UCHWAŁA NR CXVIII/2432/2020
ZARZĄDU WOJEWÓDZTWA LUBELSKIEGO

z dnia 25 lutego 2020 r.

zmieniająca uchwałę w sprawie uchwalenia Regulaminu Organizacyjnego Urzędu Marszałkowskiego Województwa Lubelskiego w Lublinie

Na podstawie art. 41 ust. 2 pkt 7 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2019 r. poz. 512, z późn. zm.) – Zarząd Województwa Lubelskiego uchwala, co następuje:

§ 1. W Regulaminie Organizacyjnym Urzędu Marszałkowskiego Województwa Lubelskiego w Lublinie stanowiącym załącznik do uchwały Nr XXIX/611/2019 Zarządu Województwa Lubelskiego z dnia 25 marca 2019 r.[1] wprowadza się następujące zmiany:

1) w § 6 ust. 4 otrzymuje brzmienie:
„4. Departamentami Urzędu kierują dyrektorzy, z zastrzeżeniem filii, którymi kierują kierownicy filii oraz Biura Rzecznika Funduszy Europejskich, którym kieruje Rzecznik Funduszy Europejskich.";

2) w § 26:
a) pkt 15 otrzymuje brzmienie:
„15) Dyrektor Departamentu Cyfryzacji i Usług IT oraz 2 zastępców,",
b) uchyla się pkt 25;

3) w § 27:
a) pkt 13 otrzymuje brzmienie:
„13) Departament Cyfryzacji i Usług IT,",
b) uchyla się pkt 23;

4) w § 30:
a) w ust. 2 uchyla się pkt 3,
b) w ust. 3 skreśla się wyrazy „Oddział Informatyki „OP-III.",";

5) w § 36 w ust. 2 w pkt 4 uchyla się lit. f;

6) w § 38 w ust. 2 w pkt 3 uchyla się lit. d i e;

7) § 40 otrzymuje brzmienie:

„§ 40.

DEPARTAMENT CYFRYZACJI I USŁUG IT

1. Pracą Departamentu kieruje Dyrektor przy pomocy 2 zastępców.
2. W Departamencie tworzy się następujące oddziały i stanowiska pracy:
   1) Oddział Obsługi Społeczeństwa Informacyjnego,
      a) kierownik oddziału,
      b) ds. społeczeństwa informacyjnego,
      c) ds. wykluczeń cyfrowych,
      d) ds. zarządzania serwisami internetowymi,

[1] Regulamin Organizacyjny Urzędu Marszałkowskiego Województwa Lubelskiego w Lublinie był zmieniany następującymi uchwałami Zarządu Województwa Lubelskiego: Nr XXXVI/832/2019 z dnia 17 kwietnia 2019 r., Nr LVII/1316/2019 z dnia 9 lipca 2019 r., Nr XCVIII/2027/2019 z dnia 9 grudnia 2019 r., Nr CVIII/2226/2020 z dnia 15 stycznia 2020 r., Nr CIX/2267/2020 z dnia 22 stycznia 2020 r., Nr CXI/2312/2020 z dnia 29 stycznia 2020 r.

e) ds. systemów informatycznych RPO.
2) Oddział Utrzymania i Rozwoju Wojewódzkiej Regionalnej Sieci Szerokopasmowej,
a) kierownik oddziału,
b) ds. zarządzania infrastrukturą sieciową,
c) ds. zarządzania Wojewódzką Regionalną Siecią Szerokopasmową,
d) ds. administrowania Wojewódzką Regionalną Siecią Szerokopasmową,
e) ds. obsługi Operatorów Sieci Dostępowych,
f) ds. utrzymania Wojewódzkiej Regionalnej Sieci Szerokopasmowej,
g) ds. awarii i uszkodzeń na sieci,
h) ds. usług związanych z utrzymaniem Wojewódzkiej Regionalnej Sieci Szerokopasmowej,
i) ds. realizacji zadań Operatora Infrastruktury,
j) ds. lokalizacji i rozwoju Wojewódzkiej Regionalnej Sieci Szerokopasmowej,
k) konserwator infrastruktury Wojewódzkiej Regionalnej Sieci Szerokopasmowej.
3) Oddział Utrzymania Infrastruktury Informatycznej,
a) kierownik oddziału,
b) ds. zarządzania systemami oraz infrastrukturą teleinformatyczną,
c) administrator systemów informatycznych,
d) administrator sieci,
e) ds. sprzętu komputerowego,
f) ds. zarządzania bazami danych,
g) ds. zarządzania infrastrukturą lokalnego systemu informatycznego RPO,
h) ds. sprzętu i oprogramowania RIIP.
4) Zespół Projektów Informatycznych,
a) ds. projektowania i wdrożeń,
b) ds. prac projektowych,
c) ds. tworzenia oprogramowania.
5) Zespół Monitorowania Infrastruktury Teleinformatycznej,
a) ds. monitorowania infrastruktury teleinformatycznej,
b) ds. monitorowania aktywności użytkowników,
c) ds. monitoringu Wojewódzkiej Regionalnej Sieci Szerokopasmowej.
6) Zespół Wsparcia i Certyfikacji,
a) ds. opracowywania strategii oraz rozwoju e-administracji Województwa Lubelskiego,
b) ds. administracyjno-prawnych związanych z działalnością telekomunikacyjną,
c) ds. sprzedaży usług telekomunikacyjnych,
d) ds. ekonomiczno-finansowych.
7) pomoc administracyjna.
8) sekretarka.

3. W znakowaniu spraw Departament Cyfryzacji i Usług IT używa symbolu „DCIT.”, Oddział Obsługi Społeczeństwa Informacyjnego „DCIT-I.”, Oddział Utrzymania i Rozwoju Wojewódzkiej Regionalnej Sieci Szerokopasmowej „DCIT-II.”, Oddział Utrzymania Infrastruktury Informatycznej „DCIT-III.”, Zespół Projektów Informatycznych „DCIT-IV.”, Zespół Monitorowania Infrastruktury Teleinformatycznej „DCIT-V.”, Zespół Wsparcia i Certyfikacji „DCIT-VI”.”;

8) w § 41 w ust. 2 w pkt 4 uchyla się lit. f;

9) w § 45 w ust. 2 w pkt 2 uchyla się lit. d;

10) § 49 otrzymuje brzmienie:

„§ 49.

BIURO BEZPIECZEŃSTWA

1. Pracą Biura kieruje Dyrektor, który pełni funkcję Pełnomocnika ds. Ochrony Informacji Niejawnych, podporządkowany bezpośrednio Marszałkowi, przy pomocy 1 zastępcy.

2. W Biurze tworzy się następujące stanowiska pracy:
   1) kierownik kancelarii tajnej,
   2) inspektor bezpieczeństwa teleinformatycznego,
   3) ds. ochrony informacji niejawnych i oświadczeń majątkowych,
   4) ds. obronnych,
   5) ds. obrony cywilnej,
   6) ds. ppoż,
   7) ds. cyberbezpieczeństwa,
   8) ds. bezpieczeństwa systemów teleinformatycznych,
   9) ds. ochrony danych osobowych,
   10) ds. związanych z realizacją zadań Inspektora Ochrony Danych,
   11) Inspektor Ochrony Danych – podporządkowany bezpośrednio Marszałkowi,
   12) pomoc administracyjna.
3. W znakowaniu spraw Biuro używa symbolu „BB.”, Inspektor Ochrony Danych „BB-I.”.”;

11) uchyla się § 50;

12) w § 58 we wprowadzeniu do wyliczenia wyrazy „Biurem Inspektora Ochrony Danych” zastępuje się wyrazami „Biurem Bezpieczeństwa – Inspektorem Ochrony Danych”;

13) w § 61:

a) w ust. 2 po pkt 10 dodaje się pkt 11 w brzmieniu:
„11) realizacja zadań obronnych w zakresie spraw kadrowych pracowników Urzędu i kierowników jednostek organizacyjnych w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.”,

b) uchyla się ust. 4,

c) w ust. 7 po pkt 10 dodaje się pkt 11 w brzmieniu:
„11) realizacja zadań obronnych w zakresie zabezpieczenia archiwum Urzędu i podległych jednostek organizacyjnych oraz dostępu do informacji publicznej w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.”,

d) w ust. 8 po pkt 2 dodaje się pkt 3 w brzmieniu:
„3) realizacja zadań obronnych w zakresie przychodzącej korespondencji w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.”,

e) w ust. 9 po pkt 8 dodaje się pkt 9 w brzmieniu:
„9) realizacja zadań obronnych w zakresie zaopatrzenia w żywność i inne artykuły przemysłowe w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.”,

f) w ust. 13 po pkt 13 dodaje się pkt 14 w brzmieniu:
„14) współudział w realizacji czynności na poszczególne Moduły zadaniowe po wprowadzeniu poszczególnych stopni alarmowych i stopni alarmowych CRP.”;

14) w § 67 w ust. 4 uchyla się pkt 10;

15) w § 69 w ust. 3 uchyla się pkt 15 i 16;

16) § 71 otrzymuje brzmienie:

„§ 71.

DEPARTAMENT CYFRYZACJI I USŁUG IT

1. Do podstawowego zakresu działania Oddziału Obsługi Społeczeństwa Informacyjnego w Departamencie Cyfryzacji i Usług IT należy w szczególności:
   1) inicjowanie i kształtowanie współpracy samorządowych jednostek administracji publicznej i innych zainteresowanych organizacji oraz podmiotów realizujących zadania publiczne w celu rozwoju społeczeństwa informacyjnego w województwie,

2) promowanie i popularyzowanie zasad funkcjonowania elektronicznej administracji publicznej,
3) współpraca z innymi departamentami w zakresie zadań e-turystyki, e-środowiska, e-zdrowia itp.,
4) utrzymanie trwałości rezultatów Projektu „Wrota Lubelszczyzny – Informatyzacja Administracji”,
5) koordynacja prac nad utrzymaniem trwałości projektów „Przeciwdziałanie wykluczeniu cyfrowemu w województwie lubelskim”,
6) monitoring i pozyskiwanie informacji związanych z zagadnieniem wykluczenia cyfrowego w województwie lubelskim,
7) administracja krajowym i lokalnym systemem informatycznym obsługującym RPO WL,
8) budowa, rozbudowa, administracja oraz modyfikacja serwisów internetowych.

2. Do podstawowego zakresu działania Oddziału Utrzymania i Rozwoju Wojewódzkiej Regionalnej Sieci Szerokopasmowej w Departamencie Cyfryzacji i Usług IT należy w szczególności:

1) realizacja zadań Operatora Infrastruktury,
2) monitoring prawidłowego działania urządzeń telekomunikacyjnych sieci oraz podejmowanie działań w celu sprawnego usuwania przeszkód w ich pracy,
3) przygotowywanie oraz realizacja działań związanych z lokalizacją i rozwojem sieci,
4) administrowanie regionalną siecią szerokopasmową, uruchamianie i rekonfigurowanie nowych elementów sieci,
5) zapewnienie poprawności działania systemów utrzymania oraz monitorowania sieci, podejmowanie działań w celu usunięcia ewentualnych nieprawidłowości,
6) zapewnienie trwałości zrealizowanego Projektu „Sieć Szerokopasmowa Polski Wschodniej – województwo lubelskie”,
7) monitoring nadzorów technicznych oraz współpraca i stały nadzór nad wszystkimi wykonawcami oraz podmiotami zaangażowanymi w utrzymanie, konserwacje i naprawy sieci, zarówno w warstwie pasywnej jak i aktywnej, w tym przygotowywanie zaleceń dotyczących bieżących przeglądów i napraw sieci, usunięcia awarii, usunięcia krytycznych usterek na sieci oraz weryfikacja ich realizacji,
8) przygotowywanie opisu przedmiotu zamówienia dla Zespołu Wsparcia i Certyfikacji z zakresu utrzymania, konserwacji, przeglądów, naprawy infrastruktury pasywnej i aktywnej sieci,
9) prowadzenie nadzorów związanych z realizacją prac, robót budowlanych przy przedsięwzięciach kolidujących z infrastrukturą sieci,
10) realizacja zadań w zakresie zawierania umów oraz obsługi zawartych umów z operatorami telekomunikacyjnymi i innymi podmiotami:
    a) ustalanie i prowadzenie polityki peeringowej z innymi operatorami,
    b) ustalenie i utrzymywanie polityki routingu BGP – z Operatorami Sieci Dostępowych (OSD) oraz innymi operatorami Tier 1, Tier 2,
    c) utrzymywanie kontaktów z RIPE NCC w celu wnioskowania o adresację potrzebną do bieżącej działalności operatorskiej,
11) przygotowywanie oferty rozwiązań technicznych odpowiednich dla konkretnego odbiorcy usług sieciowych:
    a) przygotowanie techniczne realizacji sprzedaży usług telekomunikacyjnych dla Operatorów Sieci Dostępowych na sieci, analiza technicznych możliwości zestawienia wnioskowanej usługi dla OSD oraz ustalenie zakresu zadań, które muszą być zrealizowane w określonym czasie przez każdą ze stron,
    b) weryfikacja danych dotyczących sieci w zakresie baz danych GESUT,
    c) opiniowanie projektów przyłączenia do sieci OSD wymaganych przed podpisaniem umowy szczegółowej z OSD,
    d) uzgadnianie projektów technicznych oraz koordynowanie prac projektowych związanych z przyłączaniem OSD do sieci,
    e) przygotowywanie warunków technicznych podłączenia OSD do sieci,
    f) wykonywanie czynności związanych z asystą przy przyłączaniu OSD do infrastruktury sieci,

g) udział w wizjach lokalnych w terenie/placach budowy, radach budowy, spotkaniach z inwestorami, wykonawcami robót w przypadkach uszkodzenia, awarii, przełożenia lub zabezpieczenia sieci,
h) wprowadzanie danych, weryfikacja i nadzór nad procesami obsługi OSD w CRM,

12) współpraca z jednostkami samorządu terytorialnego w zakresie utrzymania, eksploatacji i rozwoju sieci,
13) bieżąca obsługa i bieżąca aktualizacja systemu paszportyzacji sieci,
14) udział w naradach koordynacyjnych, w tym dokonywanie niezbędnych uzgodnień w sprawach związanych z infrastrukturą sieci,
15) realizacja zadań w zakresie obowiązku zapewnienia dostępu do sieci i świadczenia usług hurtowych,
16) realizacja zadań związanych z zapewnieniem dostaw energii elektrycznej dla Centrum Zarządzania Siecią oraz węzłów sieci,
17) nadzór nad zestawem podręcznym materiałów.

3. Do podstawowego zakresu działania Oddziału Utrzymania Infrastruktury Informatycznej w Departamencie Cyfryzacji i Usług IT należy w szczególności:

1) obsługa informatyczna Urzędu, w tym zakup, zagospodarowywanie, wymiana zużytych i przestarzałych składników wyposażenia komputerowego i oprogramowania,
2) administrowanie infrastrukturą teleinformatyczną zrealizowaną w ramach projektów informatycznych z zakresu e-administracji,
3) zapewnienie sprawnego funkcjonowania systemów i sieci informatycznych oraz przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych,
4) administrowanie oraz rozwijanie lokalnej sieci komputerowej w Urzędzie,
5) zarządzanie i konserwacja infrastrukturą sprzętową znajdującą się w centrach przetwarzania danych,
6) utrzymanie trwałości rezultatów Projektu „Wrota Lubelszczyzny – Informatyzacja Administracji”:
   a) administracja systemami dziedzinowymi wdrożonymi w ramach Projektu,
   b) zabezpieczenie aplikacji przed nieuprawnionymi działaniami osób trzecich,
7) zarządzanie systemami operacyjnymi serwerów, na których pracują systemy dziedzinowe,
8) zarządzanie systemami wirtualizacyjnymi,
9) zarządzanie środowiskiem bazodanowym,
10) zarządzanie środowiskiem kopii danych,
11) prowadzenie centrum certyfikacji niekwalifikowanych podpisów wykorzystywanych w systemach stworzonych w ramach zrealizowanych projektów,
12) administrowanie sprzętem teleinformatycznym i oprogramowaniem RIIP,
13) odbiór sprzętu komputerowego, oprogramowania, systemów oraz usług teleinformatycznych,
14) udzielanie instruktażu i pomocy pracownikom Urzędu, organizowanie i prowadzenie wewnętrznych szkoleń w zakresie użytkowania sprzętu komputerowego i oprogramowania,
15) realizacja zadań obronnych w zakresie zapewnienia łączności informatycznej w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,
16) współudział w realizacji czynności wynikających z poszczególnych Modułów zadaniowych, po wprowadzeniu poszczególnych stopni alarmowych i stopni alarmowych CRP,
17) współudział w funkcjonowaniu stałego dyżuru Marszałka i stanowiska kierowania Marszałka.

4. Do podstawowego zakresu działania Zespołu Projektów Informatycznych w Departamencie Cyfryzacji i Usług IT należy w szczególności:

1) inicjowanie i koordynacja realizowanych przez samorząd województwa projektów wspierających rozwój społeczeństwa informacyjnego,
2) kompleksowa realizacja projektów informatycznych i teleinformatycznych wspierających rozwój społeczeństwa informacyjnego podjętych przez Zarząd Województwa Lubelskiego,

3) rozbudowa funkcjonalności systemów będących własnością Województwa Lubelskiego,
4) budowa, rozbudowa oraz modyfikacja serwisów internetowych,
5) zbieranie i analiza wymagań funkcjonalnych i niefunkcjonalnych do tworzonego oprogramowania,
6) wdrożenia i szkolenia z zakresu wytwarzanego oprogramowania,
7) dokumentowanie, tworzenie instrukcji dla użytkowników systemów informatycznych,
8) stosowanie metodyk projektowych,
9) określanie założeń i celów tworzonych systemów informatycznych
10) opracowywanie studium wykonywalności, monitorowanie projektów pod względem racjonalności finansowej i społecznej,
11) wykonywanie dokumentacji projektowej do opracowywanych systemów informatycznych,
12) tworzenie harmonogramów prac, struktury projektu, procesów i przepływów biznesowych w aplikacjach,
13) tworzenie diagramów encji,
14) stosowanie metodyk projektowych,
15) implementacja opracowanych projektów,
16) tworzenie oprogramowania zgodnie z zasadami SOLID, DRY, stosowanie wzorców projektowych,
17) dokumentowanie tworzonego kodu źródłowego,
18) tworzenie oprogramowania dla nowych i istniejących systemów informatycznych Urzędu,
19) przeprowadzanie testów w tym jednostkowych, integracyjnych oraz akceptacyjnych tworzonego oprogramowania.

5. Do podstawowego zakresu działania Zespołu Monitorowania Infrastruktury Teleinformatycznej w Departamencie Cyfryzacji i Usług IT należy w szczególności:

1) monitorowanie dostępności i wydajności oraz stanu bezpieczeństwa eksploatowanej infrastruktury teleinformatycznej,
2) monitorowanie aktywności użytkowników eksploatowanych systemów teleinformatycznych, wykrywanie naruszeń procedur bezpieczeństwa, zabezpieczanie dowodów naruszeń obowiązujących procedur oraz ustalanie ich sprawców,
3) planowanie i przeprowadzanie testów oprogramowania i systemów,
4) zarzadzanie systemem służącym do agregacji logów systemów i infrastruktury informatycznej,
5) zarządzanie systemem do ochrony aplikacji WEB,
6) monitorowanie i nadzór nad poprawnością działania systemów utrzymania sieci szerokopasmowej,
7) realizacja zadań obronnych w zakresie zapewnienia łączności informatycznej w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,
8) współudział w realizacji czynności wynikających z poszczególnych Modułów zadaniowych, po wprowadzeniu poszczególnych stopni alarmowych i stopni alarmowych CRP,
9) współudział w funkcjonowaniu stałego dyżuru Marszałka.

6. Do podstawowego zakresu działania Zespołu Wsparcia i Certyfikacji w Departamencie Cyfryzacji i Usług IT należy w szczególności:

1) podejmowanie działań na rzecz rozwoju informatyzacji województwa poprzez:
   a) opracowywanie koncepcji rozwoju,
   b) rozpoznawanie najnowszych trendów w obszarze działalności,
   c) przygotowywanie analiz w zakresie sprzętu komputerowego, oprogramowania i systemów informatycznych,
2) podejmowanie działań na rzecz pozyskiwania i efektywnego wykorzystania środków ze źródeł krajowych i zagranicznych na zadania służące rozwojowi społeczeństwa informacyjnego województwa,
3) koordynacja współpracy Departamentu z komórką odpowiedzialną za realizację zamówień publicznych,

4) opracowywanie projektu budżetu oraz monitorowanie wykonania budżetu z zakresu działania Departamentu,
5) sprawozdawczość w zakresie funkcjonowania systemu kontroli zarządczej w ramach Departamentu,
6) nadzór, kontrola, weryfikacja, raportowanie wskaźników KPI,
7) opracowanie i aktualizacja materiałów promocyjnych dotyczących usług Departamentu,
8) ustalanie procesów sprzedaży i obsługi posprzedażnej usług Departamentu,
9) prowadzenie rozliczeń Operatora Infrastruktury na Etapie Operacyjnym,
10) realizacja zadań administracyjno-prawnych związanych z działalnością telekomunikacyjną,
11) realizacja zadań w zakresie zapewnienia praw dysponowania nieruchomością na potrzeby utrzymania i eksploatacji sieci,
12) realizacja zadań związanych z lokalizacją sieci w pasach drogowych dróg publicznych oraz terenach wodnych,
13) realizacja zadań związanych z ubezpieczeniem majątkowym infrastruktury sieci oraz ubezpieczeniem odpowiedzialności cywilnej prowadzonej przez Województwo Lubelskie działalności w zakresie telekomunikacji,
14) realizacja zadań związanych z obsługą roszczeń ubezpieczeniowych związanych z uszkodzeniami infrastruktury sieci dokonanymi przez inwestorów/wykonawców przy realizacji przedsięwzięć kolidujących z infrastrukturą sieci.

7. Departament Cyfryzacji i Usług IT ściśle współpracuje z Biurem Bezpieczeństwa w zakresie bezpieczeństwa systemów teleinformatycznych i cyberbezpieczeństwa, w szczególności poprzez:

1) udostępnienie narzędzi do monitorowania dostępności, wydajności oraz bezpieczeństwa infrastruktury teleinformatycznej,
2) udostępnienie narzędzi do monitorowania aktywności użytkowników i użytkowników uprzywilejowanych w eksploatowanych systemach teleinformatycznych oraz udostępnianie zabezpieczonych dowodów naruszeń obowiązujących procedur,
3) przekazywanie raportów z przeprowadzanych testów oprogramowania i systemów,
4) wgląd z indywidualnego konta użytkownika do sytemu agregacji logów systemowych i infrastruktury teleinformatycznej,
5) raportowanie o zaistniałych atakach cybernetycznych mogących mieć wpływ na bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo, w związku z obowiązkiem zgłaszania zaistniałych incydentów do CSIRT przy Ministerstwie Cyfryzacji,
6) zapewnienie dostępu z indywidualnego konta użytkownika do skanera podatności systemów teleinformatycznych,
7) dostęp do prowadzonego i aktualizowanego na bieżąco repozytorium z dokumentacją funkcjonujących systemów teleinformatycznych,
8) wdrażanie zaleceń Biura Bezpieczeństwa w zakresie bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa wynikających z aktów prawnych.";

17) w § 72 w ust. 4 uchyla się pkt 11;

18) w § 73:

a) w ust. 1 po pkt 12 dodaje się pkt 13 w brzmieniu:

„13) opracowanie oraz bieżąca aktualizacja dokumentacji, podejmowanie czynności organizacyjnych mających na celu przygotowanie w komórce organizacyjnej oraz w podległych jednostkach organizacyjnych zadań obronnych określonych w planie operacyjnym funkcjonowania Urzędu w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.",

b) w ust. 4 po pkt 12 dodaje się pkt 13 w brzmieniu:

„13) opracowanie oraz bieżąca aktualizacja dokumentacji, podejmowanie czynności organizacyjnych mających na celu przygotowanie w komórce organizacyjnej oraz w podległych jednostkach organizacyjnych zadań obronnych określonych w planie

operacyjnym funkcjonowania Urzędu w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.”;

19) w § 74 w ust. 8 po pkt 11 dodaje się pkt 12 w brzmieniu:

„12) opracowanie oraz bieżąca aktualizacja dokumentacji, podejmowanie czynności organizacyjnych mających na celu przygotowanie w komórce organizacyjnej oraz w podległych jednostkach organizacyjnych zadań obronnych określonych w planie operacyjnym funkcjonowania Urzędu w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.”;

20) w § 76 w ust. 2 uchyla się pkt 12 i 14;

21) § 80 otrzymuje brzmienie:

„§ 80.

BIURO BEZPIECZEŃSTWA

1. Do podstawowego zakresu działania Biura Bezpieczeństwa należy w szczególności:

1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego,
2) zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne,
3) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka,
4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, a w szczególności okresowa kontrola ewidencji, materiałów i obiegu dokumentów,
5) sporządzanie planów i dokumentacji przewidzianych ustawą o ochronie informacji niejawnych oraz ich aktualizacja,
6) organizowanie i prowadzenie szkoleń dla pracowników Urzędu w zakresie ochrony informacji niejawnych, ochrony danych osobowych i cyberbezpieczeństwa,
7) przeprowadzanie zwykłych oraz kontrolnych postępowań sprawdzających,
8) zapewnienie funkcjonowania kancelarii tajnej, odpowiedzialnej za rejestrowanie, przechowywanie, obieg i wydawanie materiałów niejawnych,
9) przyjmowanie oświadczeń majątkowych osób zobowiązanych do ich składania Marszałkowi oraz oświadczeń majątkowych radnych składanych Przewodniczącemu Sejmiku, w tym:
   a) egzekwowanie złożenia oświadczeń majątkowych w terminie przewidzianym prawem,
   b) anonimizowanie i umieszczanie oświadczeń majątkowych zgodnie z obowiązującymi przepisami w Biuletynie Informacji Publicznej Urzędu,
   c) analizowanie oświadczeń majątkowych,
   d) przekazywanie oświadczeń majątkowych do właściwych urzędów skarbowych,
   e) sporządzanie wniosków do Centralnego Biura Antykorupcyjnego o kontrolę oświadczeń majątkowych,
   f) sporządzanie rocznych informacji o oświadczeniach majątkowych,
   g) niezwłoczne informowanie Marszałka i Przewodniczącego Sejmiku o zauważonych nieprawidłowościach w oświadczeniach majątkowych, w szczególności o naruszeniu przez osoby składające oświadczenia majątkowe ustawowych zakazów dotyczących pełnienia określonych funkcji i prowadzenia działalności gospodarczej,
   h) przechowywanie oświadczeń majątkowych,
10) opracowanie i aktualizacja kompleksowej dokumentacji planistyczno-obronnej w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,
11) opracowanie i aktualizacja dokumentacji przygotowań podmiotów leczniczych podległych i nadzorowanych przez Marszałka na potrzeby obronne państwa,

12) współuczestnictwo w realizacji zadań systemu obronnego samorządu województwa, w tym:
    a) zadań społeczno-gospodarczych związanych z potrzebami obronnymi państwa,
    b) bezpieczeństwa i porządku prawnego na tle mogących wystąpić zagrożeń,
    c) obrony cywilnej, w tym udziału w powszechnym systemie ratownictwa, ochrony dóbr materialnych i kultury,
13) prowadzenie spraw wynikających z przepisów ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej,
14) przeprowadzanie kontroli z zakresu realizacji zadań obronnych w wojewódzkich samorządowych jednostkach organizacyjnych,
15) organizacja i koordynacja działalności szkoleniowej i upowszechniającej w zakresie problematyki obronnej, zarządzania kryzysowego, ochrony ludności i obrony cywilnej oraz uczestniczenie w treningach, ćwiczeniach, a także w szkoleniach obronnych organizowanych przez organy administracji rządowej i sił zbrojnych,
16) współuczestnictwo w realizacji zadań Punktu Kontaktowego systemu wsparcia przez państwo gospodarza (Host Nation Support – HNS) zgodnie z zakresem działalności odpowiednich komórek organizacyjnych Urzędu,
17) sporządzanie wniosków i zawiadomień w sprawie reklamowania od obowiązku pełnienia czynnej służby wojskowej radnych i odpowiednich pracowników Urzędu, objętych reklamowaniem z urzędu lub na wniosek,
18) współpraca ze służbami Wojewody Lubelskiego oraz z jednostkami wojskowymi, policji, państwowej straży pożarnej i innymi służbami mundurowymi w zakresie zadań obronnych i kryzysowych,
19) organizacja funkcjonowania stałego dyżuru Marszałka i stanowiska kierowania Marszałka, a także szkolenie ich obsady, zgodnie z wytycznymi Wojewody Lubelskiego,
20) opracowanie i realizacja czynności wynikających z poszczególnych Modułów zadaniowych po wprowadzeniu odpowiednich stopni alarmowych, stopni alarmowych CRP,
21) wykonywanie zadań zarządzania kryzysowego, w tym planowania cywilnego przewidzianych do realizacji przez zarząd województwa,
22) współpraca z Szefem Obrony Cywilnej Kraju oraz ze służbami administracji rządowej i samorządowej województwa lubelskiego, w których swoje siedziby ma Urząd, filie Urzędu i wojewódzkie samorządowe jednostki organizacyjne w zakresie obrony cywilnej,
23) organizacja, planowanie i szkolenie Formacji Obrony Cywilnej (FOC) – drużyny ratownictwa ogólnego do prowadzenia działań ratunkowych w obiektach Urzędu,
24) wykonywanie czynności z zakresu ochrony przeciwpożarowej zgodnie z ustawą o ochronie przeciwpożarowej, a w szczególności:
    a) kontrola przestrzegania przeciwpożarowych wymagań techniczno-budowlanych, instalacyjnych i technologicznych,
    b) kontrola wyposażenia budynków w wymagane urządzenia przeciwpożarowe i gaśnice,
    c) zapewnienie konserwacji oraz napraw urządzeń przeciwpożarowych i gaśnic w sposób gwarantujący ich sprawne i niezawodne funkcjonowanie,
    d) zapewnienie osobom przebywającym w budynku, obiekcie budowlanym lub na terenie, bezpieczeństwa i możliwości ewakuacji oraz przygotowanie budynku, obiektu budowlanego lub terenu do prowadzenia akcji ratowniczej w tym przeprowadzanie praktycznego sprawdzenia organizacji oraz warunków ewakuacji z całego obiektu,
    e) zapoznanie pracowników z przepisami przeciwpożarowymi,
    f) ustalenie sposobów postępowania na wypadek powstania pożaru, klęski żywiołowej lub innego miejscowego zagrożenia,
    g) udział w opracowywaniu instrukcji bezpieczeństwa pożarowego dla obiektu budowlanego oraz jej aktualizacja według potrzeb,
25) analiza działań administratorów w zakresie monitorowania aktywności użytkowników w systemach informatycznych,

26) projektowanie i wdrażanie środków technicznych i organizacyjnych mających na celu zwiększenie bezpieczeństwa teleinformatycznego,
27) opiniowanie planowanych rozwiązań teleinformatycznych oraz wprowadzanych procedur i regulacji wewnętrznych pod kątem ich wpływu na bezpieczeństwo teleinformatyczne,
28) monitorowanie zgodności systemu teleinformatycznego Urzędu z wymaganiami rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności,
29) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych w systemach teleinformatycznych Urzędu,
30) szacowanie ryzyka wystąpienia incydentu naruszenia bezpieczeństwa,
31) analiza przyczyn oraz wyjaśnienie incydentów bezpieczeństwa IT,
32) wykrywanie i zarządzanie podatnością na ataki cybernetyczne,
33) przygotowywanie raportów dotyczących incydentów IT,
34) zarządzanie ujawnionym w Urzędzie incydentem bezpieczeństwa informacji, w tym przygotowywanie zgłoszenia zgodnie z wytycznymi i w trybie wskazanym przez CSIRT NASK,
35) współpraca z jednostkami CERT w szczególności z CSIRT przy Ministerstwie Cyfryzacji,
36) prowadzenie kontroli w systemach teleinformatycznych z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa, zgodnie z Rozporządzeniem Rady Ministrów z dnia 20 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
37) monitorowanie realizacji zaleceń pokontrolnych wydanych w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa,
38) zabezpieczanie dowodów z naruszeń bezpieczeństwa teleinformatycznego oraz prowadzenie postępowań wyjaśniających w przedmiotowym zakresie,
39) współpraca z administratorami systemów informatycznych w celu zapewnienia funkcjonowania systemów informatycznych zgodnie z wymaganiami i zasadami bezpieczeństwa,
40) współpraca z komórką do spraw usług IT Urzędu w zakresie wykrywania incydentów naruszenia bezpieczeństwa systemów teleinformatycznych,
41) opiniowanie projektów umów, których realizacja może mieć wpływ na bezpieczeństwo teleinformatyczne,
42) przygotowywanie upoważnień do przetwarzania danych osobowych dla osób niebędących pracownikami Urzędu,
43) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
44) zapoznawanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Urzędzie,
45) opracowywanie oraz wdrażanie dokumentacji dotyczącej bezpieczeństwa informacji i ochrony danych osobowych, nadzorowanie i monitorowanie obowiązku informacyjnego,
46) prowadzenie i aktualizacja rejestrów czynności i kategorii czynności przetwarzania danych osobowych, o których mowa w art. 30 RODO,
47) prowadzenie spraw z zakresu punktu kontaktowego dla osób, których dane są przetwarzane w Urzędzie,
48) koordynacja i wsparcie w analizie ryzyka naruszenia praw lub wolności osób fizycznych prowadzonej przez komórki organizacyjne,
49) współpraca z Inspektorem Ochrony Danych w zakresie analizowania i opiniowania umów powierzenia, klauzul zgód, klauzul informacyjnych wdrażanych przez komórki organizacyjne,
50) udział w audytach prowadzonych przez Inspektora Ochrony Danych z zakresu przestrzegania przepisów ochrony danych osobowych.

2. Do podstawowego zakresu działania Inspektora Ochrony Danych należy w szczególności:

1) wykonywanie obowiązków zgodnie z art. 39 RODO tj.:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia – RODO, oraz innych przepisów Unii lub krajowych o ochronie danych i doradzanie im w tej sprawie,
   b) monitorowanie przestrzegania rozporządzenia – RODO, innych przepisów Unii lub krajowych o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
   d) współpraca z organem nadzorczym,
   e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
2) przeprowadzanie audytów zgodności przetwarzania danych osobowych z przepisami ochrony danych osobowych,
3) monitorowanie przestrzegania w Urzędzie przepisów o ochronie danych osobowych a także regulacji wewnętrznych obowiązujących w Urzędzie,
4) zapewnienie działań o charakterze edukacyjnym w obszarze ochrony danych osobowych,
5) wspieranie w opracowywaniu oraz wdrażaniu dokumentacji dotyczącej ochrony danych osobowych,
6) przyjmowanie zgłoszenia o naruszeniu ochrony danych osobowych, dokonywanie jego oceny oraz zgłaszanie organowi nadzorczemu faktu naruszenia,
7) prowadzenie rejestru naruszeń ochrony danych,
8) opiniowanie umów powierzenia, klauzul zgód, klauzul informacyjnych wdrażanych przez komórki organizacyjne.”;

22) uchyla się § 81;

23) załącznik „Graficzny schemat wewnętrznej struktury organizacyjnej Urzędu Marszałkowskiego” otrzymuje brzmienie jak w załączniku do niniejszej uchwały.

§ 2. Przyjmuje się tekst jednolity Regulaminu Organizacyjnego Urzędu Marszałkowskiego Województwa Lubelskiego w Lublinie uwzględniający zmiany wprowadzone niniejszą uchwałą, stanowiący załącznik do niniejszej uchwały.

§ 3. Wykonanie uchwały powierza się Marszałkowi Województwa Lubelskiego.

§ 4. Uchwała wchodzi w życie z dniem 1 marca 2020 r.

Członek Zarządu

Sebastian Trojak

Marszałek Województwa

Jarosław Stawiarski