Warszawa, dnia 22 sierpnia 2013 r.

Poz. 72

OBWIESZCZENIE
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 20 sierpnia 2013 r.

w sprawie ogłoszenia jednolitego tekstu zarządzenia Komendanta Głównego Policji w sprawie metod i form wykonywania zadań w zakresie przydzielania oraz postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnej centralnych systemów teleinformatycznych Policji

1. Na podstawie art. 16 ust. 3 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2011 r. Nr 197, poz. 1172 i Nr 232, poz. 1378) ogłasza się w załączniku do niniejszego obwieszczenia jednolity tekst zarządzenia nr 645 Komendanta Głównego Policji z dnia 5 czerwca 2009 r. w sprawie metod i form wykonywania zadań w zakresie przydzielania oraz postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnej centralnych systemów teleinformatycznych Policji (Dz. Urz. KGP Nr 8, poz. 35), z uwzględnieniem zmian wprowadzonych zarządzeniem nr 117 Komendanta Głównego Policji z dnia 30 kwietnia 2012 r. zmieniającym zarządzenie w sprawie metod i form wykonywania zadań w zakresie przydzielania oraz postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnej centralnych systemów teleinformatycznych Policji (Dz. Urz. KGP poz. 21).

2. Podany w załączniku do niniejszego obwieszczenia tekst jednolity zarządzenia nie obejmuje § 2 zarządzenia nr 117 Komendanta Głównego Policji z dnia 30 kwietnia 2012 r. zmieniającego zarządzenie w sprawie metod i form wykonywania zadań w zakresie przydzielania oraz postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnej centralnych systemów teleinformatycznych Policji (Dz. Urz. KGP poz. 21), który stanowi:

„§ 2. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.”.

Komendant Główny Policji

nadinsp. Marek DZIAŁOSZYŃSKI

Załącznik do obwieszczenia
Komendanta Głównego Policji
z dnia 20 sierpnia 2013 r.

ZARZĄDZENIE Nr 645
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 5 czerwca 2009 r.

w sprawie metod i form wykonywania zadań w zakresie przydzielania oraz postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnej centralnych systemów teleinformatycznych Policji

Na podstawie art. 7 ust. 1 pkt 2 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287, poz. 1687, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Zarządzenie określa metody i formy przydzielania oraz postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnej centralnych systemów teleinformatycznych Policji.

§ 2. Użyte w zarządzeniu określenia oznaczają:
1) administrator centralny - naczelnika wydziału Biura Łączności i Informatyki Komendy Głównej Policji właściwego w sprawach administrowania centralnymi systemami teleinformatycznymi Policji;
2) administrator lokalny - naczelnika właściwej komórki organizacyjnej do spraw informatyki w komendzie wojewódzkiej (Stołecznej) Policji;
3) aktywacja - umieszczenie w bazie danych informacji o wygenerowanym na KM lub KSIM certyfikacie, a w przypadku OIC o przypisanym numerze sprzętowym klucza, uprawniających do dostępu do części jawnej centralnych systemów teleinformatycznych Policji;
4) bezpośredni przełożony - komendanta wojewódzkiego (Stołecznego) Policji, kierownika komórki organizacyjnej Komendy Głównej Policji, kierownika komórki organizacyjnej komendy wojewódzkiej (Stołecznej) Policji, Komendanta - rektora Wyższej Szkoły Policji w Szczytnie, komendanta szkoły policyjnej, komendanta powiatowego (miejskiego) lub rejonowego Policji, komendanta komisariatu Policji, komendanta komisariatu specjalistycznego Policji, dowódcę oddziału prewencji Policji, dowódcę samodzielnego pododdziału prewencji Policji, dowódcę samodzielnego pododdziału antyterrorystycznego Policji, kierownika ośrodka szkolenia Policji lub osoby przez nich upoważnione do czynności związanych z przydzielaniem i postępowaniem z identyfikatorami;
5) BTUU - Bezpieczny Tryb Uwierzytelnienia Użytkowników będący systemem umożliwiającym bezpieczny dostęp do części jawnej centralnych systemów teleinformatycznych Policji;
6) Centralny Policyjny System Autoryzacji - system umożliwiający identyfikację użytkowników oraz zapewniający dostęp do centralnych systemów teleinformatycznych Policji;
7) certyfikat - zestaw podpisanych cyfrowo danych, pozwalających na dostęp do części jawnej centralnych systemów teleinformatycznych Policji;
8) CPR - Centralny Punkt Rejestracji będący elementem systemu PKI występującym w Komendzie Głównej Policji, odpowiedzialnym w szczególności za czynności związane z aktywacją, dezaktywacją, zablokowaniem i odblokwaniem KM lub KSIM;
9) dezaktywacja - umieszczenie w bazie danych systemu autoryzacji centralnych systemów teleinformatycznych Policji informacji o usunięciu certyfikatu z KM lub KSIM, a w przypadku OIC numeru sprzętowego klucza, dopuszczających do pracy w tych systemach;

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2011 r. Nr 217, poz. 1280 i Nr 230, poz. 1371, z 2012 r. poz. 627, 664, 908, 951 i 1529 oraz z 2013 r. poz. 628.

10)[2] identyfikacyjny numer kadrowy użytkownika - niepowtarzalny numer identyfikacyjny przyznany użytkownikowi;
11) identyfikator - OIC, KM lub KSIM po dokonaniu aktywacji;
12) Inspektor ds. Rejestracji - osoba upoważniona do wykonywania czynności w CPR lub PR, polegających w szczególności na aktywacji, dezaktywacji, zablokowaniu i odblokowaniu KM lub KSIM;
13) KM - kartę mikroprocesorową będącą nośnikiem danych, umożliwiającą autoryzację użytkowników w części jawnej centralnych systemów teleinformatycznych Policji;
14) kod Jednorazowy - przydzielony użytkownikowi kod autoryzacji umożliwiający dokonanie aktywacji KSIM bez jej jednoczesnej obecności w CPR lub PR;
15) kod PIN - przydzielony użytkownikowi kod autoryzacji, przypisany do identyfikatora, umożliwiający dostęp do części jawnej centralnych systemów teleinformatycznych Policji;
16) KSIM - kartę identyfikacji abonenta będącą kluczem dostępowym umożliwiającym autoryzację użytkowników w części jawnej centralnych systemów teleinformatycznych Policji, wykorzystywaną w terminalach mobilnych;
17) odblokowanie - przywrócenie identyfikatorowi uprawnień dopuszczających do pracy w centralnych systemach teleinformatycznych Policji;
18) OIC - Osobisty Identyfikator Cyfrowy będący elektronicznym kluczem stykowym, przeznaczonym do autoryzacji użytkowników w części jawnej centralnych systemów teleinformatycznych Policji;
19) operator - przedsiębiorca telekomunikacyjny, który świadczy na rzecz Policji usługi telekomunikacyjne umożliwiające funkcjonowanie KSIM;
20) PKI - Infrastrukturę Klucza Publicznego będącą systemem organizacyjno-informatycznym, którego głównym celem jest zapewnienie użytkownikom certyfikatów uprawniających do dostępu do części jawnej centralnych systemów teleinformatycznych Policji;
21) PR - Punkt Rejestracji będący elementem systemu PKI występującym w komendach wojewódzkich (Stołecznej) Policji, odpowiedzialnym, w szczególności, za czynności związane z aktywacją, dezaktywacją, zablokowaniem i odblokowaniem KM lub KSIM w podległych organizacyjnie jednostkach Policji;
22) recertyfikacja - wygenerowanie certyfikatu na kolejny okres ważności;
23)[3] użytkownik - uprawnionego do korzystania z identyfikatorów: funkcjonariusza, pracownika Policji albo osobę niebędącą policjantem lub pracownikiem Policji;
24) zablokowanie - umieszczenie w bazie danych Centralnego Policyjnego Systemu Autoryzacji lub BTUU informacji o zawieszeniu uprawnień przypisanych do identyfikatora dopuszczającego do pracy w tych systemach.

§ 3. 1. W Komendzie Głównej Policji dostęp do części jawnej centralnych systemów teleinformatycznych Policji realizowany jest za pomocą Centralnego Policyjnego Systemu Autoryzacji oraz BTUU.

2. Nadzór nad funkcjonowaniem Centralnego Policyjnego Systemu Autoryzacji oraz BTUU sprawuje administrator centralny.

§ 4. 1. W komendach wojewódzkich (Stołecznej) Policji dostęp do części jawnej centralnych systemów teleinformatycznych Policji realizowany jest za pomocą lokalnych serwerów autoryzacji oraz BTUU.

2. Nadzór nad funkcjonowaniem lokalnych serwerów autoryzacji oraz BTUU sprawują administratorzy lokalni.

§ 5. 1. Komenda Główna Policji oraz komendy wojewódzkie (Stołeczna) Policji, każda we własnym zakresie, dysponują nieaktywnymi OIC, KM i KSIM oraz są odpowiedzialne za ich przechowywanie.

2. Nieaktywnymi OIC, KM i KSIM dysponuje i przchowuje:
1) w Komendzie Głównej Policji - Biuro Łączności i Informatyki Komendy Głównej Policji;

---

[2] W brzmieniu ustalonym przez § 1 pkt 1 lit. a zarządzenia nr 117 Komendanta Głównego Policji z dnia 30 kwietnia 2012 r. zmieniającego zarządzenie w sprawie metod i form wykonywania zadań w zakresie przydzielania oraz postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnych centralnych systemów teleinformatycznych Policji (Dz. Urz. KGP poz. 21), które weszło w życie z dniem 1 maja 2012 r.

[3] W brzmieniu ustalonym przez § 1 pkt 1 lit. b zarządzenia, o którym mowa w odnośniku 2.

2) w komendach wojewódzkich (Stołecznej) Policji i szkołach policyjnych - komórka organizacyjna właściwa do spraw informatyki.

§ 6. 1. OIC oraz KSIM podlegają aktywacji, dezaktywacji, zablokowaniu lub odblokowaniu.

2. KM podlegają aktywacji, dezaktywacji, zablokowaniu, odblokowaniu oraz recertyfikacji.

§ 7. 1. Aktywacji KM dokonuje Inspektor ds. Rejestracji, zapisując w BTUU i pamięci KM dane niezbędne do bezpiecznego logowania w części jawnej centralnych systemów teleinformatycznych Policji na podstawie wniosku bezpośredniego przełożonego użytkownika, zwanego dalej "wnioskiem".

2. Aktywacja KM dokonywana jest w:

1) CPR - dla komórek organizacyjnych Komendy Głównej Policji i szkół policyjnych;
2) PR - dla komend wojewódzkich (Stołecznej) Policji, komend powiatowych (miejskich) lub rejonowych Policji, komisariatów Policji, komisariatów specjalistycznych Policji, posterunków Policji, rewirów dzielnicowych Policji, oddziałów prewencji Policji, samodzielnych pododdziałów prewencji Policji, samodzielnych pododdziałów antyterrorystycznych Policji oraz ośrodków szkolenia Policji.

3. Wniosek kierowany jest do:

1) administratora centralnego - dla podmiotów, o których mowa w ust. 2 pkt 1;
2) administratora lokalnego - dla podmiotów, o których mowa w ust. 2 pkt 2.

4. KM po aktywacji posiada jeden certyfikat przypisany wyłącznie jednemu użytkownikowi.

§ 8. 1. Po dokonaniu aktywacji KM administrator centralny lub lokalny przekazuje właściwej jednostce lub komórce, o której mowa we wniosku, KM i oddzielnie kod PIN w zamkniętej kopercie uniemożliwiającej jego odczytanie.

2. KM i kod PIN, o których mowa w ust. 1, są przekazywane użytkownikowi przez bezpośredniego przełożonego. Kod PIN jest przekazywany w zamkniętej kopercie uniemożliwiającej jego odczytanie przez osobę nieupoważnioną.

3. Odbiór KM oraz kodu PIN użytkownik potwierdza własnoręcznym podpisem na pokwitowaniu, którego wzór określa załącznik nr 1 do zarządzenia.

4. Po potwierdzeniu przez użytkownika pokwitowanie, o którym mowa w ust. 3, bezpośredni przełożony niezwłocznie zwraca administratorowi, który dokonał aktywacji KM.

§ 9. 1. Do recertyfikacji odpowiednio stosuje się § 7 ust. 1 - 3 i § 8.

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

3. Użytkownik zawiadamia bezpośredniego przełożonego o konieczności recertyfikacji KM nie później niż na trzy miesiące przed utratą ważności certyfikatu.

4. Bezpośredni przełożony, po otrzymaniu zawiadomienia, o którym mowa w ust. 3, występuje o recertyfikację KM, nie wcześniej niż przed upływem 2 miesięcy przed utratą ważności certyfikatu i nie później niż na 14 dni przed upływem tego okresu.

§ 10. 1. Aktywacji KSIM dokonuje Inspektor ds. Rejestracji, zapisując w BTUU i pamięci KSIM dane niezbędne do bezpiecznego logowania w części jawnej centralnych systemów teleinformatycznych Policji na podstawie wniosku.

2. Aktywacja KSIM może być dokonana przez użytkownika po otrzymaniu kodów Jednorazowych wygenerowanych w CPR lub PR.

3. Aktywacja KSIM oraz generowanie kodów Jednorazowych dokonywane jest w trybie określonym w § 7 ust. 2 i 3.

4. KSIM po aktywacji posiada maksymalnie trzy certyfikaty z własnymi kodami PIN przypisane odrębnie dla każdego z użytkowników.

§ 11. Do czynności po dokonaniu aktywacji KSIM oraz czynności związanych z przekazaniem wygenerowanego kodu Jednorazowego jednostce lub komórce, o której mowa we wniosku, odpowiednio stosuje się § 8.

§ 12. 1. Aktywacji OIC dokonuje administrator centralny lub administrator lokalny właściwy dla jednostki organizacyjnej Policji, zapisując w Centralnym Policyjnym Systemie Autoryzacji numer sprzętowy OIC oraz dane niezbędne do bezpiecznego logowania w części jawnej centralnych systemów teleinformatycznych Policji.

2. Aktywacja OIC dokonywana jest na podstawie wniosku, w trybie określonym w § 7 ust. 3.

3. OIC po aktywacji posiada własny kod PIN i może być używany wyłącznie przez jednego użytkownika.

§ 13. 1. Po dokonaniu aktywacji OIC administrator lokalny właściwy dla jednostki organizacyjnej Policji zwraca się do administratora centralnego za pośrednictwem policyjnej poczty elektronicznej z wnioskiem o wygenerowanie oraz przesłanie kodu PIN dla użytkownika.

2. Do pozostałych czynności po dokonaniu aktywacji OIC odpowiednio stosuje się § 8.

§ 14. 1. Identyfikatory 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 do innej komórki albo jednostki organizacyjnej Policji;
4) nie wykonywania przez użytkownika zadań związanych z dostępem do części jawnej centralnych i lokalnych systemów teleinformatycznych Policji;
5) zwrotu identyfikatora do administratora lokalnego lub centralnego;
6) decyzji bezpośredniego przełożonego użytkownika o ich dezaktywacji.

2. Dezaktywacja KM, OIC lub KSIM dokonywana jest na podstawie wniosku, w trybie określonym w § 7 ust. 3.

§ 15. 1. Identyfikatory podlegają zablokowaniu w przypadku:

1) zgubienia;
2) zniszczenia;
3) utraty stwarzającej możliwość bezpośredniego dostępu osób nieuprawnionych do centralnych systemów teleinformatycznych Policji;
4) zaistnienia uzasadnionego podejrzenia wobec użytkownika o udostępnieniu osobom nieuprawnionym danych uzyskanych z centralnych systemów teleinformatycznych Policji.

2. Zablokowanie dokonywane jest na wniosek, w trybie określonym w § 7 ust. 3.

3. W przypadku odblokowania identyfikatora ust. 2 stosuje się odpowiednio.

§ 16. Wzór formularza wniosku o:

1) aktywację, dezaktywację, recertyfikację KM lub OIC określa załącznik nr 2 do zarządzenia;
2) aktywację lub dezaktywację KSIM określa załącznik nr 3 do zarządzenia;
3) dezaktywację dotychczasowego i aktywację nowego użytkownika na tej samej KSIM lub aktywację kolejnego użytkownika, gdy do KSIM nie są przypisani trzej użytkownicy określa załącznik nr 4 do zarządzenia;
4) zablokowanie, odblokowanie KM, KSIM lub OIC określa załącznik nr 5 do zarządzenia.

§ 17. Użytkownik zobowiązany jest do:

1) wykorzystywania identyfikatora wyłącznie do realizacji zadań służbowych;
2) użytkowania i przechowywania identyfikatora w sposób uniemożliwiający jego wykorzystanie przez osobę nieuprawnioną;
3) ochrony identyfikatora przed jego zniszczeniem lub utratą;
4) niezwłocznego zwrotu identyfikatora:
   a) w przypadkach, o których mowa w § 14 ust. 1 pkt 2-4;
   b) w przypadku uszkodzenia identyfikatora;
   c) w przypadku odnalezienia utraconego identyfikatora.

§ 18. 1. Na identyfikatorach nie należy dokonywać zmian mechanicznych naruszających ich strukturę fizyczną.

2. Dopuszcza się umieszczanie na identyfikatorach tylko usuwalnych naklejek samoprzylepnych jako

oznaczeń ułatwiających użytkownikowi ich identyfikację.

§ 19. W przypadku utraty albo zniszczenia:
1) KM lub OIC - użytkownik powiadamia niezwłocznie bezpośredniego przełożonego o tym fakcie sporządzając notatkę służbową, w której opisuje okoliczności tego zdarzenia;
2) KSIM - użytkownik stosuje procedurę określoną w instrukcji sposobu postępowania w przypadku utraty aktywowanych KSIM, stanowiącej załącznik nr 6 do zarządzenia oraz w instrukcji sposobu postępowania z uszkodzonymi identyfikatorami, stanowiącej załącznik nr 7 do zarządzenia, a następnie niezwłocznie wykonuje czynności, o których mowa w pkt 1.

§ 20. W przypadku utraty albo zniszczenia identyfikatora, bezpośredni przełożony użytkownika powiadamia niezwłocznie, telefonicznie lub za pośrednictwem poczty elektronicznej, administratora centralnego lub właściwego dla jednostki organizacyjnej Policji administratora lokalnego, a następnie przekazuje temu administratorowi wniosek o zablokowanie identyfikatora.

§ 21. 1. W przypadku, o którym mowa w § 14 ust. 1 pkt 2-4 oraz § 17 pkt 4 lit. b i c, użytkownik zwraca identyfikator:
1) bezpośredniemu przełożonemu albo
2) właściwemu administratorowi centralnemu lub lokalnemu - po wyrażeniu zgody przez bezpośredniego przełożonego.

2. Bezpośredni przełożony użytkownika niezwłocznie przesyła zwrócony identyfikator właściwemu administratorowi centralnemu lub lokalnemu, który potwierdza odbiór tego identyfikatora.

3. W przypadku otrzymania identyfikatora w trybie, o którym mowa w ust. 1 pkt 2, administrator centralny lub lokalny niezwłocznie powiadamia bezpośredniego przełożonego użytkownika o tym fakcie.

§ 22. 1. W przypadku, o którym mowa w § 14 ust. 1 pkt 1-4, użytkownik KSIM posiadającej:
1) jeden certyfikat - jest zobowiązany do usunięcia swojego certyfikatu oraz zwrotu KSIM i kodu PIN do bezpośredniego przełożonego;
2) co najmniej dwa certyfikaty - jest zobowiązany do usunięcia swojego certyfikatu oraz zwrotu kodu PIN do bezpośredniego przełożonego.

2. Kod PIN bezpośredni przełożony wydaje kolejnemu użytkownikowi, który, przy użyciu kodów Jednorazowych, dokonuje wygenerowania na KSIM danych niezbędnych do dostępu do części jawnej centralnych systemów teleinformatycznych Policji.

§ 23. Traci moc zarządzenie nr 2/97 Komendanta Głównego Policji z dnia 4 lutego 1997 r. w sprawie zasad przydzielania i postępowania z Osobistym Identyfikatorem Cyfrowym (OIC), zmienione zarządzeniem nr 14/2002 z dnia 23 sierpnia 2002 r.

§ 24. Zarządzenie wchodzi w życie po upływie 30 dni od dnia podpisania.

Załączniki
do zarządzenia nr 645
Komendanta Głównego Policji
z dnia 5 czerwca 2009 r.

Załącznik nr 1

wzór

Egz. nr .....

.....
(imię i nazwisko użytkownika)
.....
(identyfikacyjny numer kadrowy)
.....
(nazwa jednostki organizacyjnej Policji)

Pokwitowanie odbioru identyfikatora/kodu PIN/kodu Jednorazowego[1)]

Potwierdzam odbiór identyfikatora ..... nr .....
(rodzaj identyfikatora)
wraz z kodem PIN do tego identyfikatora.

Jednocześnie oświadczam, że zapoznałem/am[1)] się z treścią zarządzenia nr ..... Komendanta Głównego Policji z dnia ..... 2009 r. w sprawie metod i form wykonywania zadań w zakresie przydzielania i postępowania z identyfikatorami umożliwiającymi użytkownikom dostęp do części jawnej centralnych systemów teleinformatycznych Policji.

....., dnia .....

.....
(czytelny podpis użytkownika)

.....
(imię i nazwisko wydającego oraz podpis)

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

Wyk. w 2 egz.:
egz. nr 1 - użytkownik
egz. nr 2 - a/a administrator

_____
1) niepotrzebne skreślić

Załącznik nr 2[4)]

Wzór formularza wniosku o aktywację, dezaktywację, recertyfikację KM lub OIC

.....
(miejscowość, data)

Egz. nr .....
Adresat:
.....
.....
.....
.....

Wniosek o aktywację/dezaktywację/recertyfikację[1)] KM/OIC[1)]

Lp.	Imię i nazwisko użytkownika - ...[2)]	Numer KM, OIC[3)]	Identyfikacyjny numer kadrowy użytkownika Numer PESEL użytkownika	Adres skrzynki PPE[4)]	Jednostka organizacyjna
1					
2					

Uzasadnienie:
.....
.....
.....

…….....
(pieczęć i podpis bezpośredniego przełożonego użytkownika)

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

[4)] W brzmieniu ustalonym przez § 1 pkt 2 zarządzenia, o którym mowa w odnośniku 2.

Data aktywacji/dezaktywacji/recertyfikacji[1)]	Imię i nazwisko osoby wykonującej aktywację/dezaktywację/recertyfikację[1)]

_____

1) niepotrzebne skreślić

2) po myślniku wstawić "F" - w przypadku funkcjonariusza, "P" - w przypadku pracownika lub "I" w przypadku innej osoby

3) rubrykę wypełnia administrator - w przypadku aktywacji KM lub OIC albo podmiot wnioskujący o dezaktywację - w przypadku dezaktywacji KM lub OIC

4) wypełnia się tylko w przypadku KM i KSIM

Załącznik nr 3

wzór

.....
(miejscowość, data)

Egz. Nr .....

Adresat:
.....
.....
.....
.....

Wniosek o aktywację/dezaktywację[1)] KSIM

Lp.	Imię i Nazwisko użytkownika - ..... [2)]		Identyfikacyjny numer kadrowy użytkownika Numer PESEL użytkownika	Adres skrzynki PPE	Jednostka organizacyjna
1	KSIM[3)] Nr				
2					
3					
1	KSIM[3)] Nr				
2					
3					

Uzasadnienie:
.....
.....

.....
(pieczęć i podpis bezpośredniego przełożonego użytkownika)

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

Data aktywacji/dezaktywacji[1)]	Imię i nazwisko osoby wykonującej aktywację/dezaktywację[1)]

_____
1) niepotrzebne skreślić
2) po myślniku wstawić "F" - w przypadku funkcjonariusza lub "P" - w przypadku pracownika
3) rubrykę wypełnia administrator - w przypadku aktywacji KSIM albo podmiot wnioskujący o dezaktywację - w przypadku dezaktywacji KSIM

Załącznik nr 4

wzór

.....
(miejscowość, data)

Egz. Nr .....

Adresat:
.....
.....
.....
.....

Wniosek
o dezaktywację dotychczasowego i aktywację nowego użytkownika na tej samej KSIM/ aktywację kolejnego użytkownika, gdy do KSIM nie są przypisani trzej użytkownicy[1)]

Lp.	Numer KSIM	Rodzaj czynności do wykonania na KSIM ...[2)]	Imię i Nazwisko użytkownika -...[3)]	Identyfikacyjny numer kadrowy użytkownika Numer PESEL użytkownika	Adres skrzynki PPE	Jednostka organizacyjna
1						
2						
3						
4						
5						
6						

Uzasadnienie:
.....

.....

.....
(pieczęć i podpis bezpośredniego przełożonego użytkownika)

Uwagi:[4)]
.....
.....
.....

Data dezaktywacji lub aktywacji	Imię i nazwisko osoby wykonującej dezaktywację lub aktywację

_____
1) niepotrzebne skreślić
2) wstawić "D" - w przypadku dezaktywacji lub "A" - w przypadku aktywacji
3) po myślniku wstawić "F" - w przypadku funkcjonariusza lub "P" - w przypadku pracownika
4) w przypadku gdy aktywacja użytkownika będzie oparta o kod Jednorazowy w polu "Uwagi" należy zamieścić wzmiankę, o tym fakcie według następującego wzoru: Wygenerowanie kodu Jednorazowego dla ....." (podać imię i nazwisko użytkownika).

Załącznik nr 5[5)]

Wzór formularza wniosku o zablokowanie, odblokowanie KM, KSIM lub OIC

.....
(miejscowość, data)

Egz. nr .....

Adresat:
.....
.....
.....
.....

Wniosek o zablokowanie/odblokowanie[1)] KM/KSIM/OIC[1)]

Lp.	Imię i nazwisko użytkownika - ...[2)]	Numer KM, KSIM OIC[1)]	Identyfikacyjny numer kadrowy użytkownika Numer PESEL użytkownika	Jednostka organizacyjna
1				
2				

Uzasadnienie:
.....
.....
.....

.....
(pieczęć i podpis bezpośredniego przełożonego użytkownika)

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

[5)] W brzmieniu ustalonym przez § 1 pkt 3 zarządzenia, o którym mowa w odnośniku 2.

Data zablokowania/odblokowania[1)]	Imię i nazwisko osoby wykonującej zablokowanie/odblokowanie[1)]

_____

1) niepotrzebne skreślić

2) po myślniku wstawić "F" - w przypadku funkcjonariusza, "P" - w przypadku pracownika lub "I" w przypadku innej osoby

Załącznik nr 6

Instrukcja sposobu postępowania w przypadku utraty aktywowanych KSIM

§ 1. 1. W przypadku utraty aktywowanej KSIM, skutkującej możliwością bezpośredniego dostępu osób nieuprawnionych do części jawnej centralnych systemów teleinformatycznych Policji, użytkownik pełniący służbę lub zatrudniony w:

1) komendzie wojewódzkiej (Stołecznej) Policji, oddziale prewencji Policji, samodzielnym pododdziale prewencji Policji, samodzielnym pododdziale antyterrorystycznym Policji, ośrodku szkolenia Policji, komisariacie specjalistycznym Policji, komendzie powiatowej, miejskiej, rejonowej Policji, komisariacie Policji, lub posterunku Policji - niezwłocznie powiadamia o tym fakcie telefonicznie lub drogą radiową, a następnie w formie notatki służbowej, dyżurnego właściwej terytorialnie jednostki organizacyjnej Policji;
2) Komendzie Głównej Policji lub szkole policyjnej - niezwłocznie powiadamia telefonicznie o tym fakcie dyżurnego do spraw całodobowego technologicznego utrzymania centralnych systemów teleinformatycznych Wydziału Utrzymania Systemów Informatycznych Biura Łączności i Informatyki Komendy Głównej Policji.

2. Powiadomienia, o którym mowa w ust. 1, dokonuje się podając imię i nazwisko, identyfikacyjny numer kadrowy użytkownika oraz jednostkę organizacyjną Policji, w której użytkownik pełni służbę lub jest zatrudniony.

§ 2. 1. Dyżurny, o którym mowa w § 1 ust. 1 pkt 1, po weryfikacji zgłoszenia utraty aktywowanej KSIM, przekazuje, zachowując zasady obiegu informacji określone w przepisach służby dyżurnej, dyżurnemu komendy wojewódzkiej (Stołecznej) Policji następujące informacje:

1) imię i nazwisko oraz identyfikacyjny numer kadrowy użytkownika, który zgłosił utratę KSIM;
2) nazwę jednostki organizacyjnej Policji, w której pełni służbę lub jest zatrudniony użytkownik zgłaszający utratę KSIM.

2. Informacje, o których mowa w ust. 1, przekazywane są niezwłocznie w formie telefonicznej, a następnie potwierdzane w formie pisemnej.

§ 3. Po weryfikacji zgłoszenia utraty aktywowanej KSIM, dyżurny, o którym mowa w § 1 ust. 1 pkt 2, lub dyżurny komendy wojewódzkiej (Stołecznej) Policji powiadamia telefonicznie o utracie tej KSIM właściwego operatora, który wykonuje czynności związane z zablokowaniem KSIM.

§ 4. 1. Administrator centralny jest odpowiedzialny za bieżącą aktualizację i dostarczenie:

1) do dyżurnego, o którym mowa w § 1 ust. 1 pkt 2:
   a) list zawierających wykaz KSIM z ich numerami, nazwą operatora oraz przypisanymi do nich imionami i nazwiskami wraz z identyfikacyjnymi numerami kadrowymi użytkowników, o których mowa w § 1 ust. 1 pkt 2,
   b) informacji o numerach telefonów operatorów, na które należy zgłaszać wnioski o zablokowanie KSIM;
2) operatorowi - informacji o numerach telefonów, z których będzie zgłaszany wniosek o zablokowanie KSIM.

2. Administrator lokalny jest odpowiedzialny za bieżącą aktualizację i dostarczenie:

1) do stanowiska kierowania komendy wojewódzkiej (Stołecznej) Policji:
   a) list zawierających wykaz KSIM z ich numerami, nazwą operatora oraz przypisanymi do nich imionami i nazwiskami wraz z identyfikacyjnymi numerami kadrowymi użytkowników, o których mowa w § 1 ust. 1 pkt 1,
   b) informacji o numerach, o których mowa w ust. 1 pkt 1 lit. b, działając w porozumieniu z administratorem centralnym;
2) do administratora centralnego - informacji, o których mowa w ust. 1 pkt 2.

Załącznik nr 7

Instrukcja sposobu postępowania z uszkodzonymi identyfikatorami

§ 1. Za identyfikatory uszkodzone uznaje się identyfikatory przy pomocy, których niemożliwy jest dostęp do części jawnej centralnych systemów teleinformatycznych Policji.

§ 2. Przekazywanie identyfikatorów odbywa się wyłącznie za pośrednictwem poczty specjalnej.

§ 3. 1. Uszkodzony identyfikator jest przekazywany przez użytkownika do:
1) bezpośredniego przełożonego - w przypadku komórek organizacyjnych Komendy Głównej Policji oraz komend wojewódzkich (Stołecznej) Policji, oddziałów prewencji Policji, samodzielnych pododdziałów prewencji Policji, samodzielnych pododdziałów antyterrorystycznych Policji, ośrodków szkolenia Policji, komisariatów specjalistycznych Policji, komend powiatowych, miejskich i rejonowych Policji, komisariatów Policji, posterunków Policji oraz rewirów dzielnicowych Policji;
2) kierownika komórki organizacyjnej właściwej do spraw informatyki - w przypadku szkół policyjnych.

2. Przełożony, o którym mowa w ust. 1 pkt 1, przekazuje uszkodzony identyfikator:
1) Wydziałowi Utrzymania Systemów Informatycznych Biura Łączności i Informatyki Komendy Głównej Policji, zwanemu dalej "WUSI" - w przypadku komórek organizacyjnych Komendy Głównej Policji, zwanych dalej "komórkami KGP";
2) właściwemu administratorowi lokalnemu, zwanemu dalej "AL" - w przypadku komend wojewódzkich (Stołecznej) Policji, oddziałów prewencji Policji, samodzielnych pododdziałów prewencji Policji, samodzielnych pododdziałów antyterrorystycznych Policji, ośrodków szkolenia Policji, komisariatów specjalistycznych Policji, komend powiatowych, miejskich i rejonowych Policji, komisariatów Policji, posterunków Policji oraz rewirów dzielnicowych Policji, zwanych dalej "jednostkami Policji".

3. Kierownik, o którym mowa w ust. 1 pkt 2, przekazuje uszkodzony identyfikator WUSI.

§ 4. Użytkownik, przed przekazaniem uszkodzonego KSIM do naprawy, usuwa swój certyfikat, jeśli rodzaj uszkodzenia KSIM pozwala na przeprowadzenie tej czynności.

§ 5. Uszkodzony KM lub KSIM jest przesyłany do naprawy razem z wnioskiem o dezaktywację, zawierającym w polu "Uwagi" dopisek "naprawa".

§ 6. AL, który otrzymał uszkodzony:
1) OIC - występuje o jego naprawę do WUSI lub dokonuje jego wymiany;
2) KM lub KSIM - dokonuje ich sprawdzenia, a w przypadku niemożności ich naprawy występuje do WUSI o ich sprawdzenie i ewentualną wymianę.

§ 7. WUSI przekazuje aktywowany i naprawiony lub wymieniony identyfikator:
1) bezpośredniemu przełożonemu użytkownika - w przypadku komórek KGP;
2) kierownikowi komórki organizacyjnej właściwej do spraw informatyki - w przypadku szkół policyjnych;
3) AL - w przypadku jednostek Policji.

§ 8. Podmioty, o których mowa w § 7, przekazują, otrzymany od WUSI, aktywowany i naprawiony lub wymieniony identyfikator właściwemu użytkownikowi.