UCHWAŁA NR 1275/16
Zarządu Województwa Świętokrzyskiego
z dnia 17marca 2016r.

w sprawie wprowadzenia zmian w Regulaminie Organizacyjnym Urzędu Marszałkowskiego Województwa Świętokrzyskiego w Kielcach.

Na podstawie art. 41 ust. 2 pkt 7 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2015 r. poz. 1392 z późn. zm.) uchwala się, co następuje:

§ 1.

W Regulaminie Organizacyjnym Urzędu Marszałkowskiego Województwa Świętokrzyskiego w Kielcach, stanowiącym załącznik do uchwały Nr 841/11 Zarządu Województwa Świętokrzyskiego z dnia 30 grudnia 2011r. (zmiana: uchwała Nr 1278/12 z dnia 8 sierpnia 2012r.; uchwała Nr 1786/13 z dnia 28 marca 2013r.; uchwała Nr 1800/13 z dnia 3 kwietnia 2013r.; Nr 2550/14 z dnia 20 lutego 2014r.; Nr 2870/14 z dnia 9 lipca 2014r.; Nr 2883/14 z dnia 16 lipca 2014r.; Nr 2930/14 z dnia 6 sierpnia 2014r.; Nr 2993/14 z dnia 3 września 2014r.; Nr 3032/14 z dnia 17 września 2014r.; Nr 1/14 z dnia 5 grudnia 2014r.; Nr 63/14 z dnia 17 grudnia 2014r.; Nr 335/15 z dnia 15 kwietnia 2015r.; Nr 764/15 z dnia 14 października 2015r.: Nr 822/15 z dnia 5 listopada 2015r.; Nr 1026/15 z dnia 23 grudnia 2015r. oraz Nr 1243/16 z dnia 2 marca 2016r.) wprowadza się następujące zmiany:

1) w § 12 ust.1 skreśla się tiret czwarty,
2) w § 40 ust.2 pkt 6 otrzymuje brzmienie:

6)	Biuro Spraw Obronnych, Bezpieczeństwa i Ochrony Informacji	symbol	BSO

3) w § 58 dodaje się pkt 4 i 5 o treści:

4)	Oddział Koordynacji Instytucji Pośredniczącej RPOWŚ 2014 – 2020 WUP i Kontroli	symbol	ROPS- IV
5)	Stanowisko ds. Organizacyjnych	symbol	ROPS-V

4) rozdział 17 otrzymuje brzmienie jak w załączniku Nr 1 do niniejszej uchwały,
5) w § 96 skreśla się pkt 3,
6) w § 98 skreśla się pkt 14 – 20,
7) w § 101 pkt 1 otrzymuje brzmienie:

1)	Oddział Planowania i Organizacji Transportu	symbol	WZT - I

§ 2.

Dyrektor Departamentu Organizacyjno – Administracyjnego opracuje i opublikuje jednolity tekst Regulaminu, obejmujący dotychczas wprowadzone zmiany.

§ 3.

Uchwała wchodzi w życie z dniem podjęcia.

Marszałek Województwa

Adam Jarubas

Załącznik Nr 1 do uchwały Nr 1275/16 Zarządu
Województwa Świętokrzyskiego z dnia 17 marca 2016r.

ROZDZIAŁ 17
BIURO SPRAW OBRONNYCH, BEZPIECZEŃSTWA I OCHRONY INFORMACJI

§ 91. 1. W skład Biura Spraw Obronnych, Bezpieczeństwa i Ochrony Informacji w chodzą następujące komórki organizacyjne:

1)	Kancelaria Materiałów Niejawnych	symbol	BSO -I
2)	Jednoosobowe stanowisko ds. obronnych	symbol	BSO -II
3)	Jednoosobowe stanowisko ds. bezpieczeństwa publicznego	symbol	BSO -III
4)	Administrator Bezpieczeństwa Informacji, Inspektor Bezpieczeństwa Teleinformatycznego	symbol	BSO -IV
5)	Jednoosobowe Stanowisko ds. Kontroli Systemów, Sieci i Bezpieczeństwa Teleinformatycznego oraz Administrowania Systemem BSK.	symbol	BSO -V

2. Biurem Spraw Obronnych, Bezpieczeństwa i Ochrony Informacji kieruje dyrektor.

3. Dyrektor Biura Spraw Obronnych, Bezpieczeństwa i Ochrony Informacji pełni jednocześnie obowiązki Pełnomocnika ds. Ochrony Informacji Niejawnych. Pełnomocnik w zakresie realizacji swoich zadań współpracuje z właściwymi jednostkami i komórkami organizacyjnymi służb ochrony państwa. O przebiegu tej współpracy na bieżąco informuje Marszałka Województwa.

4. W strukturze Biura Spraw Obronnych, Bezpieczeństwa i Ochrony Informacji funkcjonuje Administrator Bezpieczeństwa Informacji, bezpośrednio podlegający Marszałkowi Województwa (art.36a ust.7 ustawy z dnia 29 sierpnia 1997r.o ochronie danych osobowych – Dz. U. z 2015r. poz.2135 z późn. zm.).Pełni on również funkcję Inspektora Bezpieczeństwa Teleinformatycznego systemu TI – Bezpiecznego Stanowiska Komputerowego, w zakresie której podlega Pełnomocnikowi ds. Ochrony Informacji Niejawnych (art.52 ust.1 pkt 1 ustawy z dnia 5 sierpnia 2010r. o ochronie Informacji niejawnych – Dz. U. z 2010r. Nr 182, poz.1228 z późn. zm.).

§ 92. Do zakresu zadań Biura Spraw Obronnych, Bezpieczeństwa i Ochrony Informacji w szczególności należy:

1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego,
2) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka,
3) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów ochronie tych informacji,
4) opracowanie i aktualizowanie planu ochrony informacji niejawnych oraz instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Urzędzie i nadzorowanie jego realizacji,

5) szkolenie pracowników Urzędu Marszałkowskiego i podległych jednostek organizacyjnych w zakresie ochrony informacji niejawnych,
6) przeprowadzanie zwykłych postępowań sprawdzających oraz kontrolnego wobec pracowników Urzędu oraz kierowników i pracowników samorządowych jednostek organizacyjnych których obowiązki wymagają dostępu do informacji niejawnych,
7) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto,
8) przekazywanie ABW do ewidencji, o których mowa w art. 73 ust. 1 ustawy o ochronie informacji niejawnych , danych, o których mowa w art. 73 ust. 2, osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa,
9) opracowanie „szczegółowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (SWB)", w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne,
10) podejmowanie działań zmierzających do zapewnienia ochrony fizycznej, elektromagnetycznej systemu w ramach BSK,
11) kontrolowanie dostępu do BSK przez określenie warunków i sposobu przydzielania uprawnień ich użytkownikom,
12) bieżąca kontrola zgodności funkcjonowania systemu lub sieci teleinformatycznej z SWB,
13) zgłaszanie zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Danych Osobowych,
14) zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
15) właściwe rejestrowanie, przechowywanie i wydawanie dokumentów zawierających informacje niejawne
16) bezpośredni nadzór nad obiegiem dokumentów niejawnych w Urzędzie
17) ustalenie zasad wytwarzania, przetwarzania, przechowywania, przekazywania i przewożenia dokumentów zawierających informacje niejawne oznaczone klauzulą „poufne" lub stanowiących tajemnicę o wyższej klauzuli w Urzędzie
18) opracowanie i wdrażanie kompleksowej dokumentacji planistyczno-obronnej na czas pokoju, zagrożenia bezpieczeństwa państwa i wojny,
19) określenie, w ramach planowania operacyjnego – zadań do realizacji przez departamenty i komórki równorzędne Urzędu i podległe im jednostki organizacyjne w zakresie obronności na okres zagrożenia bezpieczeństwa państwa i wojny oraz nadzór nad ich realizacją,
20) organizowanie szkoleń oraz sporządzanie i aktualizowanie dokumentacji w zakresie spraw obronnych wynikające z ustaw
21) wykonywanie zadań bezpieczeństwa publicznego w ramach właściwości przewidzianych do realizacji przez samorząd województwa;
22) wykonywanie zadań zarządzania kryzysowego, w tym planowania cywilnego, w ramach właściwości przewidzianych do realizacji przez zarząd województwa, wynikających z jego kompetencji;
23) realizacja zadań ochrony przeciwpowodziowej, a w szczególności wyposażenia i utrzymania wojewódzkich samorządowych magazynów przeciwpowodziowych;

24) realizacja zadań obrony cywilnej, w tym udziału w powszechnym systemie ratownictwa, ochrony ludności, dóbr materialnych i kultury w jednostkach organizacyjnych samorządu województwa,
25) kontrola zabezpieczeń systemów i bezpieczeństwa sieci teleinformatycznych,
26) kontrola użytkowanych programów komputerowych pod kątem ich legalności pozyskania i zgodności z umową licencyjną,
27) kontrola sprzętu komputerowego i oprogramowania pod względem zgodności z ewidencją wyposażenia,
28) prowadzenie kontroli przetwarzania danych osobowych w systemie teleinformatycznym,
29) kontrola projektów realizowanych w ramach funduszy Unii Europejskiej w zakresie zagadnień teleinformatycznych,
30) opracowywanie i wdrażanie Globalnej Polityki Bezpieczeństwa Informacji,
31) realizacja ustawy o ochronie danych osobowych w zakresie kontroli dotyczących bezpieczeństwa informacji oraz innych ustaw i przepisów niższego rzędu odnoszących się do ochrony informacji, z wyłączeniem informacji niejawnych (nieklasyfikowanych).