DECYZJA NR .80.
DYREKTORA BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI

z dnia ..12..maja..... 2023 r.

zmieniająca decyzję w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Łączności i Informatyki Komendy Głównej Policji, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych

Na podstawie § 12 ust. 1 zarządzenia nr 2 Komendanta Głównego Policji z dnia 1 kwietnia 2016 r. w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP poz. 13, z późn. zm.[1)]) postanawia się, co następuje:

§ 1. W decyzji nr 97 Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji z dnia 27 maja 2020 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Łączności i Informatyki Komendy Głównej Policji, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych, zmienionej decyzją nr 184 z dnia 26 października 2021 r. oraz decyzją nr 40 z dnia 23 marca 2022 r., wprowadza się następujące zmiany:

1) w § 5 w pkt 52 kropkę zastępuje się średnikiem i dodaje się pkt 53 w brzmieniu:
„53) realizowanie zadań wynikających z przepisów rozporządzenia Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 131).";

2) w § 7 w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12 -30 w brzmieniu:
„12) aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (CyberThreat Intelligence i ThreatHunting);
13) analizowanie złośliwego oprogramowania;
14) badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania;
15) dokonywanie oceny bezpieczeństwa systemów informacyjnych, w tym przeprowadzanie testów penetracyjnych i audytów bezpieczeństwa;
16) prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności;
17) rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa;
18) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo;
19) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych;
20) zaawansowana obsługa incydentów;
21) szacowanie ryzyka w obszarze cyberbezpieczeństwa;
22) opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji;
23) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych;
24) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych;
25) wstępna obsługa incydentów;
26) zabezpieczenie śladów cyfrowych;
27) rozpoznawanie zagrożeń cyberbezpieczeństwa;
28) monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
29) prowadzenie akcji podnoszących świadomość w obszarze cyberbezpiczeństwa, w szczególności organizowanie ćwiczeń i szkoleń;
30) przygotowywanie rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa, w szczególności podnoszących poziom bezpieczeństwa.";

[1)] Zmiany wymienionego zarządzenia zostały ogłoszone w Dz. Urz. KGP z 2016 r. poz. 69, z 2017 r. poz. 44, z 2018 r. poz. 2, 106, i 126, z 2019 r. poz. 105 i 126, z 2020 r. poz. 16, z 2021 r. poz. 15, 57 i 101, z 2022 r. poz. 88, 199 i 218 oraz z 2023 r. poz. 7.

3) w § 8 w ust. 1 w pkt 17 kropkę zastępuje się średnikiem i dodaje się pkt 18-33 w brzmieniu:
„18) aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (CyberThreat Intelligence i ThreatHunting);
19) analizowanie złośliwego oprogramowania;
20) badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania;
21) dokonywanie oceny bezpieczeństwa systemów informacyjnych, w tym przeprowadzanie testów penetracyjnych i audytów bezpieczeństwa;
22) prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności;
23) rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa;
24) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo;
25) przyjmowanie zgłoszeń i obsługa incydentów poważnych;
26) wstępna obsługa incydentów;
27) reagowanie na incydenty oraz ich klasyfikacja;
28) korelacja danych, prowadzenie analiz lub tworzenie map sytuacyjnych;
29) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych;
30) zaawansowana obsługa incydentów;
31) analiza i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania;
32) koordynowanie obsługi zgłoszonych incydentów;
33) specjalistyczne zadania realizowane w ramach SOC lub Centrum Zarządzania Siecią (NOC) obejmujące monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów.";

4) § 9 otrzymuje brzmienie:
„**§ 9.** 1. Do zadań wspólnych Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych należy:
1) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo,
2) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych,
3) zaawansowana obsługa incydentów,
4) analizowanie i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania,
5) koordynowanie obsługi zgłoszonych incydentów,
6) specjalistyczne zadania realizowane w ramach SOC lub Centrum Zarządzania Siecią (NOC) obejmujące monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów,
7) szacowanie ryzyka w obszarze cyberbezpieczeństwa,
8) opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji,
9) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych,
10) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych,
11) reagowanie i rozwiązywanie zgłaszanych incydentów w celu zapewnienia wymaganej dostępności i bezpieczeństwa systemów.

2. W Wydziale Utrzymania Systemów Informatycznych Policyjnych i Krajowych do zadań:
1) Sekcji Administratorów należy w szczególności:
a) administrowanie centralnymi systemami informatycznymi eksploatowanymi w Policji w celu zapewnienia ich dostępności, dyspozycyjności i sprawności technicznej, w tym: serwerami, systemami operacyjnymi, bazami danych i aplikacjami,
b) administrowanie centralnymi systemami dostępowymi, za pomocą których realizowany jest dostęp centralnych systemów informatycznych Policji do krajowych systemów informatycznych, w tym: serwerami, systemami operacyjnymi, bazami danych i aplikacjami,
c) administrowanie centralnymi systemami informatycznymi Policji określonymi w rejestrze systemów i usług teleinformatycznych, administrowanych oraz utrzymywanych przez biuro, zgodnie z właściwością wydziału,
d) identyfikowanie i analizowanie potrzeb technicznych, określanie założeń i zadań inwestycyjnych

w zakresie zapewnienia należytego funkcjonowania centralnych systemów informatycznych Policji, zgodnie z właściwością wydziału,

e) udział w pracach testowych, wdrożeniowych i przyjęciu do eksploatacji nowych centralnych systemów informatycznych Policji;

2) Sekcji do spraw Obsługi Całodobowej należy w szczególności:

a) bieżące, całodobowe monitorowanie i obsługa technologiczna centralnych systemów informatycznych eksploatowanych w Policji,

b) inicjowanie i uruchamianie automatycznych oraz manualnych procedur reaktywnych i naprawczych w sytuacjach awaryjnych w celu zapewnienia nieprzerwanego działania policyjnych systemów informatycznych Policji,

c) wspieranie użytkowników w zakresie dostępu do centralnych systemów informatycznych Policji,

d) techniczne zarządzanie wybranymi uprawnieniami użytkowników centralnych systemów informatycznych Policji,

e) koordynowanie i rozwiązywanie bieżących problemów wynikających z eksploatacji centralnych systemów informatycznych Policji, w tym:
   - reagowanie na zgłoszenia użytkowników końcowych w zakresie działania systemów informatycznych,
   - obsługa dedykowanych platform zgłoszeniowych,
   - monitorowanie utrzymywanych systemów informatycznych w zakresie wykrywania i diagnozowania problemów, błędów i nieprawidłowości w działaniu systemów oraz błędów mających wpływ na jakość gromadzonych danych,
   - reagowanie na awarie systemów informatycznych: uruchamianie stosownych procedur, powiadamianie administratorów, podmiotów zewnętrznych, firm zewnętrznych oraz kierownictwa wydziału i biura o awariach systemów informatycznych,

f) bieżąca współpraca z zespołami serwisowymi podmiotów zewnętrznych,

g) monitorowanie poprawności działania sprzętu znajdującego się w serwerowni „Wiśniowa" oraz powiadamianie odpowiednich administratorów o wszystkich wykrytych nieprawidłowościach,

h) monitorowanie i odnotowywanie wszystkich wejść i wyjść z serwerowni „Wiśniowa",

i) monitorowanie prawidłowego funkcjonowania zasilania energetycznego oraz układu klimatyzacyjnego serwerowni „Wiśniowa",

j) planowanie i bieżąca konserwacja urządzeń pozostających we właściwości wydziału,

k) nadzorowanie ilościowo-asortymentowe sprzętu serwerowego, znajdującego się w serwerowi „Wiśniowa", będącego na stanie ewidencyjnym wydziału,

l) monitorowanie lub prowadzenie prac elektroinstalacyjnych w obrębie serwerowni „Wiśniowa" zgodnie z właściwością wydziału,

m) prowadzenie dokumentacji technicznej, w tym ewidencji awarii, protokołów z przeglądów urządzeń i instalacji systemów oraz książek eksploatacji urządzeń i systemów, pozostającej we właściwości wydziału;

3) Sekcji do spraw Eksploatacji należy w szczególności:

a) koordynowanie rozwiązywania bieżących problemów wynikających z eksploatacji centralnych systemów informatycznych Policji a w szczególności Systemu Wspomagania Dowodzenia oraz Krajowego Systemu Informacyjnego Policji,

b) bieżący nadzór i współpraca z zespołami serwisowymi podmiotów zewnętrznych,

c) udział w przedsięwzięciach organizacyjnych i planistycznych, związanych z eksploatacją i rozwojem centralnych systemów informatycznych Policji a w szczególności Systemu Wspomagania Dowodzenia oraz Krajowego Systemu Informacyjnego Policji,

d) identyfikowanie i analizowanie potrzeb oraz zadań inwestycyjnych w zakresie zapewnienia należytego funkcjonowania centralnych systemów informatycznych Policji,

e) ewidencjonowanie oraz przechowywanie obowiązujących i wykonywanych umów, a także innych bazowych dokumentów wynikających z realizacji kontraktów, w zakresie utrzymywanych przez wydział systemów informatycznych,

f) udział w pracach komitetów sterujących oraz zespołów i grup eksperckich, w związku z realizowanymi przez wydział przedsięwzięciami informatycznymi,
g) gromadzenie i przetwarzanie danych na potrzeby zarządzania ryzykiem zgodnie z właściwością wydziału.";

5) § 10 otrzymuje brzmienie:

„§ 10. 1. Do zadań wspólnych Wydziału Utrzymania Systemów Informatycznych Międzynarodowych należy:

1) analizowanie i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania,
2) koordynowanie obsługi zgłoszonych incydentów,
3) specjalistyczne zadania realizowane w ramach SOC lub Centrum Zarządzania Siecią (NOC) obejmujące monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów,
4) szacowanie ryzyka w obszarze cyberbezpieczeństwa,
5) opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji,
6) sprawowanie nadzoru nad procesem szacowania ryzyka w obszarze cyberbezpieczeństwa,
7) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych,
8) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych,
9) wstępna obsługa incydentów,
10) rozpoznawanie zagrożeń cyberbezpieczeństwa,
11) prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa, w szczególności organizacja ćwiczeń i szkoleń,
12) współpraca krajowa lub międzynarodowa w obszarze cyberbezpieczeństwa.

2. W Wydziale Utrzymania Systemów Informatycznych Międzynarodowych do zadań:

1) Sekcji Administratorów należy w szczególności:
a) administrowanie międzynarodowymi systemami i usługami informatycznymi określonymi w rejestrze systemów i usług teleinformatycznych administrowanych oraz utrzymywanych przez biuro, zgodnie z właściwością wydziału,
b) administrowanie centralnymi komponentami Systemu Wymiany Informacji z Europolem eksploatowanymi w Policji w celu zapewnienia ich dostępności i sprawności technicznej, w tym sprzętem serwerowym, systemami operacyjnymi, bazami danych i aplikacjami,
c) administrowanie systemami informatycznymi Centralnego Laboratorium Kryminalistycznego Policji, zwanego dalej „CLKP", określonymi w rejestrze systemów i usług teleinformatycznych administrowanych oraz utrzymywanych przez biuro,
d) monitorowanie wydajności, obciążenia i przepustowości infrastruktury informatycznej oraz podejmowanie działań modernizacyjnych w zakresie infrastruktury teleinformatycznej w celu optymalnego wykorzystania posiadanych zasobów teleinformatycznych,
e) przeprowadzanie analiz funkcjonujących usług pod kątem ich optymalizacji i lepszego dostosowania do potrzeb odbiorcy,
f) zgłaszanie potrzeb w zakresie rozwoju utrzymywanych systemów informatycznych w celu realizacji zobowiązań międzynarodowych,
g) zgłaszanie potrzeb i propozycji w zakresie optymalizacji procesów przetwarzania danych w systemach informatycznych utrzymywanych przez wydział,
h) dokonywanie niezbędnych modyfikacji procedur administracyjnych w celu zapewnienia zgodnego z założeniami i sprawnego działania systemów informatycznych pozostających we właściwości wydziału,
i) przestrzeganie harmonogramów określonych przez organy Unii Europejskiej oraz planowanie sposobu ich realizacji i wdrożenia w celu zapewnienia zgodnego z planami wdrażania, modyfikacji i testowania systemów informatycznych;

2) Sekcji do spraw Obsługi Całodobowej należy w szczególności:
   a) całodobowe monitorowanie funkcjonowania systemów informatycznych utrzymywanych przez wydział w celu weryfikacji poprawności i efektywności korzystania z zasobów tych systemów przez uprawnionych użytkowników,
   b) powiadamianie interesariuszy o awariach oraz wszelkich zaobserwowanych nieprawidłowościach w funkcjonowaniu systemów informatycznych,
   c) inicjowanie i uruchamianie stosownych procedur reaktywnych oraz naprawczych w sytuacjach awaryjnych oraz powiadamianie administratorów i kadry kierowniczej o zaistniałych incydentach,
   d) współpraca ze służbami dyżurnymi CS.SIS, CS.VIS, EURODAC, innych komórek organizacyjnych KGP oraz służbami dyżurnymi organów administracji państwowej w celu zapewnienia sprawnej komunikacji w zakresie reakcji na powstałe nieprawidłowości w funkcjonowaniu utrzymywanych systemów informatycznych,
   e) współpraca z zespołami serwisowymi podmiotów zewnętrznych w celu jak najszybszego usunięcia zgłoszonych nieprawidłowości,
   f) obsługa dedykowanych narzędzi do komunikacji z systemem centralnym CS.SIS, CS.VIS oraz EURODAC (SPOĆ, OPM, ServiceManager) w trybie 24/7 w ramach krajowego punktu kontaktowego NS.VIS, NS.SIS i NS.EURODAC,
   g) wymiana informacji w ramach punktu kontaktowego do spraw ataków na systemy teleinformatyczne, zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218 z 14.08.2013, str. 8.),
   h) bieżąca współpraca i wymiana informacji z komórkami organizacyjnymi Policji właściwymi do spraw zwalczania cyberprzestępczości,
   i) inicjowanie i uruchamianie procedur reagowania na incydenty komputerowe,
   j) monitorowanie stanu bezpieczeństwa jawnych systemów i sieci teleinformatycznych Policji,
   k) udzielanie pomocy administratorom w trakcie obsługi incydentu,
   l) bieżący, całodobowy monitoring i obsługa systemów bezpieczeństwa Centralnego Węzła Internetowego KGP,
   m) wspieranie użytkowników w zakresie dostępu do usług realizowanych przez Centralny Węzeł Internetowy KGP,
   n) techniczne zarządzanie uprawnieniami użytkowników Centralnego Węzła Internetowego KGP w zakresie dostępu mobilnego i niestandardowych usług,
   o) rozwiązywanie bieżących problemów wynikających z eksploatacji Centralnego Węzła Internetowego KGP,
   p) monitorowanie prawidłowego funkcjonowania zasilania energetycznego oraz układu klimatyzacyjnego serwerowni Centrum Przetwarzania Danych „Bielany",
   q) monitorowanie urządzeń znajdujących się w serwerowni Centrum Przetwarzania Danych „Bielany" i powiadamianie odpowiednich służb o incydentach;

3) Zespołu do spraw Zarządzania Usługami należy w szczególności:
   a) opracowywanie i udział w opracowywaniu analiz, koncepcji i rozwiązań dotyczących budowy, rozwoju i modernizacji Krajowego Systemu Informatycznego,
   b) przeprowadzanie analiz istniejących usług pod kątem ich optymalizacji i lepszego dostosowania do potrzeb odbiorcy,
   c) przestrzeganie harmonogramów narzuconych przez organy Unii Europejskiej oraz planowanie sposobu ich realizacji i wdrożenia, w celu zapewnienia zgodnego z planami wdrażania, modyfikacji i testowania systemów informatycznych.";

6) w § 11 w ust. 1 w pkt 5 w lit. c kropkę zastępuje się średnikiem i dodaje się pkt 6-13 w brzmieniu:
   „6) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo;
   7) analizowanie i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania;
   8) szacowanie ryzyka w obszarze cyberbezpieczeństwa;

9) opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji;
10) sprawowanie nadzoru nad procesem szacowania ryzyka w obszarze cyberbezpieczeństwa;
11) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych;
12) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych;
13) rozpoznawanie zagrożeń cyberbezpieczeństwa.";

7) w § 12 w ust. 1 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8-15 w brzmieniu:
„8) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo;
9) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych;
10) zaawansowana obsługa incydentów;
11) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych;
12) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych;
13) wstępna obsługa incydentów;
14) zabezpieczanie śladów cyfrowych;
15) rozpoznawanie zagrożeń cyberbezpieczeństwa.";

8) w § 13 w ust. 1 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8-35 w brzmieniu:
„8) aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (CyberThreat Intelligence i ThreatHunting);
9) analizowanie złośliwego oprogramowania;
10) badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania;
11) dokonywanie oceny bezpieczeństwa systemów informacyjnych, w tym przeprowadzanie testów penetracyjnych i audytów bezpieczeństwa;
12) prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności;
13) rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa;
14) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo;
15) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych;
16) zaawansowana obsługa incydentów;
17) analiza powłamaniowa;
18) badanie i ocena bezpieczeństwa rozwiązań ICT;
19) projektowanie, budowa i utrzymanie systemów monitorowania i detekcji incydentów oraz wsparcia funkcjonowania operacyjnego centrum bezpieczeństwa (SOC)/Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT);
20) korelacja danych, prowadzenie analiz lub tworzenie map sytuacyjnych;
21) monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
22) prowadzenie analiz incydentów poważnych, powiązań między incydentami oraz opracowywanie wniosków;
23) przyjmowanie zgłoszeń i obsługa incydentów poważnych;
24) reagowanie na incydenty oraz ich klasyfikacja;
25) analizowanie i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania;
26) koordynowanie obsługi zgłoszonych incydentów;
27) realizowanie specjalistycznych zadań w ramach SOC lub Centrum Zarządzania Siecią (NOC) obejmujące monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów;
28) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych;
29) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych;
30) wstępna obsługa incydentów;
31) rozpoznawanie zagrożeń cyberbezpieczeństwa;

32) szacowanie ryzyka w obszarze cyberbezpieczeństwa;
33) przygotowanie rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa, w szczególności podnoszących poziom bezpieczeństwa systemów informacyjnych będących w dyspozycji podmiotów krajowego systemu cyberbezpieczeństwa;
34) opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem w obszarze cyberbezpieczeństwa;
35) sprawowanie nadzoru nad procesem szacowania ryzyka w obszarze cyberbezpieczeństwa.";

9) § 14 otrzymuje brzmienie:

„**§ 14.** 1. Do zadań wspólnych Wydziału Obsługi Końcowego Użytkownika należy:
1) analizowanie złośliwego oprogramowania,
2) badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania,
3) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo,
4) szacowanie ryzyka w obszarze cyberbezpieczeństwa,
5) reagowanie na incydenty oraz ich klasyfikacja,
6) analizowanie i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania,
7) koordynowanie obsługi zgłoszonych incydentów,
8) rozpoznawanie zagrożeń cyberbezpieczeństwa.

2. W Wydziale Obsługi Końcowego Użytkownika do zadań:
1) Sekcji Obsługi Sprzętu Informatycznego należy w szczególności:
a) realizowanie zadań związanych z wypełnianiem potrzeb komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA, CLKP i pozostałych jednostek organizacyjnych Policji w obszarze obejmującym wyposażenie w sprzęt końcowy komputerowy, peryferyjny (urządzenia drukujące, monitory, skanery, zasilacze awaryjne), oprogramowanie, akcesoria, podzespoły i materiały eksploatacyjne informatyki w zakresie właściwości wydziału,
b) realizowanie zadań związanych z zapewnianiem sprzętu informatycznego i materiałów eksploatacyjnych m. in. grupom operacyjno-procesowym, oficerom łącznikowym Policji i Jednostce Specjalnej Polskiej Policji w Kosowie,
c) konfigurowanie, naprawa, modernizacja i konserwacja sprzętu komputerowego oraz urządzeń peryferyjnych użytkowanych w komórkach organizacyjnych KGP, CBŚP, BSWP,CPKP BOA, CLKP, zgodnie z obowiązującymi w tym zakresie przepisami,
d) podłączanie, przenoszenie i konfiguracja urządzeń dostępowych Policyjnej Sieci Transmisji Danych i Internet oraz do sieci lokalnej danej komórki organizacyjnej KGP, CBŚP,BSWP i CPKP BOA,
e) administrowanie urządzeniami wielofunkcyjnymi, pozostającymi we właściwości biura, w komórkach organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP,
f) wykonywanie zadań administratora technicznego stanowisk dostępowych do systemów niejawnych w KGP na podstawie przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756) i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781),
g) weryfikowanie oprogramowania zainstalowanego na sprzęcie informatycznym w komórkach organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP,
h) nadzór nad prawidłową realizacją umów na gwarancyjne i pogwarancyjne usługi naprawcze sprzętu informatycznego na potrzeby komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP oraz jednostek organizacyjnych Policji w ramach zakupów centralnych, w tym zgłaszanie i wydawanie sprzętu do naprawy oraz przyjmowanie po naprawie,
i) wsparcie w zakresie merytorycznym w opracowywaniu opisów przedmiotu zamówienia do wniosków o wszczęcie postępowania o udzielenie zamówienia publicznego zgodnie z przepisami,
j) udział w pracach komisji, zespołów i grup eksperckich, w związku z prowadzonymi w biurze projektami teleinformatycznymi,
k) opracowywanie rozdzielników dotyczących sprzętu i materiałów informatycznych oraz informatycznych materiałów eksploatacyjnych na potrzeby komórek organizacyjnych KGP,

l) prowadzenie aktualnego wykazu sprzętu informatycznego, będącego w rezerwie eksploatacyjnej i dyspozycyjnej oraz pochodzącego ze zwrotów, a także wykazów informatycznych materiałów eksploatacyjnych i podzespołów komputerowych oraz wydawanie i przyjmowanie sprzętu informatycznego zgodnie z rozdzielnikami, zgłaszanymi zapotrzebowaniami i dyspozycjami przełożonych,

m) współpraca w zakresie realizacji zadań związanych z obrotem rzeczowymi składnikami majątku w Systemie Wspomagania Obsługi Policji w obszarze gospodarki materiałowej w zakresie właściwości sekcji,

n) klasyfikowanie sprzętu informatycznego pod kątem sprzętu zbędnego i zużytego oraz jego utylizowanie zgodnie z obowiązującymi przepisami,

o) inicjowanie zmian w zakresie przepisów dotyczących norm należności w kontekście nowych rozwiązań oraz aspektów formalno-prawnych;

2) Sekcji Obsługi Sprzętu Abonenckiego należy w szczególności:

a) realizowanie zadań związanych z wypełnianiem potrzeb komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP i pozostałych jednostek organizacyjnych Policji w obszarze obejmującym wyposażenie w końcowe urządzenia telefonii stacjonarnej i komórkowej, akcesoria, podzespoły i materiały eksploatacyjne łączności w zakresie właściwości wydziału,

b) realizowanie zadań związanych z zapewnieniem sprzętu abonenckiego oraz materiałów eksploatacyjnych łączności m. in. grupom operacyjno-procesowym, oficerom łącznikowym Policji i Jednostce Specjalnej Polskiej Policji w Kosowie,

c) instalowanie i utrzymywanie w sprawności technicznej sprzętu abonenckiego, pracującego w SŁR, resortowej oraz innych operatorów na potrzeby komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP, Ministerstwa Spraw Wewnętrznych i Administracji oraz naczelnych organów administracji rządowej na terenie miasta stołecznego Warszawy,

d) instalowanie i utrzymywanie w sprawności technicznej urządzeń dyspozytorskich opartych na centralach małonumerowych, centrali policyjnej i rządowej na potrzeby komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP, Ministerstwa Spraw Wewnętrznych i Administracji oraz naczelnych organów administracji rządowej na terenie miasta stołecznego Warszawy,

e) obsługa komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP, w zakresie funkcjonowania usług i sprzętu telefonii komórkowej, zgodnie zobowiązującymi w tym zakresie przepisami,

f) wsparcie w zakresie merytorycznym w opracowywaniu opisów przedmiotu zamówienia do wniosków o wszczęcie postępowania o udzielenie zamówienia publicznego zgodnie z przepisami ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, 1812, 1933 i 2185 oraz z 2023 r. poz. 412 i 825), zwaną dalej „PZP",

g) obsługa połączeń między abonentami telefonicznej sieci rządowej i resortowej oraz operatorami sieci publicznych (tel. 7219900),

h) udzielanie informacji o numerach telefonów jednostek organizacyjnych Policji oraz Ministerstwa Spraw Wewnętrznych i Administracji (tel. 7219913),

i) przyjmowanie i obsługa zgłoszeń o uszkodzeniach i zapotrzebowaniu na materiały eksploatacyjne od użytkowników sprzętu teleinformatycznego (tel. 7219910),

j) określanie warunków technicznych dotyczących SŁR i sieci łączności resortowej w zakresie właściwości wydziału oraz opiniowanie dokumentacji technicznej z tym związanej,

k) współpraca z komórkami organizacyjnymi biura oraz obsługą techniczną centrali policyjnej i rządowej w zakresie obsługi telefonicznej SŁR i sieci łączności resortowej,

l) sprawowanie nadzoru nad firmami zewnętrznymi wykonującymi zlecone prace na rzecz KGP w zakresie sieci telefonicznej,

m) sprawowanie nadzoru nad prawidłową realizacją umów na gwarancyjne i pogwarancyjne usługi naprawcze sprzętu łączności na potrzeby komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP oraz innych jednostek organizacyjnych Policji, w ramach zakupów centralnych, w tym

zgłaszanie i wydawanie sprzętu do naprawy oraz przyjmowanie po naprawie,

n) opracowywanie rozdzielników dotyczących sprzętu i materiałów łączności,

o) prowadzenie aktualnego wykazu sprzętu łączności, będącego w rezerwie eksploatacyjnej, dyspozycyjnej oraz pochodzącego ze zwrotów, a także wykazów materiałów łączności (eksploatacyjnych, instalacyjnych, podzespołów i akcesoriów) oraz wydawanie i przyjmowanie sprzętu i materiałów łączności zgodnie z rozdzielnikami, zgłaszanymi zapotrzebowaniami i dyspozycjami przełożonych,

p) realizowanie zadań związanych z obrotem rzeczowymi składnikami majątku w Systemie Wspomagania Obsługi Policji w obszarze gospodarki magazynowej w zakresie właściwości sekcji,

q) klasyfikowanie sprzętu łączności pod kątem sprzętu zbędnego i zużytego oraz jego utylizowanie zgodnie z obowiązującymi przepisami,

r) inicjowanie zmian w zakresie przepisów dotyczących norm należności w kontekście nowych rozwiązań oraz aspektów formalno-prawnych;

3) Sekcji Obsługi Ewidencyjnej należy w szczególności:

a) realizowanie zadań związanych z wypełnianiem potrzeb komórek organizacyjnych KGP, CBŚP, BSWP, CPKP BOA i CLKP oraz pozostałych jednostek organizacyjnych Policji, w obszarze obejmującym oprogramowanie stanowiskowe, oprogramowanie specjalistyczne, dostęp do komercyjnych usług teleinformatycznych świadczonych przez zewnętrzne podmioty, w zakresie właściwości wydziału,

b) obsługa systemu SWOP w zakresie:

- prowadzenie ewidencji środków trwałych, pozostałych środków trwałych, wartości niematerialnych i prawnych, pozostałych wartości niematerialnych i prawnych oraz gospodarki materiałowej, w tym sporządzanie dokumentów obrotu rzeczowymi składnikami majątku w Systemie Wspomagania Obsługi Policji, w zakresie właściwości biura,
- prowadzenie uzgodnień ewidencji ilościowo-wartościowej rzeczowych składników majątku z ewidencją ilościową prowadzoną przez użytkowników w ramach Systemu Wspomagania Obsługi Policji,
- prowadzenie uzgodnień ewidencji ilościowo-wartościowej z ewidencją ilościową prowadzoną w magazynach Biura Logistyki Policji KGP w ramach Systemu Wspomagania Obsługi Policji,
- prowadzenie uzgodnień ewidencji rzeczowych składników majątku oraz rzeczowych aktywów obrotowych pozostających we właściwości biura z ewidencją księgową prowadzoną w Biurze Finansów KGP w ramach Systemu Wspomagania Obsługi Policji przy współpracy z wydziałami merytorycznymi biura,
- wprowadzanie i odbieranie uprawnień użytkownikom Systemu Wspomagania Obsługi Policji w zakresie majątku informatyki i łączności ewidencjonowanego w Module Środków Trwałych oraz w Module Gospodarka Materiałowa zgodnie z upoważnieniami zatwierdzonymi na podstawie aktualnie obowiązującej Polityki Bezpieczeństwa „SWOP",
- sporządzanie sprawozdań w zakresie ewidencji rzeczowych składników majątku, oraz rzeczowych aktywów obrotowych, pozostających we właściwości biura w ramach ewidencji Systemu Wspomagania Obsługi Policji,
- zarządzanie centralnym katalogiem indeksów materiałowych w zakresie grup IN (informatyka) i LA (łączność) w Module Gospodarka Materiałowa oraz Katalogiem Informacji Szczegółowych w Module Środki Trwałe,
- zarządzanie, na podstawie uzgodnień z komórkami organizacyjnymi biura, parametrami i katalogami funkcjonującymi w Systemie Wspomagania Obsługi Policji w zakresie gospodarki materiałowej i środków trwałych,
- sprawowanie nadzoru nad obiegiem dokumentów księgowych w zakresie ewidencji rzeczowych składników majątkowych pozostających we właściwości biura,
- realizacji zadań związanych z obrotem rzeczowymi składnikami majątku w obszarze gospodarki materiałowej,

c) współpraca z lokalnymi administratorami mienia informatycznego w komórkach organizacyjnych KGP, CBŚP, BSWP, CPKP BOA, w zakresie prowadzonej ewidencji,
d) wsparcie w zakresie merytorycznym w opracowywaniu opisów przedmiotu zamówienia do wniosków o wszczęcie postępowania o udzielenie zamówienia publicznego zgodnie z przepisami ustawy PZP;
e) opracowywanie rozdzielników dotyczących oprogramowania,
f) prowadzenie aktualnego wykazu oprogramowania będącego w rezerwie oraz pochodzącego ze zwrotów oraz wydawanie i przyjmowanie oprogramowania zgodnie z rozdzielnikami, zgłaszanymi zapotrzebowaniami i dyspozycjami przełożonych,
g) prowadzenie rozliczeń usług telefonii komórkowej oraz sporządzanie zestawień dotyczących obciążeń użytkowników za połączenia prywatne w celu wystawienia not obciążeniowych,
h) rozliczanie kart obiegowych w zakresie sprzętu teleinformatycznego i telefonii komórkowej oraz stacjonarnej w zakresie właściwości wydziału,
i) dokonywanie wyceny rzeczowych składników majątku, pozostających w dyspozycji wydziału, w związku z przeprowadzanymi inwentaryzacjami,
j) przygotowywanie zestawień różnic inwentaryzacyjnych na podstawie weryfikowanych spisów inwentaryzacyjnych,
k) prowadzenie gospodarki zbędnymi i zużytymi składnikami majątku ruchomego w zakresie sprzętu łączności, informatyki i telefonii komórkowej oraz oprogramowania przy współpracy z komórkami organizacyjnymi KGP, CBŚP, BSWP, CPKP BOA, CLKP,
l) sporządzanie protokołów szkód ujawnionych w wyniku inwentaryzacji oraz szkód w mieniu Skarbu Państwa – KGP, w zakresie środków trwałych, pozostałych środków trwałych, wartości niematerialnych oraz prawnych i pozostałych wartości niematerialnych i prawnych,
m) sporządzanie tabel należności sprzętu teleinformatycznego w zakresie właściwości wydziału,
n) prowadzenie ewidencji abonentów SŁR, resortowej, komórkowej i innych,
o) współpraca z Ministerstwem Spraw Wewnętrznych i Administracji w zakresie edycji spisu abonentów SŁR,
p) sporządzanie i opracowywanie „Krajowego Spisu Abonentów Urządzeń Telekopiowych Sieci POLIFAX-A i Sieci Miejskiej",
q) współpraca z obsługą techniczną centrali policyjnej i rządowej w zakresie obsługi SŁR i sieci łączności resortowej;

4) Zespołu Wsparcia Realizacji Przedsięwzięć należy w szczególności:
a) koordynowanie i realizacja zadań związanych z opracowywaniem, weryfikowaniem dokumentacji projektowej oraz sporządzaniem wniosków o udzielenie zamówień publicznych, a także uczestniczenia w pracach komisji przetargowych, podczas odbiorów jakościowych oraz ilościowych w zakresie sprzętu komputerowego i oprogramowania w celu realizacji ww. zakupów w ramach postępowań przetargowych,
b) koordynowanie działań związanych z implementacją nowych systemów komunikacyjnych i informatycznych,
c) wsparcie procesów związanych z realizacją zadań Sekcji Obsługi Sprzętu Informatycznego, Sekcji Obsługi Sprzętu Abonenckiego, Sekcji Obsługi Ewidencyjnej,
d) koordynowanie działań związanych z przygotowywaniem koncepcji i planów działań, mających na celu zaspokojenie potrzeb, a także udział w działaniach związanych z identyfikacją potrzeb końcowego użytkownika, określaniem tabel należności sprzętu oraz koordynacja i nadzorowanie wycofania z użytku sprzętu przestarzałego i związanej z tym oceny stanu technicznego sprzętu,
e) opracowywanie opisów przedmiotu zamówienia do wniosków o wszczęcie postępowania o udzielenie zamówienia publicznego zgodnie z przepisami ustawy PZP, w zakresie właściwości wydziału,
f) prowadzenie postępowań o udzielenie zamówień publicznych na zakup sprzętu teleinformatycznego, oprogramowania, materiałów eksploatacyjnych łączności i informatyki oraz napraw sprzętu teleinformatycznego zgodnie z przepisami ustawy PZP oraz związanej z tym dokumentacji,

g) sprawdzanie pod względem merytorycznym oraz prowadzenie rejestru faktur wystawionych za zrealizowane dostawy i usługi w zakresie właściwości wydziału,
h) udział w pracach komisji, zespołów i grup eksperckich, w związku z prowadzonymi w biurze projektami teleinformatycznymi oraz przygotowywanie informacji o stanie realizacji tych projektów,
i) opracowywanie rozdzielników dotyczących sprzętu i materiałów teleinformatycznych oraz teleinformatycznych materiałów eksploatacyjnych zakupionych na potrzeby jednostek organizacyjnych Policji,
j) sprawowanie nadzoru nad umowami ramowymi pozostającymi w realizacji przez wydział oraz koordynacja działań i prowadzenie czynności związanych z postępowaniami mających na celu zawarcie umów wykonawczych do umów ramowych,
k) koordynowanie działań związanych z gospodarką środkami finansowymi wydziału.";

10) w § 16:

a) w ust. 1 w pkt 12 kropkę zastępuje się średnikiem i dodaje pkt 13-24 w brzmieniu:

„13) aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (CyberThreat Intelligence i ThreatHunting);
14) analizowanie złośliwego oprogramowania;
15) badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania;
16) dokonywanie oceny bezpieczeństwa systemów informacyjnych, w tym przeprowadzanie testów penetracyjnych i audytów bezpieczeństwa;
17) prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności;
18) rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa;
19) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo;
20) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych;
21) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych;
22) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych;
23) wstępna obsługa incydentów;
24) rozpoznawanie zagrożeń cyberbezpieczeństwa.",

b) w ust. 2 w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6-17 w brzmieniu:

„6) aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (CyberThreat Intelligence i ThreatHunting);
7) analizowanie złośliwego oprogramowania;
8) badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania;
9) dokonywanie oceny bezpieczeństwa systemów informacyjnych, w tym przeprowadzanie testów penetracyjnych i audytów bezpieczeństwa;
10) prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności;
11) rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa;
12) prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwa;
13) prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych;
14) bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych;
15) poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych;
16) wstępna obsługa incydentów;
17) rozpoznawanie zagrożeń cyberbezpieczeństwa.".

§ 2. Decyzja wchodzi w życie z dniem podpisania, z mocą od dnia 1 lutego 2022 r.

DYREKTOR
BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI
insp. Przemysław WIĘCŁAW

2023 -05- 12

PODREFERENDARZ
WYDZIAŁU ANALITYCZNO-KOORDYNACYJNEGO
BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI

Piotr ULEWICZ

NACZELNIK WYDZIAŁU
ANALITYCZNO-KOORDYNACYJNEGO
BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI

mgr Sylwester WAWEREK

Uzasadnienie

Zmiana decyzji nr 97 Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji z dnia 27 maja 2020 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Łączności i Informatyki Komendy Głównej Policji, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych uporządkowuje i dostosowuje realizowane w Biurze Łączności i Informatyki Komendy Głównej Policji zadania do regulacji prawnych, wprowadzonych ustawą z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667) oraz aktem wykonawczym do ww. ustawy, tj. rozporządzeniem Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa.

Wydanie decyzji, sanuje zatem istniejący stan faktyczny, gdyż nowe zadania wynikające z uregulowań prawnych, zawartych w ww. aktach normatywnych, są już wykonywane w Biurze Łączności i Informatyki Komendy Głównej Policji, zaś nadanie wstecznej mocy obowiązywania decyzji od dnia 1 lutego 2022 r., wynika z wejścia w życie z dniem 1 lutego 2022 r., Rozkazu organizacyjnego nr 3/22 z dnia 28 stycznia 2022 r., dot. zmian organizacyjno-etatowych w Biurze Łączności i Informatyki Komendy Głównej Policji, mających na celu usprawnienie działania komórek organizacyjnych BŁiI KGP, poprzez utworzenie w Wydziale Cyberbezpieczeństwa Zespołu do spraw Obsługi Incydentów Cyberbezpieczeństwa w Poznaniu oraz zapewnienia ciągłości kierowania i sprawowania nadzoru w Sekcji do spraw Eksploatacji Wydziału Utrzymania Systemów Informatycznych Policyjnych i Krajowych BŁiI KGP.

Wejście w życie przedmiotowej decyzji nie spowoduje skutków finansowych dla budżetu Policji.