUID;

4) został dla nich utworzony patrol w SWD;

5) logują się w zdefiniowanym w SWD dniu i godzinach.

§ 17. Zabrania się użytkownikowi dokonywania instalacji oprogramowania, uruchomiania połączeń z siecią WiFi oraz przenoszenia danych.

§ 18. KM i KSD przydzielone i wykorzystywane dotychczas na podstawie zarządzenia wymienionego w § 19 zachowują swoją ważność.

§ 19. Traci moc zarządzenie nr 5 Komendanta Głównego Policji z dnia 29 stycznia 2014 r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych (Dz. Urz. KGP poz. 9, 15 i 75).

§ 20. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Komendant Główny Policji

nadinsp. Jarosław SZYMCZYK

Załączniki do zarządzenia nr 29
Komendanta Głównego Policji
z dnia 11 sierpnia 2017 r.

Załącznik nr 1

ZATWIERDZAM

Ldz. .....

……..... (miejscowość, data)

Egz. Nr .....

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

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

Lp.	Imię i nazwisko użytkownika –F/P/I[2]	Rodzaj czynności do wykonania[3]	Nr KM[4]	Identyfikator kadrowy użytkownika Numer PESEL użytkownika	Nazwa jednostki organizacyjnej
1					
2					

Załączniki:[5]
.....
Uzasadnienie:
.....
.....
.....
(pieczęć i podpis kierownika jednostki lub komórki organizacyjnej)

Uwagi:
.....
.....

Data realizacji	Imię, nazwisko i podpis osoby realizującej wniosek

Potwierdzam odbiór KM wraz z kodem PIN.
Jednocześnie oświadczam, że zapoznałam/zapoznałem[1] się z treścią zarządzenia nr ..... Komendanta Głównego Policji z dnia ..... 2017 r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych

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

[1] Niepotrzebne skreślić.
[2] Po myślniku wstawić: „F" – w przypadku funkcjonariusza lub „P" – w przypadku pracownika lub „I" – w przypadku innej uprawnionej osoby.
[3] Wstawić: A – w przypadku aktywacji, D – w przypadku dezaktywacji, R – w przypadku recertyfikacji, O – w przypadku odblokowania.
[4] W przypadku aktywacji KM rubrykę wypełnia inspektor ds. rejestracji, w pozostałych przypadkach - podmiot wnioskujący.
[5] Numery KM.

ZATWIERDZAM **Załącznik nr 2**

L.dz. .....

.....
(miejscowość, data)

Egz. Nr .....

Adresat:
.....

Nadawca:
.....

Wniosek o aktywację/dezaktywację/recertyfikację/odblokowanie[1] KSD

Lp.	Nr ..... KSD[2]	Kontener[3]	Rodzaj czynności do wykonania[4]	Imię i Nazwisko użytkownika –F/P/I[5]	Identyfikator kadrowy użytkownika Numer PESEL użytkownika	Nazwa jednostki organizacyjnej
1						
2						
3						
4						
5						
6						
7						
8						

Załączniki:[6]
Uzasadnienie:
.....

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

Uwagi: .....

Data realizacji	Imię i nazwisko osoby realizującej wniosek

Potwierdzam odbiór kodu PIN do KSD.

Jednocześnie oświadczam, że zapoznałam/zapoznałem[1] się z treścią zarządzenia nr ..... Komendanta Głównego Policji z dnia .....2017 r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych

Imię, nazwisko i podpis wydającego	Data odbioru i czytelny podpis pobierającego użytkownika

[1] Niepotrzebne skreślić.
[2] W przypadku aktywacji KSD rubrykę wypełnia inspektor ds. rejestracji, w pozostałych przypadkach – podmiot wnioskujący.
[3] F1 do F8.
[4] Wstawić: A – w przypadku aktywacji, D – w przypadku dezaktywacji, R – w przypadku recertyfikacji, O – w przypadku odblokowania.
[5] Po myślniku wstawić: „F" – w przypadku funkcjonariusza, „P" – w przypadku pracownika lub „I" – w przypadku innej uprawnionej osoby.
[6] Numer aktywowanej KSD

Załącznik nr 3

.....
(miejscowość, data)

Sekcja do Spraw Obsługi Całodobowej
Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych
Biura Łączności i Informatyki Komendy Głównej Policji/
Kierownik właściwej do spraw łączności i informatyki komórki organizacyjnej
Komendy Wojewódzkiej/Stołecznej/[1] Policji w
.....

Wniosek
o zablokowanie uprawnień użytkowników KM/KSD[1] w trybie awaryjnym

Lp.	Imię i nazwisko użytkownika	Identyfikator kadrowy użytkownika Numer PESEL użytkownika
1		
2		
3		
4		
5		
6		
7		
8		

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

Uwagi:
.....
.....
.....

[1] Niepotrzebne skreślić

Załącznik nr 4

…..
(miejscowość, data)

Sekcja do Spraw Obsługi Całodobowej
Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji/
Kierownik właściwej do spraw łączności i informatyki komórki organizacyjnej
Komendy Wojewódzkiej/Stołecznej/[1] Policji w
.....

Wniosek
o oznaczenie w systemie MDM urządzenia jako utracone i przesłanie do urządzenia konfiguracji inicjującej czyszczenie danych na urządzeniu i zgłoszenie do operatora świadczącego usługi transmisji danych zablokowania karty SIM w trybie awaryjnym.

Imię, nazwisko, identyfikator kadrowy użytkownika zgłaszającego zaginięcie lub kradzież urządzenia	
CUID SWD	
Dokładna data i godzina utraty urządzenia	

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

Uwagi:
.....……...
.....……...
.....……...

Wypełnia administrator lokalny właściwej terytorialnie komórki organizacyjnej komendy wojewódzkiej Policji lub Komendy Stołecznej Policji do spraw łączności i informatyki lub funkcjonariusz lub pracownik sekcji ds. obsługi całodobowej Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych Biura Łączności i Informatyki Komendy Głównej Policji:

IMEI urządzenia	
Nr seryjny urządzenia	
Nr karty SIM do zablokowania	
Imię, nazwisko i podpis dokonującego oznaczenie w systemie MDM urządzenia jako utracone i przesłanie do urządzenia konfiguracji inicjującej czyszczenie danych na urządzeniu	
Data i godzina oznaczenie w systemie MDM urządzenia jako utracone i przesłanie do urządzenia konfiguracji inicjującej czyszczenie danych na urządzeniu	
Imię, nazwisko i podpis dokonującego zablokowania karty SIM	
Data i godzina zablokowania karty SIM	

[1] Niepotrzebne skreślić

Załącznik nr 5

ZATWIERDZAM

L.dz. .....

.....
(miejscowość, data)

Egz. Nr .....

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

Wniosek o nadanie hasła „roboczego”/zresetowanie hasła[1)] użytkownika MTN typu 2

Lp.	Rodzaj czynności do wykonania[2)]	Imię i Nazwisko użytkownika – F/P/I[3)]	Identyfikator kadrowy użytkownika Numer PESEL użytkownika	Nazwa jednostki organizacyjnej
1				
...				
n				

Załączniki:
Uzasadnienie:
.....

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

Uwagi: .....

Data realizacji	Imię i nazwisko osoby realizującej wniosek

Oświadczam, że zapoznałam/zapoznałem[1)] się z treścią zarządzenia nr ..... Komendanta Głównego Policji z dnia .....2017 r. w sprawie form uwierzytelniania użytkowników systemów teleinformatycznych Policji przeznaczonych do przetwarzania informacji jawnych

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

[1)] Niepotrzebne skreślić.
[2)] Wstawić: N – w przypadku nadania, Z – w przypadku zresetowania do hasła „roboczego”, O – w przypadku odblokowania.
[3)] Po myślniku wstawić: „F” – w przypadku funkcjonariusza, „P” – w przypadku pracownika lub „I” – w przypadku innej uprawnionej osoby.