

ZATWIERDZAM

MINISTER FINANSÓW

Tadeusz Kościński

/podpisano kwalifikowanym
podpisem elektronicznym/

REGULAMIN ORGANIZACYJNY
CENTRUM INFORMATYKI
RESORTU FINANSÓW

Rozdział 1 Przepisy ogólne

§ 1.

Centrum Informatyki Resortu Finansów, zwane dalej „Centrum”, działa:

- 1) na podstawie statutu Centrum Informatyki Resortu Finansów, stanowiącego załącznik do zarządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 27 listopada 2020 r. w sprawie nadania statutu Centrum Informatyki Resortu Finansów (Dz. Urz. Min. Fin., Fun. i Pol. Reg. poz. 21);
- 2) zgodnie z niniejszym regulaminem, zarządzeniami, decyzjami, wytycznymi i poleceniami ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych lub osoby, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum oraz Dyrektora Centrum.

§ 2.

Regulamin określa szczegółową strukturę organizacyjną, tryb pracy i zakresy działania poszczególnych komórek organizacyjnych Centrum. Przez komórkę organizacyjną należy rozumieć wyodrębnioną pod względem właściwości merytorycznej część Centrum, powołaną do realizacji zadań wynikających z regulaminu organizacyjnego Centrum, w tym departamenty, oddziały, wydziały, zespoły, sekcje, wieloosobowe stanowiska pracy.

Rozdział 2 Struktura organizacyjna

§ 3.

W skład Kierownictwa Centrum wchodzi:

- 1) Dyrektor Centrum (D);
- 2) Dyrektor Pionu do Spraw Administracyjnych, pełniący rolę zastępcy dyrektora Centrum (ZD1);
- 3) Dyrektor Pionu do Spraw Infrastruktury, pełniący rolę zastępcy Dyrektora Centrum (ZD2);
- 4) Dyrektor Pionu do Spraw Rozwoju i Utrzymania Aplikacji, pełniący rolę zastępcy Dyrektora Centrum (ZD3);
- 5) Dyrektor Pionu do Spraw Informatyki Resortu Finansów, pełniący rolę zastępcy Dyrektora Centrum (ZD4).

§ 4.

1. W skład Centrum wchodzi następujące komórki organizacyjne:
 - 1) Pion do Spraw Administracyjnych, w którego skład wchodzi:
 - a) Departament Kadr (DK), w którego skład wchodzi:
 - Wydział Kadr (DK1),
 - Wydział Płac (DK2),
 - b) Departament Finansów (DF), w którego skład wchodzi:
 - Wydział Zarządzania Finansami (DF1),
 - Wydział Monitorowania i Rozliczania Umów (DF2),
 - Wydział Księgowości i Płatności (DF3),
 - c) Departament Zakupów (DZ), w którego skład wchodzi:
 - Wydział Zamówień Publicznych (DZ1),
 - Wydział Obsługi Procesów (DZ2),
 - d) Departament Logistyki (DL), w którego skład wchodzi:
 - Wydział Zarządzania Mieniem i Transportu (DL1),
 - Wydział Zarządzania Nieruchomościami (DL2),
 - Wydział Gospodarczy (DL3),

- Wydział Organizacyjny (DL4),
- e) Wieloosobowe stanowisko pracy do spraw bezpieczeństwa i higieny pracy (BHP);
- 2) Pion do Spraw Infrastruktury, w którego skład wchodzi:
 - a) Departament Utrzymania Infrastruktury Technicznej (DUT), w którego skład wchodzi:
 - Wydział Utrzymania Obiektów Przetwarzania Danych (DUT1),
 - Wydział Ochrony Informacji (DUT2),
 - Wydział Bezpieczeństwa Teleinformatycznego (DUT3),
 - Wydział Wewnętrznej Służby Ochrony (DUT4),
 - Inspektor Ochrony Przeciwpożarowej (DUT5),
 - b) Departament Sieci, Usług i Monitorowania (DSM), w którego skład wchodzi:
 - Wydział Projektów i Usług (DSM1),
 - Wydział Systemów Monitorowania Infrastruktury (DSM2),
 - Wydział Wsparcia i Monitorowania (DSM3),
 - Wydział Telekomunikacji (DSM4),
 - Wydział Zarządzania Siecią Rozległą (DSM5),
 - c) Departament Infrastruktury Teleinformatycznej (DIT), w którego skład wchodzi:
 - Wydział Serwerów Aplikacji i Baz Danych (DIT1),
 - Wydział Systemów Infrastrukturalnych (DIT2),
 - Wydział Integracji i Nowych Technologii (DIT3);
- 3) Pion do Spraw Rozwoju i Utrzymania Aplikacji, w którego skład wchodzi:
 - a) Departament Rozwoju i Utrzymania Aplikacji Podatkowych (DAP), w którego skład wchodzi:
 - Wydział Architektury IT (DAP1),
 - Wydział Inżynierii Wymagań (DAP2),
 - Wydział Wytwarzania Oprogramowania (DAP3),
 - Wydział Jakości Oprogramowania (DAP4),
 - Wydział Systemów Poboru Podatków (DAP5),
 - Wydział Zarządzania Projektami (DAP6),
 - b) Departament Rozwoju i Utrzymania Aplikacji Analitycznych, Celnych i Budżetowych (DAB), w którego skład wchodzi:
 - Wydział Zarządzania Usługami IT (DAB1),
 - Wydział Systemów Budżetowych (DAB2),
 - Wydział Systemów Celnych (DAB3),
 - Wydział Systemów Analitycznych (DAB4),
 - c) Departament Wsparcia Informatycznego i Utrzymania Stacji Roboczych (DWU), w którego skład wchodzi:
 - Wydział Centralnego Service Desku (DWU1),
 - Wydział Aplikacji i Oprogramowania Stacji Roboczych (DWU2),
 - Wydział Infrastruktury Komputerowej i Logistyki Informatycznej (DWU3),
 - Wydział Wsparcia Informatycznego (DWU4),
 - Wydział Sieci LAN w Ministerstwie Finansów (DWU5),
 - d) Departament Rozwoju i Utrzymania Aplikacji e-Usługowych oraz Aplikacji Gospodarki Własnej (DEG), w którego skład wchodzi:
 - Wydział Systemów Gospodarki Własnej i Wsparcia Zarządzania (DEG1),
 - Wydział Rozwoju i Utrzymania Aplikacji e-Usługowych (DEG2),
 - Wydział Automatykacji i Robotyzacji (DEG3);
- 4) Pion do Spraw Informatyki Resortu Finansów, w którego skład wchodzi:
 - a) Departament Zarządzania Regionem Zachodnim (RZA), w którego skład wchodzi:
 - Biuro Wsparcia (RZA1BW),

- Oddział Zarządzania Regionem Wielkopolskim (RZA2), w którego skład wchodzi:
 - Zespół Planowania i Logistyki Informatycznej oraz Bezpieczeństwa Informatycznego (RZA2WIIP),
 - Zespół Infrastruktury Sieciowej i Serwerowej (RZA2WIIS),
 - Zespół Helpdesk oraz Systemów Lokalnych i Bazy Wiedzy (RZA2WIIH),
 - Pierwszy Zespół Wsparcia Informatycznego (RZA2WIIW1),
 - Drugi Zespół Wsparcia Informatycznego (RZA2WIIW2),
 - Trzeci Zespół Wsparcia Informatycznego (RZA2WIIW3),
 - Czwarty Zespół Wsparcia Informatycznego (RZA2WIIW4),
 - Piąty Zespół Wsparcia Informatycznego (RZA2WIIW5),
 - Zespół Systemów Centralnych (RZA2WIIC),
 - Zespół Wsparcia Rejestracji Obsługi Wniosków (RZA2WIIR),
- Oddział Zarządzania Regionem Dolnośląskim (RZA3), w którego skład wchodzi:
 - Wydział Systemów Centralnych i Lokalnych, Bazy Wiedzy, Help Desk, Bezpieczeństwa i Licencji oraz Infrastruktury Sieciowej i Serwerowej (RZA3IIT-1), w którego skład wchodzi:
 - Zespół Bezpieczeństwa Informatycznego (RZA3DIID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy oraz Help Desk (RZA3DIIL),
 - Zespół Systemów Centralnych (RZA3DIIC),
 - Zespół Infrastruktury Sieciowej i Serwerowej (RZA3DIIS),
 - Sekcja Planowania i Logistyki Informatycznej (RZA3DIIP),
 - Wydział Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIT-2), w którego skład wchodzi:
 - Pierwszy Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW1),
 - Drugi Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW2),
 - Trzeci Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW3),
 - Czwarty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW4),
 - Piąty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW5),
 - Szósty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW6),
- Oddział Zarządzania Regionem Łódzkim (RZA4), w którego skład wchodzi:
 - Zespół Help Desk oraz Systemów Lokalnych i Bazy Wiedzy (RZA4LIH),
 - Zespół Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RZA4LIID),
 - Zespół Planowania i Logistyki Informatycznej, Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RZA4LIIP),
 - Pierwszy Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA4LIW-1),
 - Drugi Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA4LIW-2),
- Oddział Zarządzania Regionem Lubuskim (RZA5), w którego skład wchodzi:
 - Pierwszy Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i

- Serwerowej, Bezpieczeństwa Informatycznego, Systemów Lokalnych i Bazy Wiedzy, Helpdesk, Planowania i Logistyki Informatycznej (RZA5FIIW-1) – zadania wykonywane dla izby administracji skarbowej,
 - Drugi Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej, Bezpieczeństwa Informatycznego, Systemów Lokalnych i Bazy Wiedzy, Helpdesk, Planowania i Logistyki Informatycznej (RZA5FIIW-2) – zadania wykonywane dla urzędów skarbowych województwa lubuskiego i dla Lubuskiego Urzędu Celno-Skarbowego,
 - Zespół Systemów Centralnych, Systemów Lokalnych i Bazy Wiedzy, Bezpieczeństwa Informatycznego, Helpdesk, Infrastruktury Sieciowej i Serwerowej (RZA5FIIC),
 - Zespół Bezpieczeństwa Informatycznego, Helpdesk, Infrastruktury Sieciowej i Serwerowej, Planowania i Logistyki Informatycznej (RZA5FIID),
- b) Departament Zarządzania Regionem Południowym (RPD), w którego skład wchodzi:
- Biuro Wsparcia (RPD1BW),
 - Oddział Zarządzania Regionem Śląskim (RPD2), w którego skład wchodzi:
 - Wydział Helpdesk, Systemów Centralnych, Bezpieczeństwa, Programowania oraz Planowania i Logistyki Informatycznej (RPD2SIIHCDP), w którego skład wchodzi:
 - Zespół Helpdesk oraz Systemów Lokalnych i Bazy Wiedzy (RPD2SIIHL),
 - Zespół do Spraw Programowania (RPD2SIIPR),
 - Zespół Systemów Centralnych (RPD2SIIC),
 - Sekcja do Spraw Bezpieczeństwa Informatycznego (RPD2SIID),
 - Sekcja do Spraw Planowania i Logistyki Informatycznej (RPD2SIIP),
 - Pierwszy Zespół Wsparcia Informatycznego (RPD2SIIW-01),
 - Drugi Zespół Wsparcia Informatycznego (RPD2SIIW-02),
 - Trzeci Zespół Wsparcia Informatycznego (RPD2SIIW-03),
 - Czwarty Zespół Wsparcia Informatycznego (RPD2SIIW-04),
 - Piąty Zespół Wsparcia Informatycznego (RPD2SIIW-05),
 - Zespół Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RPD2SIISW),
 - Oddział Zarządzania Regionem Opolskim (RPD3), w którego skład wchodzi:
 - Zespół Bezpieczeństwa Informatycznego, Systemów Centralnych, Lokalnych i Bazy Wiedzy, Planowania i Logistyki Informatycznej oraz Helpdesk (RPD3OIIIL),
 - Pierwszy Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPD3OIIW-1),
 - Drugi Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPD3OIIW-2),
 - Oddział Zarządzania Regionem Małopolskim (RPD4), w którego skład wchodzi:
 - Wydział Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Bezpieczeństwa Informatycznego, Planowania i Logistyki Informatycznej (RPD4IIW), w skład którego wchodzi:
 - Pierwszy Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Bezpieczeństwa Informatycznego,

- Planowania i Logistyki Informatycznej (RPD4IIW-1),
 - Drugi Zespół Wsparcia Informatycznego, Infrastruktury Sietciowej i Serwerowej oraz Bezpieczeństwa Informatycznego, Planowania i Logistyki Informatycznej (RPD4IIW-2),
 - Trzeci Zespół Wsparcia Informatycznego, Infrastruktury Sietciowej i Serwerowej oraz Bezpieczeństwa Informatycznego, Planowania i Logistyki Informatycznej (RPD4IIW-3),
 - Czwarty Zespół Wsparcia Informatycznego, Infrastruktury Sietciowej i Serwerowej oraz Bezpieczeństwa Informatycznego, Planowania i Logistyki Informatycznej (RPD4IIW-4),
 - Piąty Zespół Wsparcia Informatycznego, Infrastruktury Sietciowej i Serwerowej oraz Bezpieczeństwa Informatycznego, Planowania i Logistyki Informatycznej (RPD4IIW-5),
- Zespół Systemów Centralnych (RPD4IIC),
- Zespół Helpdesk, Systemów Lokalnych i Bazy Wiedzy (RPD4IIH),
- Oddział Zarządzania Regionem Świętokrzyskim (RPD5), w którego skład wchodzi:
 - Pierwszy Zespół Wsparcia Informatycznego (RPD5TIIW-1),
 - Drugi Zespół Wsparcia Informatycznego (RPD5TIIW-2),
 - Zespół Infrastruktury Sietciowej i Serwerowej, Bezpieczeństwa Informatycznego oraz Planowania i Logistyki Informatycznej (RPD5TIIS),
 - Zespół Systemów Centralnych, Lokalnych i Bazy Wiedzy oraz Helpdesk (RPD5TIIC),
- Oddział Zarządzania Krajową Informacją Skarbową (RPD6), w którego skład wchodzi:
 - Pierwszy Zespół Informatyki (RPD6KLI1),
 - Drugi Zespół Informatyki (RPD6KLI2),
- Oddział Zarządzania Krajową Szkołą Skarbowości (RPD7), w którego skład wchodzi:
 - Zespół Zarządzania Wsparciem Informatycznym, Bezpieczeństwem Informatycznym, Infrastrukturą Sietciową i Serwerową (RPD7ZWI)
- c) Departament Zarządzania Regionem Północnym (RPN), w którego skład wchodzi:
 - Biuro Wsparcia (RPN1BW)
 - Oddział Zarządzania Regionem Kujawsko – Pomorskim (RPN2), w którego skład wchodzi:
 - Zespół Bezpieczeństwa Informatycznego oraz Planowania i Logistyki Informatycznej (RPN2IID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RPN2IIL),
 - Zespół Helpdesk (RPN2IIH),
 - Zespół Infrastruktury Sietciowej i Serwerowej oraz Planowania i Logistyki Informatycznej (RPN2IIS),
 - Zespół Wsparcia Informatycznego oraz Infrastruktury Sietciowej i Serwerowej oraz Planowania i Logistyki Informatycznej (RPN2IIP),
 - Pierwszy Zespół Wsparcia Informatycznego oraz Infrastruktury Sietciowej i Serwerowej oraz Systemów Centralnych (RPN2IIW1),
 - Drugi Zespół Wsparcia Informatycznego oraz Infrastruktury Sietciowej i Serwerowej oraz Systemów Centralnych (RPN2IIW2),
 - Trzeci Zespół Wsparcia Informatycznego oraz Infrastruktury Sietciowej i Serwerowej (RPN2IIW3),

- Czwarty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RPN2IIW4),
- Piąty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RPN2IIW5),
- Oddział Zarządzania Regionem Pomorskim (RPN3), w którego skład wchodzi:
 - Sekcja Bezpieczeństwa Informatycznego (RPN3IID),
 - Zespół Infrastruktury Sieciowej i Serwerowej (RPN3IIS),
 - Zespół Systemów Centralnych, Lokalnych i Bazy Wiedzy (RPN3IIC),
 - Zespół Helpdesk (RPN3IIH),
 - Pierwszy Zespół Wsparcia Informatycznego (RPN3IIW1),
 - Drugi Zespół Wsparcia Informatycznego (RPN3IIW2),
 - Zespół Planowania i Logistyki Informatycznej (RPN3IIP),
- Oddział Zarządzania Regionem Warmińsko – Mazurskim (RPN4), w którego skład wchodzi:
 - Sekcja Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPN4IID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy, Helpdesk, Systemów Centralnych (RPN4IIL),
 - Pierwszy Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPN4IIW1),
 - Drugi Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPN4IIW2),
 - Trzeci Zespół Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPN4IIW3),
 - Czwarty Zespół Wsparcia Informatycznego, Planowania i Logistyki Informatycznej (RPN4IIW4),
- Oddział Zarządzania Regionem Zachodniopomorskim (RPN5), w którego skład wchodzi:
 - Zespół Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Planowania i Logistyki Informatycznej (RPN5IID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RPN5IIL),
 - Sekcja Helpdesk (RPN5IIH),
 - Pierwszy Zespół Wsparcia Informatycznego (RPN5IIW1),
 - Drugi Zespół Wsparcia Informatycznego (RPN5IIW2),
 - Trzeci Zespół Wsparcia Informatycznego (RPN5IIW3),
 - Zespół Systemów Centralnych (RPN5IIC),
 - Zespół Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RPN5IIS),
- d) Departament Zarządzania Regionem Wschodnim (RWS), w którego skład wchodzi:
 - Biuro Wsparcia (RWS1BW),
 - Oddział Zarządzania Regionem Podlaskim (RWS2), w którego skład wchodzi:
 - Zespół Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej (RWS2BIID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RWS2BIIL),
 - Zespół Planowania i Logistyki Informatycznej oraz Helpdesk (RWS2BIIP),
 - Pierwszy Zespół Wsparcia Informatycznego (RWS2BIIW1),
 - Drugi Zespół Wsparcia Informatycznego (RWS2BIIW2),

- Trzeci Zespół Wsparcia Informatycznego (RWS2BIIW3),
 - Oddział Zarządzania Regionem Mazowieckim (RWS3), w którego skład wchodzi:
 - Zespół Bezpieczeństwa Informatycznego (RWS3MIID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy (RWS3MIIL),
 - Zespół Helpdesk (RWS3MIIH),
 - Wydział Wsparcia Informatycznego (RWS3MIIW), w którego skład wchodzi:
 - Pierwszy Zespół Wsparcia Informatycznego (RWS3MIIW1),
 - Drugi Zespół Wsparcia Informatycznego (RWS3MIIW2),
 - Trzeci Zespół Wsparcia Informatycznego (RWS3MIIW3),
 - Czwarty Zespół Wsparcia Informatycznego (RWS3MIIW4),
 - Piąty Zespół Wsparcia Informatycznego (RWS3MIIW5),
 - Szósty Zespół Wsparcia Informatycznego (RWS3MIIW6),
 - Siódmy Zespół Wsparcia Informatycznego (RWS3MIIW7),
 - Zespół Systemów Centralnych (RWS3MIIC),
 - Sekcja do Spraw Infrastruktury Sieciowej i Serwerowej (RWS3MIIS),
 - Sekcja do Spraw Planowania i Logistyki Informatycznej (RWS3MIIP),
 - Oddział Zarządzania Regionem Lubelskim (RWS4), w którego skład wchodzi:
 - Sekcja Bezpieczeństwa Informatycznego (RWS4LIID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy oraz Helpdesku (RWS4LIIH),
 - Zespół Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych – Centrum Kompetencyjne (RWS4LIIL),
 - Pierwszy Zespół Wsparcia Informatycznego (RWS4LIIW-1),
 - Drugi Zespół Wsparcia Informatycznego (RWS4LIIW-2),
 - Trzeci Zespół Wsparcia Informatycznego (RWS4LIIW-3),
 - Czwarty Zespół Wsparcia Informatycznego (RWS4LIIW-4),
 - Pierwszy Zespół Systemów Centralnych – Centrum Kompetencyjne (RWS4LIIC-1),
 - Zespół Infrastruktury Sieciowej i Serwerowej, Wsparcia Informatycznego oraz Planowania i Logistyki Informatycznej (RWS4LIIS),
 - Oddział Zarządzania Regionem Podkarpackim (RWS5), w którego skład wchodzi:
 - Zespół Bezpieczeństwa Informatycznego (RWS5RIID),
 - Zespół Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RWS5RIIL),
 - Zespół Helpdesk (RWS5RIIH),
 - Pierwszy Zespół Wsparcia Informatycznego (RWS5RIIW1),
 - Drugi Zespół Wsparcia Informatycznego (RWS5RIIW2),
 - Trzeci Zespół Wsparcia Informatycznego (RWS5RIIW3),
 - Zespół Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RWS5RIIS),
 - Zespół Planowania i Logistyki Informatycznej (RWS5RIIP),
 - e) Departament Bezpieczeństwa IT (DBIT), w którego skład wchodzi:
 - Wydział Administrowania Systemami do Przetwarzania Informacji Niejawnych oraz Zabezpieczeń Aplikacji (DBIT1);
 - f) Wydział Systemów Kadrowo-Płacowych Resortu Finansów (SKP);
- 5) Wydział Prawny (PR);

- 6) Audytor Wewnętrzny (AW);
 - 7) Pełnomocnik do Spraw Zmiany (PZ).
2. Schemat struktury organizacyjnej Centrum stanowi załącznik do regulaminu.

Rozdział 3 Nadzór nad Centrum

§ 5.

1. Decyzje:
 - 1) dotyczące okresowego planowania wykonywania zadań przez Centrum;
 - 2) w sprawie przyjęcia planu finansowego Centrum
– wymagają uprzedniego zatwierdzenia w ramach sprawowanego nadzoru przez ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych lub osobę, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum.
2. Dyrektor Centrum:
 - 1) składa raz na pół roku sprawozdanie z działalności Centrum ministrowi właściwemu do spraw budżetu, finansów publicznych i instytucji finansowych lub osobie, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum;
 - 2) składa wszelkie wyjaśnienia oraz informacje, na wniosek ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych lub osoby, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum;
 - 3) jest zobowiązany uczestniczyć w spotkaniach kierownictwa komórki organizacyjnej Ministerstwa Finansów prowadzącej sprawę nadzoru nad Centrum;
 - 4) jest zobowiązany realizować zadania uzgodnione lub zlecone przez ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych lub osobę, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum.
3. Dyrektor Centrum, w porozumieniu z ministrem właściwym do spraw budżetu, finansów publicznych i instytucji finansowych lub osobą, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum, powołuje wspólne organy kolegialne (komisje, rady, zespoły, itp.) Centrum oraz Ministerstwa Finansów.

Rozdział 4 **Zakres kompetencji Dyrektora Centrum i Dyrektorów Pionów pełniących rolę jego zastępców**

§ 6.

1. Dyrektorowi Centrum (D) bezpośrednio podlegają:
 - 1) Dyrektor Pionu do Spraw Administracyjnych, pełniący rolę zastępcy dyrektora Centrum (ZD1);
 - 2) Dyrektor Pionu do Spraw Infrastruktury, pełniący rolę zastępcy Dyrektora Centrum (ZD2);
 - 3) Dyrektor Pionu do Spraw Rozwoju i Utrzymania Aplikacji, pełniący rolę zastępcy Dyrektora Centrum (ZD3);
 - 4) Dyrektor Pionu do Spraw Informatyki Resortu Finansów, pełniący rolę zastępcy Dyrektora Centrum (ZD4);
 - 5) Kierownik Wydziału Prawnego (KO);
 - 6) Audytor Wewnętrzny (AW);

- 7) Pełnomocnik do Spraw Zmiany (PZ);
 - 8) Pełnomocnik ds. ochrony informacji niejawnych (PO);
 - 9) Inspektor ochrony danych (IO).
2. Do zakresu zadań **Dyrektora Centrum (D)** należy w szczególności:
 - 1) sprawowanie nadzoru nad prawidłowym funkcjonowaniem Centrum;
 - 2) realizowanie zadań kierownika państwowej jednostki budżetowej, wynikających z przepisów ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, z późn. zm.), zwanej dalej „ustawą o finansach publicznych” oraz ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2019 r. poz. 351, z późn. zm.), zwanej dalej „ustawą o rachunkowości”;
 - 3) planowanie wykonywania przez Centrum zadań, zgodnych z obowiązującym prawem oraz uzgodnieniami i zleceniami ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych lub osoby, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum;
 - 4) podpisywanie zakresów czynności bezpośrednio podległym pracownikom;
 - 5) stanowienie aktów wewnętrznych w sprawach organizacji i realizacji zadań Centrum;
 - 6) prowadzenie polityki kadrowo-płacowej;
 - 7) dysponowanie Zakładowym Funduszem Świadczeń Socjalnych;
 - 8) podejmowanie decyzji w zakresie wydatkowania środków finansowych, w tym, zatwierdzanie dokumentów związanych z udzielaniem zamówień publicznych;
 - 9) wypełnianie obowiązków dysponenta środków budżetu państwa trzeciego stopnia podległego dysponentowi głównemu;
 - 10) zapewnienie właściwych warunków bezpieczeństwa i higieny pracy;
 - 11) reprezentowanie Centrum na zewnątrz w sprawach dotyczących zakresu jego działania;
 - 12) podejmowanie działań na rzecz rozwoju Centrum;
 - 13) rozstrzyganie sporów kompetencyjnych pomiędzy komórkami organizacyjnymi;
 - 14) delegowanie uprawnień w zakresie załatwiania spraw i podpisywania dokumentów w jego imieniu poprzez udzielanie pełnomocnictw i upoważnień pracownikom;
 - 15) wykonywanie innych zadań w zakresie wynikającym z zajmowanego stanowiska pracy zleconych przez ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych lub osobę, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum.
 3. Dyrektor Centrum podpisuje:
 - 1) pisma, opracowania i inne dokumenty skierowane do ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych lub osoby, której minister właściwy do spraw budżetu, finansów publicznych i instytucji finansowych powierzył nadzór nad działalnością Centrum;
 - 2) pisma i dokumenty kierowane na zewnątrz Centrum.
 4. Dyrektor Centrum zatwierdza:
 - 1) plan finansowy Centrum;
 - 2) dokumenty zawierające plany wykonania zadań Centrum;
 - 3) sprawozdania finansowe i budżetowe Centrum;
 - 4) dowody finansowo-księgowe;
 - 5) dokumenty płacowe.
 5. Dyrektor Centrum może zlecić pracownikom wykonywanie innych zadań niż określone w zakresie czynności na zajmowanym stanowisku pracy.
 6. Dyrektor Centrum może powoływać organy kolegialne (komisje, rady, zespoły itp.) o charakterze stałym lub doraźnym w celu realizacji określonych zadań ustalając skład, cel powołania, zakres zadań i tryb pracy organu kolegialnego.

7. Dyrektora Centrum podczas nieobecności zastępuje wyznaczony przez niego Dyrektor Pionu pełniący rolę zastępcy Dyrektora Centrum.
8. W przypadku wakatu na stanowisku Dyrektora Centrum, Centrum kieruje Dyrektor Pionu, pełniący rolę zastępcy Dyrektora Centrum wyznaczony przez ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych. W przypadku wakatu na stanowisku Dyrektora Centrum i Dyrektora Pionu, pełniącego rolę zastępcy Dyrektora Centrum, Centrum kieruje pracownik wyznaczony przez ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych.

§ 7.

1. Dyrektorowi Pionu do Spraw Administracyjnych, pełniącemu rolę zastępcy Dyrektora Centrum (ZD1) podlega:
 - 1) Departament Kadr (DK);
 - 2) Departament Finansów (DF);
 - 3) Departament Zakupów (DZ);
 - 4) Departament Logistyki (DL);
 - 5) Wieloosobowe stanowisko pracy do spraw bezpieczeństwa i higieny pracy (BHP).
2. Dyrektorowi Pionu do Spraw Infrastruktury, pełniącemu rolę zastępcy Dyrektora Centrum (ZD2) podlega:
 - 1) Departament Utrzymania Infrastruktury Technicznej (DUT);
 - 2) Departament Sieci, Usług i Monitorowania (DSM);
 - 3) Departament Infrastruktury Teleinformatycznej (DIT).
3. Dyrektorowi Pionu do Spraw Rozwoju i Utrzymania Aplikacji, pełniącemu rolę zastępcy Dyrektora Centrum (ZD3) podlega:
 - 1) Departament Rozwoju i Utrzymania Aplikacji Podatkowych (DAP);
 - 2) Departament Rozwoju i Utrzymania Aplikacji Analitycznych, Celnych i Budżetowych (DAB);
 - 3) Departament Wsparcia Informatycznego i Utrzymania Stacji Roboczych (DWU);
 - 4) Departament Rozwoju i Utrzymania Aplikacji e-Usługowych oraz Aplikacji Gospodarki Własnej (DEG).
4. Dyrektorowi Pionu do Spraw Informatyki Resortu Finansów, pełniącemu rolę zastępcy Dyrektora Centrum (ZD4) podlega:
 - 1) Departament Zarządzania Regionem Zachodnim (RZA);
 - 2) Departament Zarządzania Regionem Południowym (RPD);
 - 3) Departament Zarządzania Regionem Północnym (RPN);
 - 4) Departament Zarządzania Regionem Wschodnim (RWS);
 - 5) Departament Bezpieczeństwa IT (DBIT);
 - 6) Wydział Systemów Kadrowo-Płacowych Resortu Finansów (SKP).
5. Dyrektor Pionu, pełniący rolę zastępcy Dyrektora Centrum kieruje pracą podległych komórek organizacyjnych oraz odpowiada bezpośrednio przed Dyrektorem Centrum za prawidłowe, terminowe i zgodne z przepisami prawa wykonywanie zadań przez podległe komórki organizacyjne.
6. Do zakresu zadań Dyrektora Pionu, pełniącego rolę zastępcy Dyrektora Centrum należy w szczególności:
 - 1) zapewnienie prawidłowej, efektywnej i terminowej realizacji zadań przez podległe komórki organizacyjne, zleconych przez Dyrektora Centrum;
 - 2) zapewnienie zgodności działania podległych komórek organizacyjnych z obowiązującymi przepisami prawa, regulacjami wewnętrznymi i kierunkami określonymi przez Dyrektora Centrum;
 - 3) zapewnienie organizacji pracy podległych komórek organizacyjnych;
 - 4) dbałość o rozwój zawodowy pracowników w podległych komórkach organizacyjnych;

- 5) bieżące informowanie Dyrektora Centrum o przebiegu prac i stanie realizacji wykonywanych zadań, w tym o stwierdzonych nieprawidłowościach i zagrożeniach;
 - 6) dbanie o skuteczny przepływ informacji wewnątrz, jak i na zewnątrz podległych komórek organizacyjnych;
 - 7) dokonywanie oceny proponowanego rozstrzygnięcia w zakresie merytorycznym i formalnoprawnym przed zatwierdzeniem lub przekazaniem do zatwierdzenia Dyrektorowi Centrum;
 - 8) przedstawianie Dyrektorowi Centrum wniosków w sprawie zatrudniania, zwalniania, awansowania, nagradzania, wyróżniania i karania bezpośrednio podległych pracowników;
 - 9) nadzór nad przestrzeganiem przez bezpośrednio podległych pracowników zasad bezpieczeństwa i higieny pracy, bezpieczeństwa przeciwpożarowego oraz określających porządek, organizację i dyscyplinę pracy;
 - 10) udzielanie upoważnień bezpośrednio podległym pracownikom w zakresie przyznaných kompetencji;
 - 11) udzielanie urlopów wypoczynkowych bezpośrednio podległym pracownikom;
 - 12) udzielanie zwolnień w godzinach pracy bezpośrednio podległym pracownikom;
 - 13) podpisywanie poleceń wyjazdu służbowego podległym pracownikom;
 - 14) podpisywanie zakresów czynności bezpośrednio podległym pracownikom;
 - 15) wykonywanie innych zadań w zakresie wynikającym z zajmowanego stanowiska pracy zleconych przez Dyrektora Centrum.
7. Dyrektor Pionu, pełniący rolę zastępcy Dyrektora Centrum podpisuje:
 - 1) pisma i dokumenty w zakresie właściwości podległych komórek organizacyjnych, niezastrzeżone do podpisu Dyrektora Centrum;
 - 2) pisma i dokumenty, do których został upoważniony przez Dyrektora Centrum.
 8. Dyrektora Pionu, pełniącego rolę zastępcy Dyrektora Centrum podczas nieobecności zastępuje inny Dyrektor Pionu, pełniący rolę zastępcy Dyrektora Centrum wyznaczony przez Dyrektora Centrum lub bezpośrednio podległy mu Dyrektor Departamentu.
 9. W przypadku wakatu na stanowisku Dyrektora Pionu, pełniącego rolę zastępcy Dyrektora Centrum, komórką organizacyjną kieruje inny Dyrektor Pionu, pełniący rolę zastępcy Dyrektora Centrum lub Dyrektor Departamentu w danym pionie wyznaczony przez Dyrektora Centrum.

Rozdział 5

Zakres zadań Dyrektora Departamentu, osób kierujących pracownikami oraz zatrudnionych na samodzielnych stanowiskach pracy w Centrum

§ 8.

1. Dyrektor Departamentu kieruje pracą podległych komórek organizacyjnych oraz odpowiada przed bezpośrednim przełożonym za prawidłowe, terminowe i zgodne z przepisami prawa wykonywanie zadań przez podległe komórki organizacyjne.
2. Do zakresu zadań **Dyrektora Departamentu** należy w szczególności:
 - 1) organizowanie pracy oraz kontrola realizacji zadań przez podległe komórki organizacyjne;
 - 2) zapewnienie dyscypliny pracy w podległych komórkach organizacyjnych;
 - 3) zapewnienie prawidłowego, efektywnego i terminowego wykonywania zadań przez podległe komórki organizacyjne;
 - 4) przekazywanie podległym komórkom organizacyjnym dyspozycji i wytycznych niezbędnych do wykonywania zadań;
 - 5) udział w procesie planowania budżetu rzeczowo-finansowego jednostki w zakresie właściwości podległych komórek organizacyjnych;

- 6) bieżące informowanie bezpośredniego przełożonego o przebiegu prac i stanie realizacji wykonywanych zadań, w tym o stwierdzonych nieprawidłowościach i zagrożeniach;
 - 7) dbanie o skuteczny przepływ informacji wewnątrz, jak i na zewnątrz podległych komórek organizacyjnych;
 - 8) dokonywanie oceny proponowanego rozstrzygnięcia w zakresie merytorycznym i formalnoprawnym przed zatwierdzeniem lub przekazaniem do zatwierdzenia do bezpośredniego przełożonego;
 - 9) przedstawianie bezpośrednio przełożonemu wniosków w sprawie zatrudniania, zwalniania, awansowania, nagradzania, wyróżniania i karania bezpośrednio podległych pracowników;
 - 10) nadzór nad przestrzeganiem przez bezpośrednio podległych pracowników zasad bezpieczeństwa i higieny pracy, bezpieczeństwa przeciwpożarowego oraz określających porządek, organizację i dyscyplinę pracy;
 - 11) udzielanie upoważnień bezpośrednio podległym pracownikom w zakresie przyznanych kompetencji;
 - 12) udzielanie urlopów wypoczynkowych bezpośrednio podległym pracownikom;
 - 13) udzielanie zwolnień w godzinach pracy bezpośrednio podległym pracownikom;
 - 14) podpisywanie poleceń wyjazdu służbowego podległym pracownikom;
 - 15) podpisywanie zakresów czynności bezpośrednio podległym pracownikom;
 - 16) wykonywanie innych zadań w zakresie wynikającym z zajmowanego stanowiska pracy zleconych przez bezpośredniego przełożonego.
3. Dyrektor Departamentu podpisuje:
 - 1) pisma i dokumenty w zakresie właściwości podległych komórek organizacyjnych, niezastrzeżone do podpisu bezpośredniego przełożonego lub Dyrektora Centrum;
 - 2) pisma i dokumenty, do których został upoważniony przez bezpośredniego przełożonego lub Dyrektora Centrum.
 4. Dyrektora Departamentu podczas nieobecności zastępuje wyznaczony przez niego kierownik komórki organizacyjnej.
 5. W przypadku wakatu na stanowisku Dyrektora Departamentu, komórką organizacyjną kieruje Dyrektor Pionu, pełniący rolę zastępcy Dyrektora Centrum lub kierownik komórki organizacyjnej w danym pionie wyznaczony przez Dyrektora Pionu, pełniącego rolę zastępcy Dyrektora Centrum.

§ 9.

1. Kierownik komórki organizacyjnej kieruje pracą podległej komórki organizacyjnej oraz odpowiada przed bezpośrednim przełożonym za prawidłowe, terminowe i zgodne z przepisami prawa wykonywanie zadań przez podległą komórkę organizacyjną.
2. Do zakresu zadań **kierownika komórki organizacyjnej** należy w szczególności:
 - 1) organizowanie pracy oraz kontrola realizacji zadań przez bezpośrednio podległych pracowników;
 - 2) kontrolowanie dyscypliny pracy wśród bezpośrednio podległych pracowników;
 - 3) ponoszenie odpowiedzialności za prawidłowe, efektywne i terminowe wykonanie zadań przez bezpośrednio podległych pracowników;
 - 4) przekazywanie bezpośrednio podległym pracownikom dyspozycji i wytycznych niezbędnych do wykonywania zadań;
 - 5) dbanie o skuteczny przepływ informacji wewnątrz, jak i na zewnątrz podległej komórki organizacyjnej;
 - 6) nadzór nad monitorowaniem realizacji umów, nad którymi podległa komórka organizacyjna sprawuje nadzór merytoryczny;
 - 7) ocena proponowanego rozstrzygnięcia w zakresie merytorycznym, przed przekazaniem do zatwierdzenia bezpośrednio przełożonemu;

- 8) bieżące informowanie bezpośredniego przełożonego o przebiegu prac i stanie realizacji wykonywanych zadań, w tym o stwierdzonych nieprawidłowościach i zagrożeniach;
 - 9) przedstawianie bezpośredniemu przełożonemu wniosków w sprawie zatrudniania, zwalniania, awansowania, nagradzania, wyróżniania i karania bezpośrednio podległych pracowników;
 - 10) nadzór nad przestrzeganiem przez bezpośrednio podległych pracowników zasad bezpieczeństwa i higieny pracy, bezpieczeństwa przeciwpożarowego oraz określających porządek, organizację i dyscyplinę pracy;
 - 11) udzielanie upoważnień bezpośrednio podległym pracownikom w zakresie przyznanych kompetencji;
 - 12) udzielanie urlopów wypoczynkowych bezpośrednio podległym pracownikom;
 - 13) udzielanie zwolnień w godzinach pracy bezpośrednio podległym pracownikom;
 - 14) podpisywanie poleceń wyjazdu służbowego podległym pracownikom;
 - 15) podpisywanie zakresów czynności bezpośrednio podległym pracownikom;
 - 16) parafowanie pism, dokumentów i materiałów sporządzonych w podległej komórce organizacyjnej;
 - 17) wykonywanie innych zadań w zakresie wynikającym z właściwości zajmowanego stanowiska pracy zleconych przez bezpośredniego przełożonego.
3. Kierownik komórki organizacyjnej podpisuje:
 - 1) pisma i dokumenty o charakterze porządkowym lub informacyjnym w zakresie właściwości podległej komórki organizacyjnej, niezastrzeżone do podpisu bezpośredniego przełożonego lub Dyrektora Centrum;
 - 2) pisma i dokumenty, do których został upoważniony przez bezpośredniego przełożonego lub Dyrektora Centrum.
 4. Kierownika komórki organizacyjnej podczas nieobecności zastępuje zastępca kierownika lub wyznaczony przez niego pracownik podległej komórki organizacyjnej.
 5. W przypadku wakatu na stanowisku kierownika komórki organizacyjnej, komórką organizacyjną kieruje zastępca kierownika lub pracownik wyznaczony przez bezpośredniego przełożonego.

§ 10.

1. Zastępca kierownika kieruje pracą komórki organizacyjnej podczas nieobecności kierownika komórki organizacyjnej i jest odpowiedzialny za prawidłowe i terminowe realizowanie przydzielonych zadań oraz zgodność działania komórki organizacyjnej z przepisami prawa i wytycznymi bezpośredniego przełożonego.
2. Do zakresu zadań **zastępcy kierownika** należy w szczególności:
 - 1) realizacja zadań zleconych przez kierownika komórki organizacyjnej;
 - 2) podejmowanie decyzji w sprawach realizowanych przez podległą komórkę organizacyjną w zakresie kompetencji określonych w zakresie czynności opracowanym przez bezpośredniego przełożonego;
 - 3) wykonywanie innych zadań w zakresie wynikającym z właściwości zajmowanego stanowiska pracy zleconych przez bezpośredniego przełożonego.
3. Szef ochrony kieruje pracą Wydziału Wewnętrznej Służby Ochrony i jest odpowiedzialny za prawidłowe i terminowe realizowanie przydzielonych zadań oraz zgodność działania Wewnętrznej Służby Ochrony z przepisami prawa i wytycznymi bezpośredniego przełożonego. Szef ochrony realizuje zadania określone w § 9 ust. 2. Szefa ochrony podczas nieobecności zastępuje wyznaczony przez niego pracownik Wydziału Wewnętrznej Służby Ochrony.

§ 11.

1. Do zakresu zadań **Głównego Księgowego** należy w szczególności:
 - 1) prowadzenie rachunkowości Centrum zgodnie z przepisami prawa;

- 2) wykonywanie dyspozycji środkami finansowymi;
 - 3) sporządzanie planu finansowego i sprawozdań dotyczących realizacji budżetu Centrum, jako dysponenta środków budżetu państwa trzeciego stopnia;
 - 4) koordynowanie wykorzystania przydzielonych Centrum środków finansowych;
 - 5) nadzorowanie funkcjonowania obiegu i kontroli dowodów finansowo-księgowych;
 - 6) dokonywanie wstępnej kontroli zgodności operacji gospodarczych i finansowych z planem finansowym;
 - 7) dokonywanie wstępnej kontroli kompletności i rzetelności dokumentów dotyczących operacji gospodarczych i finansowych;
 - 8) sprawowanie nadzoru nad prawidłowym i terminowym regulowaniem zobowiązań finansowych Centrum, w tym z tytułu dostaw i usług, zobowiązań podatkowych, ubezpieczeniowych i innych publicznoprawnych;
 - 9) parafowanie umów zawieranych przez Centrum, celem potwierdzenia zabezpieczenia środków finansowych na realizację planowanych wydatków w planie finansowym;
 - 10) realizowanie zadań głównego księgowego jednostki budżetowej, wynikających z przepisów ustawy o finansach publicznych oraz ustawy o rachunkowości.
2. Główny Księgowy podpisuje:
 - 1) pisma i dokumenty w zakresie właściwości stanowiska pracy, niezastrzeżone do podpisu bezpośredniego przełożonego lub Dyrektora Centrum;
 - 2) pisma i dokumenty, do podpisywania których został upoważniony przez bezpośredniego przełożonego lub Dyrektora Centrum.
 3. Głównego Księgowego podczas nieobecności zastępuje zastępca Głównego Księgowego lub wyznaczony przez niego pracownik podległej komórki organizacyjnej.

§ 12.

1. Do zakresu zadań **Audytora Wewnętrznego (AW)** należy w szczególności:
 - 1) sporządzanie rocznych i wieloletnich planów audytu wewnętrznego;
 - 2) sporządzanie sprawozdań z wykonania planu audytu wewnętrznego;
 - 3) udostępnianie na wniosek planu audytu oraz sprawozdań z wykonania planu audytu stanowiących informację publiczną, zgodnie z obowiązującymi przepisami prawa;
 - 4) prowadzenie bieżących akt audytu wewnętrznego w celu dokumentowania przebiegu i wyników audytu wewnętrznego;
 - 5) prowadzenie audytu wewnętrznego zgodnie z przepisami ustawy o finansach publicznych;
 - 6) parafowanie pism, dokumentów i materiałów sporządzonych na stanowisku pracy;
 - 7) wykonywanie innych zadań w zakresie właściwości zajmowanego stanowiska pracy zleconych przez Dyrektora Centrum.
2. Auditor Wewnętrzny podpisuje:
 - 1) pisma i dokumenty w zakresie właściwości stanowiska pracy, niezastrzeżone do podpisu Dyrektora Centrum;
 - 2) pisma i dokumenty, do podpisywania których został upoważniony przez Dyrektora Centrum.

§ 13.

1. Do zadań **Pełnomocnika do Spraw Zmiany (PZ)** należy w szczególności:
 - 1) doradzanie Dyrektorowi Centrum oraz Dyrektorom Pionów, pełniącym rolę zastępców Dyrektora Centrum w zakresie strategicznego planowania zmiany Centrum w zakresie dopasowania organizacji do zmieniających się potrzeb resortu finansów i trendów rynkowych;
 - 2) inicjowanie, koordynowanie i monitorowanie działań wspierających zmianę w zakresie uzgodnionym z Dyrektorem Centrum;

- 3) wspieranie interesariuszy zmiany wskazanych przez Dyrektora Centrum w uzgodnionym zakresie;
 - 4) raportowanie Dyrektorowi Centrum stanu nadzorowanych działań;
 - 5) samodzielna identyfikacja i współpraca z interesariuszami zmiany;
 - 6) reprezentowanie Dyrektora Centrum we wskazanych przez niego działaniach dotyczących zmiany;
 - 7) wykonywanie innych zadań w zakresie właściwości zajmowanego stanowiska pracy zleconych przez Dyrektora Centrum.
2. Pełnomocnik do spraw zmiany podpisuje:
- 1) pisma i dokumenty w zakresie właściwości stanowiska pracy, niezastrzeżone do podpisu Dyrektora Centrum;
 - 2) pisma i dokumenty, do podpisywania których został upoważniony przez Dyrektora Centrum.

§ 14.

1. Do zakresu zadań **Pełnomocnika ds. ochrony informacji niejawnych (PO)** należy w szczególności:
- 1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
 - 2) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;
 - 3) zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;
 - 4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa kontrola ewidencji materiałów i obiegu dokumentów niejawnych;
 - 5) prowadzenie szkoleń dla pracowników w zakresie ochrony informacji niejawnych;
 - 6) przeprowadzenie dochodzeń związanych z naruszeniem zasad bezpieczeństwa;
 - 7) kontrola udostępniania informacji niejawnych w toku prowadzenia postępowań o udzielenie zamówień publicznych, postępowań o dokonanie zakupów udzielonych poza ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 z późn. zm.) oraz wykonywania umów;
 - 8) prowadzenie zwykłych postępowań sprawdzających;
 - 9) przygotowywanie stosownej dokumentacji do postępowań sprawdzających dla Agencji Bezpieczeństwa Wewnętrznego wobec pracowników upoważnionych do dostępu do informacji niejawnych oznaczonych klauzulą „tajne” i „ściśle tajne”;
 - 10) prowadzenie aktualnego wykazu osób zatrudnionych w Centrum, które posiadają uprawnienia do dostępu do informacji niejawnych oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
 - 11) opracowywanie trybu i sposobu postępowania z informacjami niejawnymi oznaczonymi klauzulą „poufne” i „zastrzeżone” w Centrum;
 - 12) opracowywanie planu ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego;
 - 13) wykonywanie innych zadań w zakresie właściwości zajmowanego stanowiska pracy zleconych przez Dyrektora Centrum.
2. Pełnomocnik ds. ochrony informacji niejawnych podpisuje:
- 1) pisma i dokumenty w zakresie właściwości stanowiska pracy, niezastrzeżone do podpisu Dyrektora Centrum;
 - 2) pisma i dokumenty, do podpisywania których został upoważniony przez Dyrektora Centrum.

§ 15.

1. Do zadań **Inspektora ochrony danych (IO)** należy w szczególności:
 - 1) informowanie administratora danych oraz pracowników przetwarzających dane, o spoczywających na nich obowiązkach;
 - 2) monitorowanie przestrzegania przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk Centrum w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia pracowników uczestniczących w operacjach przetwarzania oraz powiązane z tym audyty;
 - 3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
 - 4) współpraca z organem nadzorczym w zakresie ochrony danych;
 - 5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w zakresie ochrony danych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
 - 6) pełnienie funkcji punktu kontaktowego dla wszystkich pracowników, których dane dotyczą, w sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów prawa w zakresie ochrony danych;
 - 7) prowadzenie rejestru czynności przetwarzania lub rejestru kategorii czynności przetwarzania;
 - 8) wykonywanie innych zadań w zakresie właściwości zajmowanego stanowiska pracy zleconych przez Dyrektora Centrum.
2. Inspektor ochrony danych podpisuje:
 - 1) pisma i dokumenty w zakresie właściwości stanowiska pracy, niezastrzeżone do podpisu Dyrektora Centrum;
 - 2) pisma i dokumenty, do podpisywania których został upoważniony przez Dyrektora Centrum.

Rozdział 6

Zadania wspólne komórek organizacyjnych

§ 16.

Do zadań wspólnych komórek organizacyjnych Centrum należy w szczególności:

- 1) zapewnienie realizacji celów i zadań Centrum w sposób zgodny z prawem, efektywny, oszczędny i terminowy;
- 2) współdziałanie z innymi komórkami organizacyjnymi Centrum;
- 3) ochrona informacji niejawnych i danych osobowych;
- 4) sporządzanie informacji, analiz i sprawozdań;
- 5) inicjowanie, opracowywanie, opiniowanie oraz uzgadnianie projektów aktów wewnętrznych Centrum;
- 6) realizowanie wniosków i zaleceń pokontrolnych instytucji uprawnionych do kontroli;
- 7) realizowanie spraw w zakresie prowadzenia postępowań sądowych;
- 8) udział w realizowaniu zakupów i zamówień publicznych, w tym szacowanie wartości przedmiotu zamówienia, przygotowywanie i weryfikowanie opisu przedmiotu zamówienia, w zakresie zadań realizowanych przez Centrum;
- 9) podejmowanie działań w celu podnoszenia jakości funkcjonowania Centrum;
- 10) archiwizowanie dokumentów zgodnie z przepisami prawa;
- 11) bieżące przekazywanie materiałów do wykorzystania na stronie internetowej Centrum;
- 12) dostarczanie i utrzymywanie usług informatycznych w Ministerstwie Finansów i w jednostkach organizacyjnych podległych ministrowi właściwemu do spraw budżetu,

- finansów publicznych i instytucji finansowych lub przez niego nadzorowanych, zwanych dalej „resortem finansów”, na poziomie uzgodnionym z Ministerstwem Finansów;
- 13) zarządzanie dostępnością, ciągłością i pojemnością usług informatycznych;
 - 14) zapewnienie bezpieczeństwa systemów informatycznych oraz bezpieczeństwa cyberprzestrzeni w Ministerstwie Finansów i resorcie finansów we współpracy z kierownikami jednostek organizacyjnych resortu finansów oraz komórką organizacyjną Ministerstwa Finansów właściwą w sprawach bezpieczeństwa i ochrony informacji;
 - 15) delegowanie pracowników Centrum do udziału w realizacji inicjatyw prowadzonych w resorcie finansów;
 - 16) udział w analizie, projektowaniu, budowie, testowaniu, wdrażaniu oraz wsparciu usług w zakresie infrastruktury informatycznej w Ministerstwie Finansów oraz w resorcie finansów;
 - 17) badanie rynku, pod kątem ewentualnego wykorzystania nowych rozwiązań w bieżących pracach Ministerstwa Finansów i Centrum;
 - 18) współpraca z Ministerstwem Finansów w zakresie wyznaczania osób do wykonywania funkcji administratora systemu informatycznego (ASI), w odniesieniu do systemów Ministerstwa Finansów;
 - 19) współpraca z komórkami organizacyjnymi Centrum, Ministerstwa Finansów oraz z resortem finansów, w celu zapewnienia prawidłowej i terminowej realizacji zadań;
 - 20) opracowywanie, wdrażanie i utrzymywanie standardów, procedur i innych formalnych uregulowań a także dokumentów, w zakresie realizowanych zadań;
 - 21) sprawdzanie pod względem merytorycznym dowodów finansowo-księgowych dotyczących zakupów realizowanych na potrzeby komórki organizacyjnej;
 - 22) monitorowanie realizacji umów, nad którymi komórka organizacyjna sprawuje nadzór merytoryczny;
 - 23) analiza wykorzystania środków finansowych przydzielonych danej komórce organizacyjnej na realizację bieżących zadań;
 - 24) udział w pracach z zakresu zarządzania kryzysowego, obronności i bezpieczeństwa państwa oraz zarządzania ciągłością działania;
 - 25) udział w uruchamianiu i realizacji inicjatyw informatycznych w zakresie opiniowania i ustalania architektury rozwiązań Centrum;
 - 26) współpraca z właścicielami biznesowymi systemów informatycznych;
 - 27) dostarczanie i utrzymanie rozwiązań informatycznych w zakresie robotyzacji i automatyzacji procesów w Ministerstwie Finansów i resorcie finansów, na poziomie uzgodnionym z Ministerstwem Finansów;
 - 28) współpraca z właściwą komórką organizacyjną Ministerstwa Finansów w zakresie zamówień publicznych;
 - 29) współpraca z właściwą komórką organizacyjną Ministerstwa Finansów w zakresie przygotowania budżetu Centrum, jako dysponenta środków budżetu państwa trzeciego stopnia;
 - 30) współpraca z właściwą komórką organizacyjną Ministerstwa Finansów w zakresie:
 - a) opiniowania projektów aktów prawnych i innych dokumentów w zakresie informatyzacji,
 - b) udzielania odpowiedzi na zapytania mediów w zakresie informatyzacji,
 - c) zarządzania projektami i inicjatywami informatycznymi, w tym weryfikacja zasadności ich realizacji pod kątem biznesowym, architektonicznym, finansowym oraz spójności z innymi inicjatywami realizowanymi w obszarze budżet, finanse publiczne i instytucje finansowe, w Ministerstwie Finansów i w resorcie finansów,
 - d) kontroli zewnętrznych i wewnętrznych,
 - e) udzielania informacji publicznej,

- f) odpowiedzi na interpelacje poselskie, zapytania i wystąpienia poselskie, oświadczenia i wystąpienia senatorskie, dezyderaty, opinie i wystąpienia komisji parlamentarnych oraz wystąpienia posłów Parlamentu Europejskiego, petycje, skargi i wnioski oraz wystąpienia obywateli, organizacji i instytucji.

Rozdział 7

Zakres zadań komórek organizacyjnych

§ 17.

Pion do Spraw Administracyjnych Departament Kadr (DK)

1. Do zakresu zadań **Wydziału Kadr (DK1)** należy w szczególności:
 - 1) organizowanie i przeprowadzanie procesu naboru;
 - 2) prowadzenie spraw kadrowych pracowników związanych z nawiązywaniem i rozwiązywaniem stosunku pracy oraz przebiegiem zatrudnienia, w tym:
 - a) prowadzenie akt osobowych oraz dokumentacji pracowniczej pracowników,
 - b) przygotowywanie dokumentów dotyczących całokształtu spraw związanych z nawiązaniem, zmianą oraz rozwiązaniem stosunku pracy,
 - c) sporządzanie dokumentacji związanej ze zgłoszeniem do ubezpieczeń społecznych i ubezpieczenia zdrowotnego pracowników,
 - d) wydawanie zaświadczeń potwierdzających zatrudnienie,
 - e) prowadzenie ewidencji czasu pracy;
 - 3) realizacja zadań związanych z podnoszeniem kwalifikacji zawodowych przez pracowników;
 - 4) nadzór nad przestrzeganiem prawa pracy;
 - 5) współpraca z organizacjami związkowymi w zakresie wynikającym z przepisów prawa pracy;
 - 6) monitorowanie stanu zatrudnienia;
 - 7) sporządzanie sprawozdań w zakresie zatrudnienia;
 - 8) prowadzenie spraw socjalnych pracowników w zakresie Zakładowego Funduszu Świadczeń Socjalnych;
 - 9) prowadzenie czynności związanych z nawiązywaniem i realizacją umów cywilnoprawnych;
 - 10) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Płac (DK2)** należy w szczególności:
 - 1) naliczanie wynagrodzeń i innych świadczeń związanych z pracą dla pracowników oraz sporządzanie list płac;
 - 2) naliczanie i sporządzanie list wypłat dla osób zatrudnionych na podstawie umowy cywilnoprawnej;
 - 3) sporządzanie dokumentacji podatkowej i ubezpieczeniowej;
 - 4) sporządzenie rocznych deklaracji podatkowych dla pracowników;
 - 5) realizacja obowiązków rozliczeniowych i informacyjnych względem właściwych organów i instytucji;
 - 6) nadzorowanie wykorzystania funduszu wynagrodzeń;
 - 7) sporządzanie sprawozdań w zakresie wynagrodzenia;
 - 8) wystawianie zaświadczeń o wynagrodzeniu;
 - 9) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 18.

Departament Finansów (DF)

1. Do zakresu zadań **Wydziału Zarządzania Finansami (DF1)** należy w szczególności:
 - 1) sporządzanie planu finansowego Centrum, proponowanie i realizacja bieżących zmian w planie finansowym;
 - 2) zarządzanie środkami finansowymi będącymi w dyspozycji Centrum, z wyłączeniem budżetu wynagrodzeń, pochodnych, Zakładowego Funduszu Świadczeń Socjalnych;
 - 3) zarządzanie środkami na zamówienia na usługi i dostawy informatyczne (lista podstawowa i rezerwowa zadań informatycznych);
 - 4) prowadzenie spraw finansowych związanych z planowaniem i realizacją środków finansowych będących w dyspozycji Centrum;
 - 5) analiza wykorzystania środków finansowych przydzielonych z budżetu państwa na realizację bieżących zadań Centrum;
 - 6) przygotowywanie wniosków o zewnętrzne zmiany w planie;
 - 7) wnioskowanie oraz obsługa zapewnień finansowania;
 - 8) koordynowanie tworzenia oraz obsługa planu rzeczowo-finansowego Centrum;
 - 9) sporządzanie zestawień i raportów w zakresie wykorzystania środków finansowych;
 - 10) opracowanie procedury przygotowania planu finansowego i procedury inicjowania i dokonywania zmian w planie;
 - 11) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Monitorowania i Rozliczania Umów (DF2)** należy w szczególności:
 - 1) ewidencjonowanie wniosków zakupowych oraz umów cywilnoprawnych zawieranych przez Centrum, dowodów finansowo-księgowych oraz innych dokumentów księgowych w programie finansowo-księgowym;
 - 2) weryfikowanie projektów umów na etapie postępowania o udzielenie zamówienia publicznego;
 - 3) kontrola procesu angażowania środków oraz realizacji zmian w tym obszarze;
 - 4) koordynowanie rozliczania umów zawieranych przez Centrum, w tym:
 - a) nadzór nad obiegiem dowodów finansowo-księgowych,
 - b) opisywanie otrzymanych od dostawców dowodów finansowo-księgowych - weryfikacja dokumentów odbioru dostaw i usług pod kątem kompletności i terminowości wynikających z zawartych umów, naliczanie kar umownych;
 - 5) prowadzenie ewidencji i monitorowanie realizacji umów z wykonawcami pod kątem finansowo-księgowym;
 - 6) prowadzenie spraw związanych z obsługą finansową projektów współfinansowanych ze środków Unii Europejskiej;
 - 7) rozliczanie Programów Inwestycyjnych po zakończonej inwestycji budowlanej;
 - 8) sprawdzanie pod względem formalnym dowodów finansowo-księgowych oraz prawidłowości opisywania w nich zdarzeń gospodarczych;
 - 9) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Księgowości i Płatności (DF3)** należy w szczególności:
 - 1) opracowywanie zasad (polityki) rachunkowości, instrukcji obiegu i kontroli dowodów finansowo-księgowych;
 - 2) prowadzenie ksiąg rachunkowych Centrum;
 - 3) nadzór nad obiegiem dowodów finansowo-księgowych;
 - 4) sprawdzanie pod względem rachunkowym dowodów finansowo-księgowych oraz prawidłowości opisywania w nich zdarzeń gospodarczych;
 - 5) prowadzenie rozliczeń podatku od towarów i usług;
 - 6) sporządzanie sprawozdań budżetowych i finansowych Centrum z zachowaniem wyznaczonych zasad i terminów;
 - 7) sporządzanie planu dochodów budżetowych;
 - 8) refakturowanie usług;

- 9) prowadzenie syntetycznej ewidencji wartościowej środków trwałych, pozostałych środków trwałych, wartości niematerialnych i prawnych, wyposażenia;
- 10) prowadzenie ewidencji wartościowej gospodarki magazynowej;
- 11) rozliczanie różnic inwentaryzacyjnych;
- 12) rozliczanie podróży służbowych i zaliczek pracowników;
- 13) planowanie i obsługa zapotrzebowania na środki w systemie Trezor;
- 14) sporządzanie i wysyłanie poleceń przelewów z tytułu dostaw i usług, wynagrodzeń, innych świadczeń związanych z zatrudnieniem, umów cywilnoprawnych, Zakładowego Funduszu Świadczeń Socjalnych, zobowiązań ubezpieczeniowych, podatkowych i innych publicznoprawnych;
- 15) dekretowanie i księgowanie dowodów finansowo-księgowych zgodnie z zakładowym planem kont obowiązującym w Centrum;
- 16) obsługa gwarancji i zabezpieczeń należytego wykonania umów;
- 17) sporządzanie potwierdzeń sald;
- 18) nadzór nad obiegiem dowodów finansowo-księgowych do akceptacji Głównego Księgowego oraz zatwierdzenia do wypłaty przez Dyrektora Centrum;
- 19) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 19

Departament Zakupów (DZ)

1. Do zakresu zadań **Wydziału Zamówień Publicznych (DZ1)** należy w szczególności:
 - 1) opracowywanie regulaminów dotyczących przygotowania i przeprowadzenia postępowań o udzielenie zamówień publicznych;
 - 2) przygotowywanie i przeprowadzenie postępowań o udzielenie zamówień publicznych realizowanych przez Centrum;
 - 3) sporządzanie i aktualizacja na wniosek komórek organizacyjnych planu zamówień publicznych dla Centrum;
 - 4) udział w pracach komisji przetargowych w postępowaniach o udzielenie zamówień publicznych;
 - 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Obsługi Procesów (DZ2)** należy w szczególności:
 - 1) współpraca z pracownikami merytorycznymi komórek organizacyjnych w zakresie przygotowywania wniosków w sprawie realizacji zamówień;
 - 2) opracowywanie projektów umów i aneksów;
 - 3) monitorowanie postępu prowadzonych spraw w komórkach organizacyjnych Centrum zaangażowanych w proces przygotowania i prowadzenia postępowania o dokonanie zamówienia;
 - 4) prowadzenie działań mających na celu optymalizację działań zakupowych Centrum;
 - 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 20

Departament Logistyki (DL)

1. Do zakresu zadań **Wydziału Zarządzania Mieniem i Transportu (DL1)** należy w szczególności:
 - 1) gospodarowanie mieniem Centrum;
 - 2) sporządzanie sprawozdania o stanie i ruchu środków trwałych;
 - 3) weryfikowanie opisów przedmiotu zamówienia pod kątem wprowadzenia dostaw na ewidencję mienia;
 - 4) prowadzenie spraw związanych z gospodarką i eksploatacją służbowych samochodów, w tym:

- a) zapewnienie obsługi transportowej,
 - b) prowadzenie dokumentacji technicznej i eksploatacyjnej samochodów służbowych, w tym kart drogowych,
 - c) planowanie pozyskiwania samochodów służbowych,
 - d) nadzorowanie i planowanie serwisów, badań technicznych, bieżących napraw, wymiany kół,
 - e) zapewnienie dostaw paliwa, części zamiennych, innych materiałów eksploatacyjnych do samochodów służbowych oraz usługi mycia,
 - f) zapewnienie ubezpieczenia samochodów służbowych oraz prowadzenie spraw w zakresie szkód i postępowań odszkodowawczych,
 - g) rejestracja samochodów służbowych;
- 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Zarządzania Nieruchomościami (DL2)** należy w szczególności:
- 1) zapewnienie niezbędnych dostaw i usług związanych z eksploatacją nieruchomości, w tym nadzór nad realizacją umów z dostawcami zewnętrznymi;
 - 2) zarządzanie służbowymi telefonami stacjonarnymi, w tym weryfikowanie zgłoszeń dotyczących ich przydziału, zakresu połączeń oraz weryfikacja billingów w zakresie korzystania ze służbowych telefonów stacjonarnych zgodnie z przepisami wewnętrznymi;
 - 3) zarządzanie służbowymi kartami SIM do usług głosowych i do usług transmisji danych, w tym wyposażanie pracowników w służbowe telefony komórkowe, weryfikowanie zgłoszeń dotyczących przydziału kart SIM i telefonów komórkowych oraz weryfikacja billingów w zakresie korzystania ze służbowych telefonów komórkowych zgodnie z przepisami wewnętrznymi;
 - 4) nadzór nad aktualnością danych w zakresie numerów służbowych stacjonarnych i komórkowych we właściwych zbiorach;
 - 5) sporządzanie i składanie do właściwego organu deklaracji na podatek dochodowy od nieruchomości;
 - 6) zapewnienie ubezpieczenia majątkowego;
 - 7) prowadzenie spraw związanych ze sprawowaniem trwałego zarządu nad nieruchomością;
 - 8) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Gospodarczego (DL3)** należy w szczególności:
- 1) prowadzenie spraw gospodarczo-zaopatrzeniowych;
 - 2) prowadzenie gospodarki magazynowej;
 - 3) przygotowanie i przeprowadzenie inwentaryzacji mienia i magazynu;
 - 4) nadzór nad realizacją porozumień zawartych pomiędzy Dyrektorem Centrum a Dyrektorem Generalnym Ministerstwa Finansów, Dyrektorem Krajowej Informacji Skarbowej, Dyrektorem Krajowej Szkoły Skarbowości, dyrektorami izb administracji skarbowej;
 - 5) wystawianie poświadczenia należytego wykonania umowy na wniosek dostawców zewnętrznych;
 - 6) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
4. Do zakresu zadań **Wydziału Organizacyjnego (DL4)** należy w szczególności:
- 1) prowadzenie składnicy akt/archiwum zakładowego;
 - 2) sporządzanie sprawozdania z działalności Centrum;
 - 3) sporządzanie sprawozdania z przyjmowania i załatwiania skarg i wniosków w Centrum;
 - 4) realizacja zadań w zakresie udostępniania informacji publicznej;
 - 5) koordynowanie prac związanych z realizacją procedur kontroli zarządczej zgodnie z obowiązującymi przepisami prawa;

- 6) koordynowanie spraw w zakresie aktów wewnętrznych Centrum, w tym prowadzenie rejestru wydanych przez Dyrektora Centrum aktów wewnętrznych;
- 7) koordynowanie spraw w zakresie upoważnień i pełnomocnictw oraz prowadzenie rejestru udzielonych upoważnień i pełnomocnictw;
- 8) organizacja pracy sekretariatu;
- 9) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 21.

1. Do zakresu zadań **Wieloosobowego stanowiska pracy do spraw bezpieczeństwa i higieny pracy (BHP)** należy w szczególności:
 - 1) przeprowadzanie kontroli warunków pracy oraz przestrzegania przepisów i zasad bezpieczeństwa i higieny pracy w Centrum na wszystkich stanowiskach pracy, ze szczególnym uwzględnieniem stanowisk pracy, na których są zatrudnieni pracownicy wykonujący pracę zmianową, w tym pracujący w nocy;
 - 2) bieżące informowanie bezpośredniego przełożonego i Dyrektora Centrum o stwierdzonych zagrożeniach zawodowych, wraz z wnioskami zmierzającymi do usuwania tych zagrożeń;
 - 3) sporządzanie i przedstawianie bezpośredniemu przełożonemu i Dyrektorowi Centrum okresowych analiz stanu bezpieczeństwa i higieny pracy wraz z propozycjami przedsięwzięć organizacyjnych i technicznych mających na celu zapobieganie zagrożeniom oraz poprawę warunków pracy;
 - 4) opracowywanie aktów wewnętrznych dotyczących bezpieczeństwa i higieny pracy oraz ustalanie zadań dla osób kierujących komórką organizacyjną w zakresie bezpieczeństwa i higieny pracy;
 - 5) opiniowanie szczegółowych instrukcji dotyczących bezpieczeństwa i higieny pracy na poszczególnych stanowiskach pracy;
 - 6) w zakresie wypadków przy pracy:
 - a) udział w ustalaniu okoliczności i przyczyn wypadków przy pracy,
 - b) opracowywanie protokołów wynikających z badania przyczyn i okoliczności wypadków przy pracy oraz zachorowań na choroby zawodowe,
 - c) prowadzenie rejestrów, kompletowanie i przechowywanie dokumentów dotyczących wypadków przy pracy, stwierdzonych chorób zawodowych,
 - d) przechowywanie wyników badań i pomiarów czynników szkodliwych dla zdrowia w środowisku pracy;
 - 7) doradztwo w zakresie stosowania przepisów oraz zasad bezpieczeństwa i higieny pracy;
 - 8) doradztwo w zakresie organizacji i metod pracy na stanowiskach pracy, na których występują czynniki szkodliwe dla zdrowia, dobór właściwych środków ochrony zbiorowej i indywidualnej;
 - 9) współpraca z komórkami organizacyjnymi w zakresie organizowania i zapewnienia odpowiedniego poziomu szkoleń w dziedzinie bezpieczeństwa i higieny pracy oraz zapewnienie właściwej adaptacji zawodowej nowozatrudnionych pracowników;
 - 10) udział w dokonywaniu oceny ryzyka zawodowego, które wiąże się z wykonywaną pracą;
 - 11) wnioskowanie do bezpośredniego przełożonego i Dyrektora Centrum o niezwłoczne wstrzymanie pracy w przypadku stwierdzenia bezpośredniego zagrożenia życia lub zdrowia pracowników lub innych osób;
 - 12) współdziałanie z lekarzem sprawującym profilaktyczną opiekę zdrowotną nad pracownikami oraz społecznym inspektorem pracy;
 - 13) nadzór nad przestrzeganiem terminowości szkoleń z zakresu bezpieczeństwa i higieny pracy;
 - 14) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

2. Jeżeli Centrum zatrudnia więcej niż jedną osobę do realizacji zadań w zakresie bezpieczeństwa i higieny pracy, jednej z tych osób powierza się koordynację pracy w komórce organizacyjnej.
3. Koordynator kieruje pracą w komórce organizacyjnej.
4. W stosunku do pozostałych pracowników komórki organizacyjnej koordynator realizuje zadania w zakresie określonym w § 9 ust. 2.

§ 22.

Pion do Spraw Infrastruktury Departament Utrzymania Infrastruktury Technicznej (DUT)

1. Do zakresu zadań **Wydziału Utrzymania Obiektów Przetwarzania Danych (DUT1)** należy w szczególności:
 - 1) administrowanie systemami technicznymi Centrum w tym kontroli dostępu, sygnalizacji włamania i napadu, ochrony przeciwpożarowej oraz telewizji dozorowej Centrum w Radomiu;
 - 2) zarządzanie systemem BMS (Building Management System), systemami zasilania gwarantowanego i ogólnego, systemem klimatyzacji precyzyjnej i wentylacji Centrum w Radomiu;
 - 3) zarządzanie systemami monitoringu infrastruktury technicznej oraz kontroli dostępu Centrum w Warszawie;
 - 4) planowanie rozwoju i wdrażanie zmian w podległej infrastrukturze;
 - 5) współpraca ze służbami technicznymi Ministerstwa Finansów w zakresie eksploatacji systemów zasilania gwarantowanego, klimatyzacji, sygnalizacji włamania i napadu oraz ochrony przeciwpożarowej Centrum w Warszawie;
 - 6) współpraca z usługodawcami zewnętrznymi w zakresie serwisu i konserwacji podległej infrastruktury technicznej i budowlanej;
 - 7) inicjowanie i koordynowanie zadań inwestycyjnych i remontowych dotyczących rozwoju i utrzymania instalacji elektroenergetycznych, instalacji klimatyzacyjnych, instalacji niskoprądowych, inwestycji i remontów obiektów kubaturowych zarządzanych przez Centrum;
 - 8) planowanie rozwoju i nadzorowanie wdrażania zmian w podległej infrastrukturze, w tym zasilania gwarantowanego i klimatyzacji precyzyjnej oraz instalacjach niskoprądowych dla planowanych i instalowanych systemów informatycznych;
 - 9) współpraca w planowaniu i optymalizacji zagospodarowania przestrzeni technicznej wymaganej do umieszczenia w Centrum systemów informatycznych;
 - 10) utrzymywanie zarządzanej infrastruktury technicznej i budowlanej na poziomie wyznaczonym przez politykę bezpieczeństwa;
 - 11) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Ochrony Informacji (DUT2)** należy w szczególności:
 - 1) nadzór nad wdrażaniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji w Centrum, w tym okresowe szacowanie ryzyka na podstawie przyjętych kryteriów;
 - 2) tworzenie, wdrażanie i utrzymanie polityki bezpieczeństwa danych osobowych w Centrum oraz monitorowanie jej realizacji;
 - 3) administrowanie, uzgadnianie, weryfikacja i wdrażanie dokumentacji bezpieczeństwa ochrony informacji;
 - 4) prowadzenie szkoleń z zakresu ochrony danych osobowych dla pracowników Centrum;
 - 5) przeprowadzanie audytów przez zespół audytorów wewnętrznych w celu oceny skuteczności Systemu Zarządzania Bezpieczeństwem Informacji;
 - 6) prowadzenie szkoleń z zakresu bezpieczeństwa ochrony informacji;
 - 7) prowadzenie kancelarii materiałów niejawnych;

- 8) koordynacja i nadzór prac z zakresu zarządzania kryzysowego, w szczególności:
 - a) koordynacja i realizacja zadań związanych z zarządzaniem kryzysowym,
 - b) obsługa organizacyjno-administracyjna zespołu zarządzania kryzysowego,
 - c) opracowywanie, analiza oraz opiniowanie dokumentacji dotyczącej zarządzania kryzysowego;
 - 9) koordynacja i nadzór prac z zakresu obronności, w szczególności:
 - a) planowanie operacyjne i programowanie obronne,
 - b) przygotowanie systemu kierowania Centrum,
 - c) realizacja zadań związanych z podwyższeniem gotowości obronnej państwa,
 - d) planowanie i organizacja szkoleń obronnych,
 - e) reklamowanie od obowiązku pełnienia czynnej służby wojskowej w razie ogłoszenia mobilizacji i w czasie wojny,
 - f) realizacja zadań wynikających z obowiązków państwa gospodarza (HNS);
 - 10) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Bezpieczeństwa Teleinformatycznego (DUT3)** należy w szczególności:
- 1) administrowanie systemami i narzędziami bezpieczeństwa środowiska teleinformatycznego Centrum;
 - 2) realizacja zadań związanych z wdrożeniem, utrzymaniem i monitorowaniem systemów i rozwiązań w obszarze cyberbezpieczeństwa będących w zakresie odpowiedzialności Centrum;
 - 3) zarządzanie bezpieczeństwem i monitoring urządzeń przenośnych i stacji roboczych Centrum;
 - 4) określanie standardów technicznych bezpieczeństwa środowiska teleinformatycznego ze szczególnym uwzględnieniem stacji roboczych, serwerów, usług i aplikacji oraz kanałów dostępowych do infrastruktury teleinformatycznej Centrum;
 - 5) monitorowanie procesu zarządzania kontami uprzywilejowanymi;
 - 6) monitorowanie dostępu dostawców zewnętrznych do systemów i usług środowiska teleinformatycznego Centrum;
 - 7) zapobieganie i przeciwdziałanie skutkom cyberincydentów w zakresie świadczonych usług;
 - 8) nadzorowanie i koordynowanie obsługi incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego Centrum;
 - 9) opracowanie bieżących wytycznych i rekomendacji dotyczących bezpieczeństwa środowiska teleinformatycznego wynikających z incydentów;
 - 10) współpraca z jednostkami zewnętrznymi w zakresie bezpieczeństwa teleinformatycznego;
 - 11) identyfikacja i analiza podatności systemów operacyjnych, serwerów aplikacyjnych i baz danych zarządzanych przez Centrum;
 - 12) identyfikacja i analiza podatności infrastruktury środowiska teleinformatycznego Centrum;
 - 13) identyfikacja i analiza podatności dotyczących złośliwego oprogramowania na stacjach roboczych i serwerach zarządzanych przez Centrum;
 - 14) analiza nadużyć związanych z bezpieczeństwem środowiska teleinformatycznego Centrum;
 - 15) testowanie i wybór nowych narzędzi bezpieczeństwa;
 - 16) nadzór nad niszczeniem wycofywanych z użycia nośników informacji Centrum;
 - 17) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
4. Do zakresu zadań **Wydziału Wewnętrznej Służby Ochrony (DUT4)** należy w szczególności:
- 1) zapewnienie bezpieczeństwa osób i mienia znajdujących się w granicach chronionych obszarów i obiektów Centrum;

- 2) zapobieganie zakłóceniom porządku oraz dewastacji mienia na terenie Centrum;
 - 3) niezwłoczne powiadomienie organów ścigania o czynach przestępnych zaistniałych na terenie Centrum i zabezpieczenie miejsca ich popełnienia do czasu przybycia organów ścigania;
 - 4) organizacja ruchu osobowego, materiałowego i samochodowego;
 - 5) obsługa elektronicznych urządzeń sygnalizacji alarmowej (p.poż. i napadu) poprzez wykonywanie stałego dozoru sygnałów alarmowych, wizyjnych i akustycznych oraz podejmowanie reakcji, stosownie do tego rodzaju sygnałów;
 - 6) współpraca z komendą Policji w zakresie zapewnienia bezpieczeństwa i ochrony budynków Centrum oraz mienia i osób przebywających na terenie Centrum;
 - 7) współpraca z Państwową Strażą Pożarną w zakresie zabezpieczenia przeciwpożarowego w budynkach Centrum oraz likwidacji pożarów na terenie Centrum;
 - 8) przyjmowanie korespondencji wpływającej do Centrum, przekazywanej przez operatora usługi pocztowej oraz doręczanych przez kurierów przesyłek kurierskich;
 - 9) sprawdzanie stanu opakowania doręczanej korespondencji wpływającej oraz przesyłek kurierskich;
 - 10) potwierdzenie przyjęcia przesyłek poleconych ze zwrotnym potwierdzeniem odbioru i wykazie przesyłek poleconych dostarczonych przez doręczyciela;
 - 11) ewidencjonowanie korespondencji wpływającej do Centrum oraz przesyłek kurierskich w rejestrze korespondencji wpływającej prowadzonym przez pracowników Wydziału Wewnętrznej Służby Ochrony;
 - 12) przekazywanie korespondencji wpływającej oraz przesyłek kurierskich do pracownika obsługującego sekretariat w siedzibie Centrum;
 - 13) sporządzanie i aktualizacja planu ochrony Centrum;
 - 14) podejmowanie działań zmierzających do stałego doskonalenia form i metod ochrony w Centrum;
 - 15) dokonywanie okresowych analiz oceny stanu bezpieczeństwa fizycznego w Centrum;
 - 16) informowanie Dyrektora Centrum oraz bezpośredniego przełożonego o stanie zagrożenia i ochrony w Centrum;
 - 17) sprawowanie nadzoru nad przechowywaniem przedmiotów przeznaczonych do obezwładniania osób za pomocą energii elektrycznej o średniej wartości prądu w obwodzie przekraczającej 10mA, a także ich ewidencjonowanie;
 - 18) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
5. Do zakresu zadań **Inspektora Ochrony Przeciwożarowej (DUT5)** należy w szczególności:
- 1) przeprowadzenie w Centrum kontroli przestrzegania zasad i przepisów dotyczących ochrony przeciwpożarowej;
 - 2) sporządzanie protokołów z kontroli i projektów wniosków w sprawie usunięcia stwierdzonych nieprawidłowości;
 - 3) sprawdzanie gotowości sprzętu i urządzeń przeciwpożarowych na terenie Centrum i prawidłowego ich rozmieszczenia;
 - 4) kontrolowanie właściwej i terminowej konserwacji sprzętu i urządzeń przeciwpożarowych;
 - 5) prowadzenie wszelkiej dokumentacji związanej z ochroną przeciwpożarową Centrum;
 - 6) branie udziału w dochodzeniach przeciwpożarowych;
 - 7) utrzymywanie ścisłego i stałego kontaktu z właściwą terenowo komendą straży pożarnej;
 - 8) przeprowadzenie szkoleń z zakresu wykonywania czynności ochrony przeciwpożarowej i ewakuacji pracowników zgodnie z przepisami o ochronie przeciwpożarowej;

- 9) sporządzanie i przedstawianie bezpośrednio przełożonemu i Dyrektorowi Centrum okresowych analiz stanu z zakresu ochrony przeciwpożarowej wraz z propozycjami przedsięwzięć organizacyjnych i technicznych mających na celu zapobieganie zagrożeniom pożarowym;
- 10) opracowywanie aktów wewnętrznych dotyczących zabezpieczenia przeciwpożarowego;
- 11) ustalanie zadań dla osób kierujących komórką organizacyjną w zakresie ochrony przeciwpożarowej;
- 12) doradztwo w zakresie stosowania przepisów ochrony przeciwpożarowej;
- 13) przeprowadzenie kontroli stanu bezpieczeństwa pożarowego w siedzibie Centrum oraz współpraca z konserwatorami instalacji technicznych zabezpieczeń przeciwpożarowych pod kątem zapewnienia ich sprawności;
- 14) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 23.

Departament Sieci, Usług i Monitorowania (DSM)

1. Do zakresu zadań **Wydziału Projektów i Usług (DSM1)** należy w szczególności:
 - 1) opiniowanie materiałów związanych z realizacją projektów;
 - 2) prowadzenie rejestru projektów Centrum oraz bieżące raportowanie ich stanu;
 - 3) wsparcie realizacji projektów, w których uczestniczy Centrum;
 - 4) utrzymywanie dokumentacji projektowej tworzonej przez Centrum;
 - 5) utrzymywanie informacji o planowanych i świadczonych usługach Centrum, w tym zarządzanie katalogiem usług;
 - 6) przygotowywanie, utrzymywanie i nadzorowanie umów SLA świadczonych przez Centrum i świadczonych na rzecz Centrum;
 - 7) utrzymywanie dokumentacji technicznej i infrastrukturalnej Centrum;
 - 8) budowa, rozwój i zarządzanie wybranymi procesami ITIL;
 - 9) współpraca z właściwymi komórkami organizacyjnymi Ministerstwa Finansów oraz komórkami organizacyjnymi Centrum w obszarze dostarczania usług infrastrukturalnych i projektów;
 - 10) generowanie oraz przekazywanie kierownictwu Centrum raportów odnośnie usług świadczonych przez Centrum;
 - 11) udział w uruchamianiu i realizacji inicjatyw informatycznych;
 - 12) publikacja informacji zamieszczanych na stronie intranetowej Ministerstwa Finansów;
 - 13) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Systemów Monitorowania Infrastruktury (DSM2)** należy w szczególności:
 - 1) planowanie rozwoju, wdrażanie zmian i administrowanie systemami monitorującymi infrastrukturę teleinformatyczną Centrum;
 - 2) administrowanie systemem centralnej bazy elementów konfiguracji zarządzanym przez Centrum;
 - 3) dostarczanie usług z obszaru monitorowania infrastruktury, w tym zarządzania zdarzeniami, zarządzania świadczeniem i wsparciem usług, zarządzania infrastrukturą serwerową i aplikacyjną zarządzanych przez Centrum;
 - 4) współpraca z właściwymi komórkami organizacyjnymi Ministerstwa Finansów oraz komórkami organizacyjnymi Centrum w obszarze monitorowania i zarządzania usługami infrastrukturalnymi;
 - 5) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw zarządzanego oprogramowania;
 - 6) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Wsparcia i Monitorowania (DSM3)** należy w szczególności:

- 1) monitorowanie parametrów infrastruktury teleinformatycznej i poziomu świadczenia usług Centrum;
- 2) zapewnienie pojedynczego punktu kontaktu dla użytkowników usług Centrum, w tym mechanizmów zgłaszania wniosków o standardowe usługi Centrum i ich obsługa oraz uzgadnianie umów o gwarantowanym poziomie wsparcia oraz świadczenia usług;
- 3) zarządzanie procesem realizacji wniosków o usługi infrastrukturalne Centrum;
- 4) realizacja standardowych operacji w zakresie eksploatacji usług Centrum na podstawie zdefiniowanych instrukcji;
- 5) generowanie oraz przekazywanie kierownictwu Centrum raportów odnośnie usług świadczonych przez Centrum;
- 6) publikacja informacji zamieszczanych na stronie internetowej Centrum;
- 7) zapewnienie bieżącego wsparcia dla użytkowników końcowych Centrum, w tym:
 - a) instalowanie i konfigurowanie sprzętu komputerowego, biurowego,
 - b) konserwacja i zgłaszanie sprzętu komputerowego, biurowego do serwisu,
 - c) pomoc merytoryczna w obsłudze sprzętu komputerowego, biurowego, systemów i narzędzi wykorzystywanych przez pracowników Centrum w bieżącej pracy;
- 8) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
4. Do zakresu zadań **Wydziału Telekomunikacji (DSM4)** należy w szczególności:
 - 1) administrowanie siecią Centrum;
 - 2) administrowanie łączami zewnętrznymi;
 - 3) dostarczanie usług z obszaru sieci teleinformatycznej Centrum;
 - 4) planowanie rozwoju i wdrażanie zmian infrastruktury teleinformatycznej Centrum;
 - 5) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw sprzętu teleinformatycznego i oprogramowania;
 - 6) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
5. Do zakresu zadań **Wydziału Zarządzania Siecią Rozległą (DSM5)** należy w szczególności:
 - 1) administrowanie rozległą siecią (Wide Area Network – WAN);
 - 2) dostarczanie usług z obszaru sieci teleinformatycznej WAN;
 - 3) planowanie rozwoju i wdrażanie zmian infrastruktury teleinformatycznej WAN;
 - 4) współpraca z usługodawcami zewnętrznymi w zakresie świadczonych usług sieci WAN;
 - 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 24.

Departament Infrastruktury Teleinformatycznej (DIT)

1. Do zakresu zadań **Wydziału Serwerów Aplikacji i Baz Danych (DIT1)** należy w szczególności:
 - 1) administrowanie serwerami aplikacji, systemami zarządzania bazami danych oraz systemami operacyjnymi z rodziny Linux zarządzanymi przez Centrum;
 - 2) dostarczanie usług z obszaru serwerów aplikacji, baz danych i systemów operacyjnych Linux;
 - 3) planowanie rozwoju i wdrażanie zmian środowisk serwerów aplikacji, baz danych i systemów operacyjnych Linux zarządzanych przez Centrum;
 - 4) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw oprogramowania;
 - 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Systemów Infrastrukturalnych (DIT2)** należy w szczególności:
 - 1) administrowanie systemami na poziomie infrastruktury serwerowej i systemów operacyjnych z rodziny Windows zarządzanymi przez Centrum;

- 2) dostarczanie usług z obszaru platformy wirtualizacji, poczty elektronicznej, zarządzania tożsamością (usługa katalogowa dla resortu finansów) zarządzanych przez Centrum;
 - 3) planowanie rozwoju i wdrażanie zmian środowisk systemów infrastrukturalnych Centrum;
 - 4) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw sprzętu i oprogramowania;
 - 5) zarządzanie infrastrukturą klucza publicznego w Centrum;
 - 6) administrowanie systemami pamięci masowych Centrum;
 - 7) administrowanie systemami kopii bezpieczeństwa w Centrum;
 - 8) dostarczanie usług z obszaru infrastruktury serwerowej, systemów operacyjnych i pamięci masowych (w tym administrowanie sieciami Storage Area Network – SAN) zarządzanych przez Centrum;
 - 9) planowanie rozwoju i wdrażanie zmian w infrastrukturze serwerowej, systemów operacyjnych i pamięci masowych w Centrum;
 - 10) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Integracji i Nowych Technologii (DIT3)** należy w szczególności:
- 1) administrowanie warstwą „middleware” resortu finansów;
 - 2) udział w administrowaniu systemami operacyjnymi z rodziny Linux i Windows zarządzanymi przez Centrum;
 - 3) udział w planowaniu, rozwoju i wdrażaniu zmian w środowiskach systemów infrastrukturalnych, w warstwie middleware, infrastrukturze serwerowej i systemach operacyjnych zarządzanych przez Centrum;
 - 4) udział w uruchamianiu i realizacji inicjatyw informatycznych w zakresie opiniowania i ustalania architektury rozwiązań Centrum, także w kontekście propozycji wdrażania technologii, nie wchodzących w skład katalogu usług Centrum;
 - 5) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw oprogramowania;
 - 6) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 25.

Pion do Spraw Rozwoju i Utrzymania Aplikacji

Departament Rozwoju i Utrzymania Aplikacji Podatkowych (DAP)

1. Do zakresu zadań **Wydziału Architektury IT (DAP1)** należy w szczególności:
 - 1) zarządzanie architekturą usług informatycznych w domenie danych i aplikacji, w tym:
 - a) opracowanie i utrzymanie procesu zarządzania architekturą w Ministerstwie Finansów, między innymi przez:
 - opracowywanie architektury w domenach danych i aplikacji,
 - utrzymanie modeli architektonicznych w podległych domenach,
 - optymalizacja architektury w podległych domenach;
 - b) przeprowadzanie analiz mających na celu optymalizację modeli w domenach danych i aplikacji,
 - c) opracowanie i utrzymanie architektury referencyjnej w podległych domenach,
 - d) opracowanie i utrzymanie pryncypiów architektonicznych,
 - e) wyznaczanie i utrzymywanie standardów w obszarze architektury systemów,
 - f) proponowanie zmian w procesach dostarczania i utrzymania usług informatycznych w celu podnoszenia jakości tych usług dostarczanych Ministerstwu Finansów,
 - g) monitorowanie przestrzegania obowiązujących regulacji w obszarze architektury,

- h) koordynowanie współpracy z komórkami organizacyjnymi Ministerstwa Finansów realizującymi zadania w obszarze architektury będącej w zakresie właściwości komórki organizacyjnej,
 - i) podejmowanie działań, w tym organizowanie warsztatów i spotkań dla pracowników Ministerstwa Finansów, mających na celu poszerzenie wiedzy w obszarze architektury,
 - j) utrzymanie i rozwój repozytorium architektonicznego;
- 2) planowanie zmian systemu informacyjnego resortu finansów z wykorzystaniem zarządzania architekturą korporacyjną;
 - 3) analizowanie oraz opiniowanie projektów aktów prawnych, z punktu widzenia możliwości ich implementacji w systemach informatycznych i ich wpływu na systemy informatyczne eksploatowane w Ministerstwie Finansów;
 - 4) współpraca z wykonawcami zewnętrznymi w zakresie przygotowania architektury usług informatycznych;
 - 5) utrzymanie i rozwój usług integracyjnych;
 - 6) określanie standardów technologicznych dla usług informatycznych;
 - 7) analizowanie technologicznych rozwiązań informatycznych;
 - 8) określanie zasad ładu architektonicznego IT;
 - 9) prowadzenie dokumentacji technicznej pozostającej w zakresie właściwości komórki organizacyjnej;
 - 10) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Inżynierii Wymagań (DAP2)** należy w szczególności:
- 1) prowadzenie analiz biznesowych dla usług informatycznych, w tym:
 - a) zarządzanie wymaganiami oraz regułami biznesowymi,
 - b) modelowanie procesów biznesowych,
 - c) ustalanie pojęć biznesowych i ich modelowanie,
 - d) utrzymywanie aktualności i spójności modeli powstających podczas analizy biznesowej;
 - 2) prowadzenie analiz systemowych dla usług informatycznych, w tym:
 - a) zarządzanie wymaganiami funkcjonalnymi oraz poza funkcjonalnymi,
 - b) modelowanie wymagań funkcjonalnych oraz ich prototypowanie,
 - c) modelowanie danych,
 - d) utrzymywanie aktualności i spójności modeli powstających podczas analizy systemowej;
 - 3) proponowanie zmian w procesach dostarczania i utrzymania usług informatycznych w zakresie właściwości komórki organizacyjnej;
 - 4) planowanie rozwoju technologii w obszarze inżynierii wymagań;
 - 5) utrzymanie i rozwój repozytoriów analitycznych;
 - 6) wdrożenia zmian w procesach dostarczania i utrzymania usług informatycznych, w celu podnoszenia jakości usług dostarczanych komórkom organizacyjnym Ministerstwa Finansów;
 - 7) wyznaczanie i utrzymanie standardów analitycznych;
 - 8) prowadzenie dokumentacji technicznej pozostającej w zakresie właściwości komórki organizacyjnej;
 - 9) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Wytwarzania Oprogramowania (DAP3)** należy w szczególności:
- 1) projektowanie i implementacja systemów informatycznych, w tym:
 - a) projektowanie nowych systemów informatycznych oraz zmian do systemów informatycznych już eksploatowanych,
 - b) przygotowywanie nowych systemów informatycznych i kolejnych wydań tych systemów,

- c) przygotowywanie i utrzymanie kodów źródłowych oprogramowania oraz pakietów instalacyjnych systemów informatycznych,
 - d) współpraca z Ministerstwem Finansów oraz wykonawcami zewnętrznymi w zakresie projektowania i wytwarzania oprogramowania, wsparcia w procesie wytwórczym, odbiorów kodów źródłowych oprogramowania i pakietów instalacyjnych usług informatycznych,
 - e) utrzymanie i rozwój narzędzi i środowisk projektowania i implementacji systemów informatycznych,
 - f) wsparcie projektowe i programistyczne świadczonych usług informatycznych,
 - g) wyznaczanie i utrzymanie standardów w obszarze projektowania i programowania oraz standardów technologicznych,
 - h) monitorowanie przestrzegania regulacji w obszarze projektowania i programowania,
 - i) utrzymanie i rozwój repozytorium projektowego, kodów źródłowych oprogramowania oraz pakietów instalacyjnych usług informatycznych;
- 2) projektowanie i implementowanie informatycznych usług publicznych;
 - 3) utrzymywanie dokumentacji technicznej pozostającej w zakresie właściwości komórki organizacyjnej;
 - 4) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
4. Do zakresu zadań **Wydziału Jakości Oprogramowania (DAP4)** należy w szczególności:
- 1) weryfikowanie jakości dostarczanych systemów informatycznych (wewnętrznych oraz poprzez dostawców zewnętrznych), w tym:
 - a) wykonywanie testów systemowych, akceptacyjnych, integracyjnych i wydajnościowych nowych oraz kolejnych wydań usług informatycznych we współpracy z Ministerstwem Finansów oraz wykonawcami zewnętrznymi,
 - b) współpraca z Ministerstwem Finansów w zakresie przygotowania testów akceptacyjnych,
 - c) monitorowanie i raportowanie wyników testów systemów informatycznych,
 - d) utrzymanie i rozwój środowisk testowych, w tym zarządzanie dostępnością środowisk testowych,
 - e) wyznaczanie i utrzymanie standardów w obszarze testowania usług informatycznych,
 - f) monitorowanie przestrzegania regulacji w obszarze testowania usług informatycznych,
 - g) proponowanie zmian w procesach dostarczania i utrzymania usług informatycznych, w celu podnoszenia jakości tych usług dostarczanych Ministerstwu Finansów,
 - h) podejmowanie działań, w tym organizowanie warsztatów i spotkań dla pracowników Ministerstwa Finansów mających na celu poszerzanie wiedzy w obszarze testowania usług informatycznych,
 - i) utrzymanie i rozwój repozytorium testów;
 - 2) utrzymywanie dokumentacji technicznej pozostającej w zakresie właściwości komórki organizacyjnej;
 - 3) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
5. Do zakresu zadań **Wydziału Systemów Poboru Podatków (DAP5)** należy w szczególności:
- 1) realizowanie zadań w obszarze rozwoju, utrzymania i wsparcia systemów:
 - a) wspierających realizację zadań związanych z obsługą rozliczeń podatkowych,
 - b) rachunkowości podatkowej,
 - c) wspierających wypełnianie i składanie deklaracji i wniosków,
 - d) poboru należności wynikających z grzywien i mandatów,
 - e) metadanych referencyjnych, wzorów dokumentów elektronicznych i słowników,
 - f) systemów wymiany informacji wewnątrzspółnotowej i ze Stanami Zjednoczonymi Ameryki,

- g) rejestracji i ewidencji klientów Krajowej Administracji Skarbowej,
 - h) obsługujących proces egzekucji i zabezpieczeń należności podatkowych i celnych;
 - 2) projektowanie nowych systemów informatycznych oraz zmian do systemów informatycznych już eksploatowanych;
 - 3) przygotowywanie nowych systemów informatycznych i kolejnych wydań tych systemów;
 - 4) przygotowywanie i utrzymanie kodów źródłowych oprogramowania oraz pakietów instalacyjnych systemów informatycznych;
 - 5) administrowanie usługami informatycznymi dostarczonymi Ministerstwu Finansów w zakresie właściwości komórki organizacyjnej;
 - 6) prowadzenie dokumentacji usług informatycznych i procesów, w zakresie właściwości komórki organizacyjnej;
 - 7) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
6. Do zakresu zadań **Wydziału Zarządzania Projektami (DAP6)** należy w szczególności:
- 1) identyfikowanie zmian biznesowych w obszarze IT;
 - 2) priorytetyzowanie zmian biznesowych w obszarze IT;
 - 3) zarządzanie ryzykiem związanym z realizacją zmian biznesowych w obszarze IT;
 - 4) koordynowanie i wsparcie działań przygotowywania, przez właścicieli zmian biznesowych, analiz dla projektowanej zmiany biznesowej w obszarze IT;
 - 5) określanie zasad i procedur wytwarzania systemów informatycznych, w tym utrzymywanie obowiązującej metodyki wytwórczej służącej do formalnego zapisu wymagań, analizy systemowej, produkcji i konserwacji oprogramowania oraz monitorowanie poprawności realizacji procesu wytwórczego;
 - 6) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 26.

Departament Rozwoju i Utrzymania Aplikacji Analitycznych, Celnych i Budżetowych (DAB)

1. Do zakresu zadań **Wydziału Zarządzania Usługami IT (DAB1)** należy w szczególności:
- 1) określanie zasad, kierunków rozwoju i warunków świadczenia usług informatycznych;
 - 2) zarządzanie procesem zarządzania zmianą w usługach i systemach IT;
 - 3) zarządzanie katalogiem usług informatycznych, poprzez:
 - a) utrzymywanie aktualności katalogu usług IT resortu finansów w zakresie usług centralnych i lokalnych,
 - b) publikowanie i utrzymywanie definicji usług w katalogu usług,
 - c) współpracę z klientami w zakresie opracowywania definicji usług;
 - 4) zarządzanie systemami monitorowania usługi, poprzez ich administrowanie, utrzymywanie i eksploatację;
 - 5) określanie wymagań funkcjonalnych dla systemów monitorowania i konfiguracji komponentów usług informatycznych;
 - 6) zarządzanie poziomem usług informatycznych, poprzez:
 - a) uzgadnianie poziomu jakości usług,
 - b) monitorowanie jakości usług IT,
 - c) raportowanie poziomu usług klientowi,
 - d) dokonywanie okresowych przeglądów usług w celu ich oceny i identyfikacji możliwości doskonalenia poziomu jakości,
 - e) przeprowadzanie okresowych badań satysfakcji użytkowników usług;
 - 7) współpraca z Ministerstwem Finansów w zakresie:
 - a) identyfikacji potrzeb dostawy nowych oraz modyfikacji świadczonych usług informatycznych,
 - b) planowania dostaw usług informatycznych i ich zmian,

- c) organizacji wsparcia przy wdrażaniu usług informatycznych,
 - d) organizacji utrzymania usług informatycznych;
- 8) proponowanie zmian w procesach dostarczania i utrzymania usług informatycznych w celu podnoszenia jakości tych usług dostarczanych Ministerstwu Finansów;
 - 9) koordynowanie przejmowania do eksploatacji usług informatycznych;
 - 10) pełnienie wiodącej roli w budowie i rozwijaniu usługowego modelu współpracy departamentu z Ministerstwem Finansów w zakresie świadczenia usług informatycznych dla Ministerstwa Finansów;
 - 11) opracowywanie, utrzymywanie oraz monitorowanie porozumień SLA pomiędzy departamentem a klientami usług informatycznych;
 - 12) rozwijanie funkcjonalności oprogramowania specjalistycznego do zarządzania usługami informatycznymi, w zakresie właściwości komórki organizacyjnej;
 - 13) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Systemów Budżetowych (DAB2)** należy w szczególności:
 - 1) realizowanie zadań w obszarze utrzymania i wsparcia rozwoju systemów do obsługi budżetu państwa i jednostek samorządu terytorialnego;
 - 2) projektowanie nowych systemów informatycznych oraz zmian do systemów informatycznych już eksploatowanych;
 - 3) przygotowywanie nowych systemów informatycznych i kolejnych wydań tych systemów;
 - 4) przygotowywanie i utrzymanie kodów źródłowych oprogramowania oraz pakietów instalacyjnych systemów informatycznych;
 - 5) prowadzenie dokumentacji usług informatycznych i procesów w zakresie właściwości komórki organizacyjnej;
 - 6) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
 3. Do zakresu zadań **Wydziału Systemów Celnych (DAB3)** należy w szczególności:
 - 1) realizowanie zadań w obszarze rozwoju, utrzymania i wsparcia systemów zapewniających wymianę informacji pomiędzy państwami członkowskimi Wspólnoty Europejskiej oraz Organizacji Współpracy Gospodarczej i Rozwoju, w zakresie transakcji dokonywanych wewnątrz Wspólnoty oraz Organizacji Współpracy Gospodarczej i Rozwoju oraz informacji o podatnikach VAT zarejestrowanych dla potrzeb handlu wewnątrz UE;
 - 2) zapewnienie sprawności technicznej warstwy aplikacyjnej systemów informatycznych, w szczególności poprzez:
 - a) zarządzanie unijną Siecią CCN / CCN2,
 - b) projektowanie nowych systemów informatycznych oraz zmian do systemów informatycznych już eksploatowanych,
 - c) przygotowywanie nowych systemów informatycznych i kolejnych wydań tych systemów,
 - d) przygotowywanie i utrzymanie kodów źródłowych oprogramowania oraz pakietów instalacyjnych systemów informatycznych,
 - e) zapewnienie odpowiedniej wydajności systemów informatycznych,
 - f) weryfikacja i obsługa zgłoszeń otrzymanych od użytkowników oraz wykonywanie prac niezbędnych do eksploatacji systemów,
 - g) współpraca z użytkownikami w zakresie rozwiązywania incydentów i realizacji wniosków,
 - h) usuwanie awarii,
 - i) instalowanie nowych wydań i patch'y,
 - j) instalowanie kluczy licencyjnych;
 - 3) wsparcie projektowe i programistyczne eksploatowanych systemów informatycznych;

- 4) administrowanie techniczne warstwą aplikacyjną systemów informatycznych w stopniu umożliwiającym zachowanie jej bezpieczeństwa i zabezpieczenie danych przed nieupoważnionym dostępem;
- 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
4. Do zakresu zadań **Wydziału Systemów Analitycznych (DAB4)** należy w szczególności:
 - 1) realizowanie zadań w obszarze utrzymania i wsparcia rozwoju:
 - a) systemów kontrolnych i audytowych,
 - b) systemów do gromadzenia, przechowywania, integracji i udostępniania danych,
 - c) systemów analitycznych, analizy ryzyka, raportowych i sprawozdawczych;
 - 2) zapewnienie utrzymania i rozwoju hurtowni danych w tym:
 - a) przygotowywanie widoków struktur danych oraz raportów danych,
 - b) obsługa zasileń hurtowni i przetwarzania danych,
 - c) tworzenie i optymalizacja zapytań danych do hurtowni,
 - d) monitorowanie i koordynacja procesów realizowanych w ramach hurtowni danych,
 - e) obsługa zgłoszeń w Centralnym Service Desku dotyczących hurtowni danych,
 - f) zapewnienie i utrzymanie narzędzi analitycznych do hurtowni danych,
 - g) nadzór nad mechanizmami integracji hurtowni danych z systemami dziedzinowymi, działającymi na rzecz departamentów merytorycznych,
 - h) utrzymanie i rozwój modeli analitycznych/rozwiązań pracujących w obszarach hurtowni danych;
 - 3) współpraca przy budowie i rozwoju centralnej hurtowni danych resortu;
 - 4) administrowanie usługami informatycznymi dostarczonymi Ministerstwu Finansów w zakresie właściwości komórki organizacyjnej;
 - 5) pełnienie roli administratora technicznego STIR;
 - 6) prowadzenie dokumentacji usług informatycznych i procesów, w zakresie właściwości komórki organizacyjnej;
 - 7) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 27.

Departament Wsparcia Informatycznego i Utrzymania Stacji Roboczych (DWU)

1. Do zakresu zadań **Wydziału Centralnego Service Desku (DWU1)** należy w szczególności:
 - 1) koordynowanie działań związanych z określaniem wymagań funkcjonalnych oraz wdrożeniem Centralnego Service Desku dla resortu finansów;
 - 2) zarządzanie procesem wsparcia użytkowników usług informatycznych, świadczonych przez centralne systemy informatyczne eksploatowane w resorcie finansów, w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) informowanie użytkowników o stanie realizacji zgłoszenia,
 - e) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi, Ministerstwem Finansów oraz wykonawcami zewnętrznymi,
 - f) monitorowanie postępów prac nad zgłoszeniami;
 - 3) optymalizacja jakości świadczonych usług informatycznych, poprzez:
 - a) monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - b) zarządzanie i monitorowanie uaktualniania Baz Wiedzy,
 - c) realizacja i publikacja raportów z obsługi w Service Desk zgłoszeń, incydentów, wniosków,

- d) badanie satysfakcji użytkowników z realizacji wsparcia świadczonego dla usług informatycznych,
 - e) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 4) zapewnienie przekazywania użytkownikom informacji w zakresie dostępności usług informatycznych, w tym informowanie użytkowników o istotnych zmianach, utrudnieniach i przestojach w działaniu usług centralnych;
 - 5) rozwijanie funkcjonalności i zarządzanie systemem wsparcia informatycznego, w zakresie właściwości komórki organizacyjnej;
 - 6) utrzymywanie funkcji Service Desk, zarządzanie procesami: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem, poprzez analizę i nadzór nad stanem zgłoszeń, wniosków, incydentów oraz problemów;
 - 7) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - 8) zgłaszanie postulatów zmian oraz propozycji nowych rozwiązań funkcjonalności systemów informatycznych;
 - 9) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
 - 10) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Aplikacji i Oprogramowania Stacji Roboczych (DWU2)** należy w szczególności:
- 1) zarządzanie procesem wsparcia użytkowników usług informatycznych w obszarze oprogramowania, w tym:
 - a) przywracanie funkcjonowania świadczonych usług z zakresu informatycznych stanowisk pracy,
 - b) zapewnienie możliwości pracy użytkownikom systemów informatycznych Ministerstwa Finansów, polegające na instalacji sprzętu komputerowego, oprogramowania systemowego, aplikacji biurowych oraz oprogramowania wspomagającego i specjalistycznego, a także pomocy merytorycznej dla użytkowników Ministerstwa Finansów w obsłudze aplikacji biurowych, systemu operacyjnego i urządzeń mobilnych;
 - 2) utrzymywanie zarządzanej infrastruktury komputerowej, w tym urządzeń mobilnych, zgodnie z zasadami bezpieczeństwa teleinformatycznego, we współpracy z Wydziałem Administrowania Systemami do Przetwarzania Informacji Niejawnych oraz Zabezpieczeń Aplikacji;
 - 3) wdrażanie zmian w podległej infrastrukturze komputerowej;
 - 4) analiza zapotrzebowania na oprogramowanie standardowe w Ministerstwie Finansów;
 - 5) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw oprogramowania;
 - 6) udział w projektach informatycznych w zakresie:
 - a) opiniowania i ustalania zapewnienia drugiej linii wsparcia, po przekazaniu systemu do eksploatacji w zakresie usług lokalnych Ministerstwa Finansów,
 - b) opiniowania i ustalania zasobów infrastruktury komputerowej, niezbędnych do funkcjonowania systemu informatycznego, po przekazaniu systemu do eksploatacji;
 - 7) opracowywanie i utrzymanie standardów dotyczących oprogramowania;
 - 8) zarządzanie:
 - a) usługą katalogową Active Directory obsługującą pracowników Ministerstwa Finansów,
 - b) systemem wideokonferencyjnym Skype For Bussines,
 - c) systemem pomocy zdalnej,
 - d) stacjami końcowymi użytkowników;

- 9) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Infrastruktury Komputerowej i Logistyki Informatycznej (DWU3)** należy w szczególności:
- 1) zarządzanie procesem wsparcia użytkowników usług informatycznych w obszarze infrastruktury komputerowej, w tym:
 - a) przywracanie funkcjonowania świadczonych usług z zakresu informatycznych stanowisk pracy,
 - b) zapewnienie możliwości pracy użytkownikom systemów informatycznych Ministerstwa Finansów, polegające na:
 - pomocy merytorycznej dla użytkowników Ministerstwa Finansów w obsłudze sprzętu informatycznego,
 - instalacji sprzętu drukującego, skanującego i oprogramowania dedykowanego dla infrastruktury komputerowej,
 - bieżącej konserwacji i serwisu sprzętu komputerowego;
 - 2) planowanie rozwoju podległej infrastruktury komputerowej;
 - 3) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw sprzętu komputerowego oraz drukującego;
 - 4) zarządzanie urządzeniami drukującymi/komputerowymi będącymi w posiadaniu Ministerstwa Finansów, w tym wyposażanie Ministerstwa Finansów w urządzenia drukujące i komputerowe oraz zapewnianie ich prawidłowego działania;
 - 5) analizowanie potrzeb i planowanie zakupów nowych urządzeń drukujących/komputerowych, części zamiennych oraz materiałów eksploatacyjnych;
 - 6) weryfikowanie celowości zakupów w zakresie sprzętu komputerowego, w celu zapewnienia informatycznych stanowisk pracy w Ministerstwie Finansów;
 - 7) zarządzanie sprzętem komputerowym i przydzielanie oprogramowania w Ministerstwie Finansów, w tym:
 - a) opracowywanie i utrzymanie standardów w zakresie spraw związanych z zarządzaniem licencjami oprogramowania i sprzętem komputerowym,
 - b) przydzielanie poszczególnym usługom informatycznym właściwego oprogramowania oraz licencji,
 - c) zarządzanie zasobami niezbędnymi do zapewnienia informatycznych stanowisk pracy,
 - d) wnioskowanie w szczególności w sprawach zakupów, zwrotów, przemieszczeń, utylizacji, nieodpłatnego przekazywania składników majątku do innych jednostek, zgodnie z odrębnymi przepisami,
 - e) aktualizacja danych w systemie ewidencji mienia;
 - 8) prowadzenie magazynu informatycznego, zgodnie z obowiązującymi przepisami w zakresie gospodarki magazynowej;
 - 9) wycofywanie sprzętu komputerowego, urządzeń drukujących wyeksploatowanych technicznie oraz prowadzenie spraw związanych ze sprzedażą lub nieodpłatnym przekazaniem urządzeń, zgodnie z odrębnymi przepisami;
 - 10) współpraca z właściwą komórką organizacyjną Centrum w przygotowywaniu zamówień informatycznych w ramach grupowych wniosków zakupowych;
 - 11) koordynowanie prac związanych z rozliczaniem umów na zakupy i zamówienia informatyczne na potrzeby ewidencji mienia, we współpracy z właściwą komórką organizacyjną Centrum;
 - 12) współpraca z właściwą komórką organizacyjną Centrum w zakresie rozliczania zakupów informatycznych na potrzeby ewidencji mienia, tj. środków trwałych, pozostałych środków trwałych, praw na dobrach niematerialnych, a także prowadzonych inwentaryzacji mienia według planów inwentaryzacji za dany rok;
 - 13) użyczanie sprzętu informatycznego i oprogramowania na rzecz Ministerstwa Finansów i resortu finansów;

- 14) administrowanie sprzętem użyczonym na rzecz Ministerstwa Finansów i resortu finansów;
 - 15) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
4. Do zakresu zadań **Wydziału Wsparcia Informatycznego (DWU4)** należy w szczególności:
- 1) zarządzanie procesem wsparcia użytkowników usług informatycznych, świadczonych przez lokalne systemy informatyczne, eksploatowane w Ministerstwie Finansów, w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi, Ministerstwem Finansów oraz wykonawcami zewnętrznymi,
 - e) monitorowanie postępów prac nad zgłoszeniami;
 - 2) optymalizacja jakości świadczonych usług informatycznych, poprzez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) udział w tworzeniu porozumień SLA oraz OLA;
 - 4) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
5. Do zakresu zadań **Wydziału Sieci LAN w Ministerstwie Finansów (DWU5)** należy w szczególności:
- 1) zarządzanie lokalną siecią teleinformatyczną w budynku Ministerstwa Finansów, zwaną dalej „siecią strukturalną LAN”, w tym:
 - a) konfiguracja urządzeń sieciowych,
 - b) planowanie rozbudowy/modyfikacji sieci strukturalnej LAN,
 - c) zarządzanie siecią Wi-Fi,
 - d) utrzymanie infrastruktury sieciowej zgodnie z zasadami/standardami bezpieczeństwa,
 - e) zarządzanie urządzeniami sieciowymi;
 - 2) zarządzanie procesem wsparcia użytkowników usług informatycznych w obszarze infrastruktury sieci strukturalnej LAN, w tym:
 - a) przywracanie funkcjonowania świadczonych usług z zakresu informatycznych stanowisk pracy,
 - b) zapewnienie możliwości pracy użytkownikom systemów informatycznych Ministerstwa Finansów, polegającej na konfiguracji urządzeń sieciowych, a także pomocy merytorycznej dla użytkowników systemów informatycznych Ministerstwa w zakresie zagadnień związanych z siecią strukturalną LAN;
 - 3) analizowanie potrzeb i planowanie zakupów urządzeń sieciowych, w tym wszystkich podzespołów niezbędnych do sprawnego funkcjonowania sieci strukturalnej LAN;
 - 4) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw sprzętu związanego z siecią strukturalną LAN;
 - 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 28.

Departament Rozwoju i Utrzymania Aplikacji e-Usługowych oraz Aplikacji Gospodarki Własnej (DEG)

1. Do zakresu zadań **Wydziału Systemów Gospodarki Własnej i Wsparcia Zarządzania (DEG1)** należy w szczególności:
 - 1) realizowanie zadań w obszarze rozwoju, utrzymania i wsparcia:
 - a) systemów gospodarki własnej,
 - b) systemów elektronicznego zarządzania dokumentacją,
 - c) serwisów WWW i biuletynów informacji publicznej,
 - d) narzędzi do ankietowania,
 - e) systemów e-learningowych,
 - f) systemów do przekazywania informacji o schematach podatkowych;
 - 2) projektowanie nowych systemów informatycznych oraz zmian do systemów informatycznych już eksploatowanych;
 - 3) przygotowywanie nowych systemów informatycznych i kolejnych wydań tych systemów;
 - 4) przygotowywanie i utrzymanie kodów źródłowych oprogramowania oraz pakietów instalacyjnych systemów informatycznych;
 - 5) administrowanie usługami informatycznymi dostarczonymi komórkom organizacyjnym Ministerstwa Finansów z obszaru właściwości komórki organizacyjnej;
 - 6) prowadzenie dokumentacji usług informatycznych i procesów w zakresie właściwości komórki organizacyjnej;
 - 7) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
2. Do zakresu zadań **Wydziału Rozwoju i Utrzymania Aplikacji e-Uslugowych (DEG2)** należy w szczególności:
 - 1) koordynowanie działań związanych z dostarczaniem Ministerstwu Finansów nowych oraz zmodyfikowanych aplikacji e-usługowych;
 - 2) koordynowanie i wsparcie działań przygotowywania, przez właścicieli zmian biznesowych, analiz dla projektowanej zmiany biznesowej w ramach aplikacji e-Uslugowych;
 - 3) priorytetyzowanie zmian biznesowych w ramach aplikacji e-Uslugowych;
 - 4) zarządzanie ryzykiem związanym z rozwojem i utrzymaniem aplikacji e-Uslugowych;
 - 5) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.
3. Do zakresu zadań **Wydziału Automatyzacji i Robotyzacji (DEG3)** należy w szczególności:
 - 1) analizowanie i mapowanie procesów biznesowych;
 - 2) optymalizowanie i przygotowywanie procesów biznesowych do automatyzacji i robotyzacji;
 - 3) analiza korzyści z wdrożenia automatyzacji i robotyzacji;
 - 4) budowa, wdrożenie i utrzymanie automatyzacji i robotów;
 - 5) udział w tworzeniu strategii zastosowania automatyzacji i robotyzacji;
 - 6) zarządzanie ryzykiem związanym z rozwojem i utrzymaniem automatyzacji i robotyzacji;
 - 7) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 29.

Pion do Spraw Informatyki Resortu Finansów

Departament Zarządzania Regionem Wschodnim (RWS)

1. Do zakresu zadań **Biura Wsparcia (RWS1BW)** należy w szczególności:
 - 1) wsparcie osób zarządzających departamentem w zakresie obsługi biurowej;
 - 2) wsparcie w zapewnieniu dyscypliny pracy w podległych komórkach organizacyjnych;

- 3) wsparcie w skutecznym przepływie informacji wewnątrz regionu;
- 4) wsparcie w procesie planowania budżetu rzeczowo-finansowego regionu w zakresie właściwości podległych komórek organizacyjnych;
- 5) obsługa obiegu dowodów finansowo-księgowych dotyczących zakupów realizowanych na potrzeby podległych komórek organizacyjnych

2. Oddział Zarządzania Regionem Podlaskim (RWS2):

1) do zakresu zadań **Zespołu Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej (RWS2BIID)** należy w szczególności:

- a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania,
- b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
- c) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania,
- d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,
- e) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
- f) współpraca z komórką bezpieczeństwa i ochrony informacji w Izbie Administracji Skarbowej w Białymstoku w zakresie zarządzania bezpieczeństwem teleinformatycznym,
- g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
- h) administrowanie serwerowniami i sprzętem serwerowym,
- i) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
- j) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
- k) planowanie rozbudowy i modyfikacji podległej infrastruktury,
- l) zarządzanie kopiami bezpieczeństwa,
- m) administrowanie domeną na poziomie regionalnym,
- n) nadzorowanie systemów bezpieczeństwa obiektów granicznych,
- o) wsparcie użytkowników usług informatycznych w zakresie:
 - analizowania, weryfikowania i rozwiązywania zgłoszeń oraz udzielanie konsultacji użytkownikom regionu,
 - przekazywania nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - optymalizacji jakości świadczonych usług informatycznych między innymi poprzez inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,

2) do zakresu zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RWS2BIIL)** należy w szczególności:

- a) przygotowywanie, wdrażanie i administrowanie nowych lokalnych, regionalnych i centralnych systemów informatycznych,

- b) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Białymstoku i podległymi jej urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
- c) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
- d) rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
- e) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
- f) prowadzenie dokumentacji usług informatycznych,
- g) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-iej linii wsparcia, regionalnie i lokalnie,
- h) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych,
- i) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
- j) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,
- k) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
- l) realizacja zadań scentralizowanych w zakresie:
 - utrzymania i rozwoju procedur poboru obszaru RB hurtowni WHTAX,
 - utrzymania i rozwoju aplikacji SPIN-System Prezentacji Informacji dla Nadzoru,
 - utrzymania i rozwoju aplikacji RATY-Rozkładanie na raty zobowiązań podatkowych,
- m) realizacja zadań z zakresu wsparcia informatycznego komórek organizacyjnych IAS Białystok,
- n) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
 - wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - prowadzenie analiz systemowych dla usług informatycznych,
 - projektowanie usług informatycznych,
 - implementacja usług informatycznych,
 - weryfikowanie jakości dostarczanych usług informatycznych,
 - administrowanie techniczne komponentami usług informatycznych,
- o) udzielanie merytorycznego i technicznego wsparcia dla struktur regionalnych zarządzanych systemów centralnych,
- p) wsparcie użytkowników usług informatycznych w zakresie:
 - analizowania, weryfikowania i rozwiązywania zgłoszeń oraz udzielanie konsultacji użytkownikom regionu,
 - przekazywania nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - optymalizacji jakości świadczonych usług informatycznych między innymi poprzez inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- q) wsparcie komórki Ministerstwa Finansów właściwej do spraw bezpieczeństwa i ochrony informacji w zakresie utrzymania i rozwoju Systemu Infrastruktury Klucza Publicznego (PKI), w tym:
 - prowadzenie wsparcia użytkowników,
 - zapewnienie ciągłości działania systemu,
 - utrzymanie, administrowanie i rozwój systemu w zakresie uzgodnionym z właścicielem biznesowym systemu,

- projektowanie i wdrażane zmian w zakresie merytorycznym i technicznym uzgodnionych z właścicielem biznesowym systemu,
- 3) do zakresu zadań **Zespołu Planowania i Logistyki Informatycznej oraz Helpdesk (RWS2BIIP)** należy w szczególności:
- a) planowanie rozwoju podległej infrastruktury informatycznej,
 - b) prowadzenie spraw z zakresu planowania i wykonywania inwestycji dotyczących przejść granicznych w porozumieniu z wojewodą oraz innymi instytucjami, ich modernizacji w zakresie elektronicznych systemów ochrony obiektów i teletechniki,
 - c) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie i podległych urzędach,
 - d) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
 - e) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
 - f) wsparcie osób zarządzających oddziałem w zakresie obsługi biurowej,
 - g) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami,
 - h) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - i) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
 - j) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
 - k) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie i podległych urzędach,
 - l) realizacja zadań z zakresu wsparcia informatycznego komórek organizacyjnych Izby,
- 4) do zakresu zadań **Pierwszego Zespołu Wsparcia Informatycznego (RWS2BIIW1)** należy w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,

- c) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - e) wsparcie techniczne zadań związanych z informatyką śledczą,
 - g) realizacja zadań z zakresu wsparcia informatycznego komórek organizacyjnych w obiektach:
 - Pierwszego Urzędu Skarbowego w Białymstoku,
 - Drugiego Urzędu Skarbowego w Białymstoku,
 - Podlaskiego Urzędu Skarbowego w Białymstoku,
 - Urzędu Skarbowego w Bielsku Podlaskim,
 - Urzędu Skarbowego w Siemiatyczach,
 - Urzędu Skarbowego w Sokółce,
 - Urzędu Skarbowego w Hajnówce,
 - Urzędu Skarbowego w Mońkach
 oraz innych komórek w tych lokalizacjach,
 - h) wsparcie użytkowników usług informatycznych w zakresie:
 - analizowania, weryfikowania i rozwiązywania zgłoszeń oraz udzielanie konsultacji użytkownikom regionu,
 - przekazywania nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - optymalizacji jakości świadczonych usług informatycznych między innymi poprzez inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- 5) do zakresu zadań **Drugiego Zespołu Wsparcia Informatycznego (RWS2BIIW2)** należy w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - c) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,

- nadzorowanie systemów bezpieczeństwa obiektów,
- d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
- e) realizacja zadań z zakresu wsparcia informatycznego komórek organizacyjnych w obiektach:
 - Urzędu Skarbowego w Łomży,
 - Urzędu Skarbowego w Kolnie,
 - Urzędu Skarbowego w Grajewie,
 - Urzędu Skarbowego w Zambrowie,
 - Urzędu Skarbowego w Wysokiem Mazowieckiem,
 - Podlaskiego Urzędu Celno-Skarbowego w Białymstoku zlokalizowanych w Łomży,
 - Delegatury Podlaskiego Urzędu Celno-Skarbowego w Łomży,
 - Oddziału Celnego w Łomży
 oraz innych komórek w tych lokalizacjach,
- f) wsparcie użytkowników usług informatycznych w zakresie:
 - analizowania, weryfikowania i rozwiązywania zgłoszeń oraz udzielanie konsultacji użytkownikom regionu,
 - przekazywania nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - optymalizacji jakości świadczonych usług informatycznych między innymi poprzez inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- 6) do zakresu zadań **Trzeciego Zespołu Wsparcia Informatycznego (RWS2BIIW3)** należy w szczególności:
 - a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - c) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - nadzorowanie systemów bezpieczeństwa obiektów,
 - d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - e) realizacja zadań z zakresu wsparcia informatycznego komórek organizacyjnych w obiektach:
 - Urzędu Skarbowego w Suwałkach,
 - Stałego Punktu Obsługi Podatników w Sejnach,
 - Urzędu Skarbowego w Augustowie,
 - Podlaskiego Urzędu Celno-Skarbowego w Białymstoku zlokalizowanych w Budzisku,

- Delegatury Podlaskiego Urzędu Celno-Skarbowego w Suwałkach,
 - Oddziału Celnego w Suwałkach,
 - Oddziału Celnego w Augustowie,
 - Miejsca Wyznaczonego w Rudawce
- oraz innych komórek w tych lokalizacjach,
- f) wsparcie użytkowników usług informatycznych w zakresie:
- analizowania, weryfikowania i rozwiązywania zgłoszeń oraz udzielanie konsultacji użytkownikom regionu,
 - przekazywania nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - optymalizacji jakości świadczonych usług informatycznych między innymi poprzez inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,

3. Oddział Zarządzania Regionem Mazowieckim (RWS3):

- 1) do zadań **Zespołu Bezpieczeństwa Informatycznego (RWS3MIID)** należy w szczególności:
- a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - c) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowywanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
 - d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia, w tym w zakresie stanowisk komputerowych udostępnionych podatnikom w podległych urzędach;
 - e) opracowywanie dokumentacji bezpieczeństwa teleinformatycznego;
 - f) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Warszawie;
 - g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji;
- 2) Do zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy (RWS3MIIL)** należy w szczególności:
- a) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
 - b) współpraca z komórkami organizacyjnymi izby i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
 - c) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
 - d) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;

- e) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
 - f) prowadzenie dokumentacji usług informatycznych;
 - g) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie;
 - h) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
 - i) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
 - j) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;
 - k) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy;
 - l) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów;
- 3) Do zadań **Zespołu Helpdesk (RWS3MIIH)** należy w szczególności:
- a) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi izby i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami;
 - b) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - c) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - d) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,;
 - e) określanie pozafunkcjonalnych wymagań dla lokalnych systemów informatycznych w Izbie i podległych urzędach;
 - f) zarządzanie katalogiem usług informatycznych poprzez:
 - określanie zawartości i formy katalogu usług,
 - utrzymywanie aktualności katalogu usług,
 - współpracę z klientami w zakresie opracowywania katalogu usług;
 - g) zarządzanie procesami: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem, poprzez analizę i nadzór nad stanem zgłoszeń, wniosków incydentów oraz problemów;
 - h) identyfikowanie poziomu usług informatycznych poprzez:
 - monitorowanie usług,
 - raportowanie poziomu usług,
 - dokonywanie okresowych przeglądów usług w celu ich oceny oraz zapewnienia uzgodnionego poziomu jakości,

- przeprowadzanie okresowych badań satysfakcji użytkowników usług;
 - i) zgłaszanie postulatów zmian oraz propozycji nowych rozwiązań funkcjonalności systemów informatycznych;
- 4) Do zadań **Wydziału Wsparcia Informatycznego** (RWS3MIIW) w skład którego wchodzi **Pierwszy Zespół Wsparcia Informatycznego** (RWS3MIIW1), **Drugi Zespół Wsparcia Informatycznego** (RWS3MIIW2), **Trzeci Zespół Wsparcia Informatycznego** (RWS3MIIW3), **Czwarty Zespół Wsparcia Informatycznego** (RWS3MIIW4), **Piąty Zespół Wsparcia Informatycznego** (RWS3MIIW5), **Szósty Zespół Wsparcia Informatycznego** (RWS3MIIW6), **Siódmy Zespół Wsparcia Informatycznego** (RWS3MIIW7) należy w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - c) administrowanie lokalnymi systemami informatycznymi w obsługiwanych urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - e) wsparcie techniczne zadań związanych z informatyką śledczą;
 - f) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych urzędach;
 - g) koordynacja i realizacja wsparcia informatycznego w Izbie i urzędach;
 - h) prowadzenie dokumentacji Wydziału;
 - i) współpraca z Wieloosobowym Stanowiskiem ds. Infrastruktury Sieciowej i Serwerowej w zakresie utrzymywania infrastruktury sieciowej i serwerowej zgodnie z zasadami i standardami bezpieczeństwa w Izbie i urzędach;
 - j) prowadzenie dokumentacji lokalnych usług informatycznych;
- 5) Do zadań **Zespołu Systemów Centralnych** (RWS3MIIC) należy w szczególności:
- a) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych;
 - b) prowadzenie analiz systemowych dla usług informatycznych;
 - c) projektowanie usług informatycznych;
 - d) implementacja usług informatycznych;
 - e) weryfikowanie jakości dostarczanych usług informatycznych;
 - f) administrowanie techniczne komponentami usług informatycznych;
 - g) utrzymywanie oraz aktualizacja aplikacji e-ORUS na rzecz wszystkich izb administracji skarbowej i urzędów w kraju.

- 1) Do zadań **Sekcji do Spraw Infrastruktury Sieciowej i Serwerowej (RWS3MIIS)** należy w szczególności:
 - a) administrowanie serwerowniami i sprzętem serwerowym;
 - b) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - c) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - d) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - e) zarządzanie kopiami bezpieczeństwa;

- 2) Do zadań **Sekcji do Spraw Planowania i Logistyki Informatycznej (RWS3MIIP)** należy w szczególności:
 - a) planowanie rozwoju podległej infrastruktury informatycznej;
 - b) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w izbie i podległych urzędach;
 - c) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania;
 - d) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
 - e) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej;
 - f) tworzenie i prowadzenie dokumentacji o udzielenie zamówienia publicznego w zakresie definiowania opisu przedmiotu zamówienia;
 - g) odbiór jakościowy i ilościowy zamawianego sprzętu;

4. Oddział Zarządzania Regionem Lubelskim (RWS4):

- 1) do zadań **Sekcji Bezpieczeństwa Informatycznego (RWS4LIID)** należy w szczególności:
 - a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - c) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
 - d) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
 - e) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia;
 - f) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
 - g) współpraca z komórką bezpieczeństwa i ochrony informacji w Izbie Administracji Skarbowej w Lublinie w zakresie realizowania, koordynowania i nadzoru nad realizacją w izbie i podległych urzędach zadań w obszarze bezpieczeństwa teleinformatycznego;
 - h) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji;

- i) testowanie i wdrażanie nowych wydań i poprawek systemu (WSUS);
 - j) zarządzanie oprogramowaniem antywirusowym na poziomie regionu;
 - k) nadzór nad niszczeniem wycofywanych z użycia nośników informacji;
 - l) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych.
- 2) Do zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy oraz Helpdesku (RWS4LIH)** należy w szczególności:
- a) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
 - b) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Lublinie w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
 - c) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
 - d) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
 - e) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
 - f) prowadzenie dokumentacji usług informatycznych;
 - g) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II linii wsparcia, regionalnie i lokalnie;
 - h) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
 - i) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
 - j) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy;
 - k) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących systemy informatyczne resortu finansów, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi izby i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami;
 - l) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - m) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - n) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
 - o) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w izbie i podległych urzędach.

- 3) Do zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych – Centrum Kompetencyjne (RWS4LIIL)** należy w szczególności:
- a) wdrażanie i administrowanie lokalnymi i regionalnymi systemami informatycznymi;
 - b) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Lublinie w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
 - c) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
 - d) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
 - e) prowadzenie dokumentacji usług informatycznych;
 - f) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II linii wsparcia, regionalnie i lokalnie;
 - g) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
 - h) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
 - i) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;
 - j) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
 - k) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w izbie i podległych urzędach;
 - l) administrowanie sprzętem serwerowym, lokalną siecią komputerową i urządzeniami sieciowymi;
- 4) Do zadań **Pierwszego Zespołu Wsparcia Informatycznego (RWS4LIW-1)** należy świadczenie usług informatycznych w Lubelskim Urzędzie Skarbowym w Lublinie, Pierwszym Urzędzie Skarbowym w Lublinie, Urzędzie Skarbowym w Białej Podlaskiej, Urzędzie Skarbowym w Lubartowie, Urzędzie Skarbowym w Łukowie, Urzędzie Skarbowym w Opolu Lubelskim, Urzędzie Skarbowym w Parczewie, Urzędzie Skarbowym w Puławach, Urzędzie Skarbowym w Radzynie Podlaskiej, Urzędzie Skarbowym w Rykach, Urzędzie Skarbowym we Włodawie, w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - c) administrowanie lokalnymi systemami informatycznymi, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;

- e) administrowanie serwerowniami i sprzętem serwerowym;
 - f) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - g) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - h) zarządzanie na poziomie lokalnym kontami użytkowników w wybranych systemach i aplikacjach centralnych (zakładanie kont, nadawanie, modyfikacja, odbieranie uprawnień);
 - i) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych poprzez formułowanie zapytań do baz danych, tworzenie skryptów;
- 5) Do zadań **Drugiego Zespołu Wsparcia Informatycznego (RWS4LIIW-2)** należy świadczenie usług informatycznych w Drugim Urzędzie Skarbowym w Lublinie, Trzecim Urzędzie Skarbowym w Lublinie, Urzędzie Skarbowym w Biłgoraju, Urzędzie Skarbowym w Chełmie, Urzędzie Skarbowym w Hrubieszowie, Urzędzie Skarbowym w Janowie Lubelskim, Urzędzie Skarbowym w Krasnymstawie, Urzędzie Skarbowym w Kraśniku, Urzędzie Skarbowym w Tomaszowie Lubelskim, Urzędzie Skarbowym w Zamościu, Urzędzie Skarbowym w Łęcznej, w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - c) administrowanie lokalnymi systemami informatycznymi, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - e) administrowanie serwerowniami i sprzętem serwerowym;
 - f) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - g) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - h) zarządzanie na poziomie lokalnym kontami użytkowników w wybranych systemach i aplikacjach centralnych (zakładanie kont, nadawanie, modyfikacja, odbieranie uprawnień);
 - i) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych poprzez formułowanie zapytań do baz danych, tworzenie skryptów;
- 6) Do zadań **Trzeciego Zespołu Wsparcia Informatycznego (RWS4LIIW-3)** należy świadczenie usług informatycznych dla oddziałów celnych granicznych urzędu celno-skarbowego, dla komórek organizacyjnych urzędu celno-skarbowego zlokalizowanych w Białej Podlaskiej oraz komórek organizacyjnych Delegatur urzędu celno-skarbowego w Białej Podlaskiej i w Zamościu, w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;

- b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - c) administrowanie lokalnymi systemami informatycznymi w podległych jednostkach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo–programowej;
 - d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - e) wsparcie techniczne zadań związanych z informatyką śledczą;
 - f) administrowanie serwerowniami i sprzętem serwerowym;
 - g) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - h) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - i) zarządzanie na poziomie lokalnym kontami użytkowników w wybranych systemach i aplikacjach centralnych (zakładanie kont, nadawanie, modyfikacja, odbieranie uprawnień);
 - j) monitorowanie działania lokalnych i regionalnych granicznych systemów informatycznych, zgłaszanie i usuwanie awarii;
- 7) Do zadań **Czwartego Zespołu Wsparcia Informatycznego (RWS4LIW-4)** należy świadczenie usług informatycznych dla komórek organizacyjnych Lubelskiego Urzędu Celno-Skarbowego zlokalizowanych w Lublinie i w Zamościu oraz komórek organizacyjnych Delegatury Lubelskiego Urzędu Celno-Skarbowego w Lublinie, w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - b) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - c) administrowanie lokalnymi systemami informatycznymi w podległych jednostkach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo–programowej;

- d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - e) wsparcie techniczne zadań związanych z informatyką śledczą;
 - f) administrowanie serwerowniami i sprzętem serwerowym;
 - g) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - h) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - i) zarządzanie na poziomie lokalnym kontami użytkowników w wybranych systemach i aplikacjach centralnych (zakładanie kont, nadawanie, modyfikacja, odbieranie uprawnień);
- 8) Do zadań **Pierwszego Zespołu Systemów Centralnych – Centrum Kompetencyjne (RWS4LIIC-1)** należy, w szczególności:
- a) w ramach Centrum Kompetencyjnego wspierającego komórki Ministerstwa właściwe do spraw analiz, nadzoru nad kontrolami oraz poboru podatków w zakresie utrzymania i wsparcia technicznego w obszarze Repozytorium JPK, JPK Lunetka oraz Repozytorium e-Paragonów:
 - stanowienie centrum utrzymania i monitorowania ciągłości działania usługi JPK, JPK Lunetka oraz Centralnego Rejestru Kas (CRK), w tym:
 - - reagowanie na wykryte nieprawidłowości poprzez eliminowanie błędów i wspieranie w usuwaniu tych błędów dostawców usług,
 - - współpraca w aktualizacji dokumentacji technicznej i procedur,
 - - współpraca w rozwoju usług i produktów z nimi związanych,
 - - uczestnictwo w pracach zespołów resortowych, pracujących nad utrzymaniem i rozwojem ww. usług,
 - sugerowanie zmian zarówno w działaniu, jak i wykorzystywanych i udostępnianych przez Ministerstwo Finansów narzędziach w ramach ww. usług,
 - - współpraca w aktualizacji przyjętych rozwiązań informatycznych oraz ich zgodnością z obowiązującymi procedurami i wytycznymi,
 - - uczestnictwo w spotkaniach roboczych z dostawcami oprogramowania w zakresie utrzymania i rozwoju ww. usług,
 - świadczenie usługi II linii wsparcia technicznego w ramach Service Desk w obszarze JPK, JPK Lunetka oraz CRK dla pracowników Krajowej Administracji Skarbowej, podatników oraz podmiotów udostępniających rozwiązania informatyczne w tym zakresie,
 - stanowienie ośrodka wymiany doświadczeń oraz dobrych praktyk, w obszarze JPK, JPK Lunetka oraz CRK, w tym zgłaszanie postulatów zmian oraz propozycji nowych rozwiązań funkcjonalności systemów informatycznych, wykorzystywanych w ww. usługach,
 - a) wsparcie i nadzór nad działaniem usługi Repozytorium Jednolity Plik Kontrolny;
- 9) Do zadań **Zespołu Infrastruktury Sieciowej i Serwerowej, Wsparcia Informatycznego oraz Planowania i Logistyki Informatycznej (RWS4LIIS)** należy, w szczególności:
- a) administrowanie serwerowniami i sprzętem serwerowym;
 - b) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - c) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - d) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - e) planowanie rozwoju podległej infrastruktury informatycznej;
 - f) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Lublinie i jednostkach podległych;
 - g) udział w procesie realizacji procesu zakupów sprzętu komputerowego, usług i oprogramowania;

- h) realizacja procesu wsparcia użytkowników usług informatycznych w zakresie administrowanych systemów;
- i) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej w Lublinie w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami izby,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowej i programowej izby;
- j) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- k) wsparcie osób zarządzających oddziałem w zakresie obsługi biurowej.

5. Oddział Zarządzania Regionem Podkarpackim (RWS5):

- 1) do zadań **Zespołu Bezpieczeństwa Informatycznego (RWS5RIID)** należy w szczególności:
 - a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania,
 - b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - c) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania,
 - d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,
 - e) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
 - f) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Rzeszowie,
 - g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
 - h) obsługa zgłoszeń w systemach wsparcia użytkownika;

- 2) do zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RWS5RIIL)** należy w szczególności:
- a) w zakresie systemów lokalnych i bazy wiedzy:
 - przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,
 - współpraca z komórkami organizacyjnymi Izby i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
 - monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
 - rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
 - koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
 - prowadzenie dokumentacji usług informatycznych,
 - zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-ej linii wsparcia, regionalnie i lokalnie,
 - organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych,
 - obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych,
 - monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
 - zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,
 - obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
 - b) w zakresie systemów centralnych dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
 - wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - prowadzenie analiz systemowych dla usług informatycznych,
 - projektowanie usług informatycznych,
 - implementacja usług informatycznych,
 - weryfikowanie jakości dostarczanych usług informatycznych,
 - administrowanie techniczne komponentami usług informatycznych;
 - c) obsługa zgłoszeń w systemach wsparcia użytkownika;
- 3) do zadań **Zespołu Helpdesk (RWS5RIIH)** należy w szczególności:
- a) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami,
 - b) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,

- monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydemów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- c) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
- d) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
- e) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie i podległych urzędach,
- f) obsługa zgłoszeń w systemach wsparcia użytkownika;
- 4) do zadań **Pierwszego Zespołu Wsparcia Informatycznego (RWS5RIIW1)**, **Drugiego Zespołu Wsparcia Informatycznego (RWS5RIIW2)** oraz **Trzeciego Zespołu Wsparcia Informatycznego (RWS5RIIW3)** należy w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
- b) optymalizacja jakości świadczonych usług informatycznych, przez:
- monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- c) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
- utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
- d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
- e) obsługa zgłoszeń w systemach wsparcia użytkownika;
- 5) do zadań **Zespołu Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RWS5RIIS)** należy w szczególności:
- a) w zakresie infrastruktury sieciowej i serwerowej:
- administrowanie serwerowniami i sprzętem serwerowym,
 - administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - zarządzanie kopiami bezpieczeństwa,
- b) w zakresie wsparcia informatycznego:
- zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - optymalizacja jakości świadczonych usług informatycznych, przez:

- - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
 - - utrzymanie ciągłości działania systemów informatycznych,
 - - zapewnienie odpowiedniej wydajności systemów,
 - - instalowanie nowych wydań i poprawek,
 - - zarządzanie kontami użytkowników oraz uprawnieniami,
 - - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - c) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - d) obsługa zgłoszeń w systemach wsparcia użytkownika;
- 6) do zadań **Zespołu Planowania i Logistyki Informatycznej (RWS5RIIP)** należy w szczególności:
- a) planowanie rozwoju podległej infrastruktury informatycznej,
 - b) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie i podległych urzędach,
 - c) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
 - d) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
 - e) wsparcie osób zarządzających oddziałem w zakresie obsługi biurowej,
 - f) obsługa zgłoszeń w systemach wsparcia użytkownika.

§ 30.

Departament Zarządzania Regionem Północnym (RPN)

- I. Do zakresu zadań **Biura Wsparcia (RPN1BW)** należy, w szczególności:
- a) wsparcie osób zarządzających Departamentem Zarządzania Regionem w zakresie obsługi biurowej,
 - b) wsparcie w zapewnieniu dyscypliny pracy w podległych komórkach organizacyjnych,
 - c) wsparcie w skutecznym przepływie informacji wewnątrz regionu,
 - d) wsparcie w procesie planowania budżetu rzeczowo – finansowego regionu w zakresie właściwości podległych komórek organizacyjnych,
 - e) obsługa obiegu dowodów finansowo – księgowych dotyczących zakupów realizowanych na potrzeby podległych komórek organizacyjnych;
- II. **Oddział Zarządzania Regionem Kujawsko – Pomorskim (RPN2):**
1. Do zakresu zadań **Zespołu Bezpieczeństwa Informatycznego oraz Planowania i Logistyki Informatycznej (RPN2IID)** należy, w szczególności:
- a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania,
 - b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,

- c) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania,
- d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,
- e) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
- f) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Bydgoszczy,
- g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
- h) planowanie rozwoju podległej infrastruktury informatycznej,
- i) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w izbie i podległych urzędach,
- j) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
- k) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
- l) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowe;

2. Do zakresu zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RPN2III)** należy, w szczególności:

- a. przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,
- b. współpraca z komórkami organizacyjnymi izby i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
- c. monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
- d. rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
- e. koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
- f. prowadzenie dokumentacji usług informatycznych,
- g. zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-iej linii wsparcia, regionalnie i lokalnie,
- h. organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych,
- i. obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych,
- j. monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
- k. zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,

- l. obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
 - m. wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - n. prowadzenie analiz systemowych dla usług informatycznych,
 - o. projektowanie usług informatycznych,
 - p. implementacja usług informatycznych,
 - q. weryfikowanie jakości dostarczanych usług informatycznych,
 - r. administrowanie techniczne komponentami usług informatycznych,
 - s. zapewnienie wsparcia od strony informatycznej dla Centrum Kompetencyjnego Centralnego Rejestru Beneficjentów Rzeczywistych.
3. Do zakresu zadań **Zespołu Helpdesk (RPN2IIIH)** należy, w szczególności:
- 1) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Bydgoszczy i podległymi izbie urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami,
 - 2) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - 3) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
 - 4) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
 - 5) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w izbie i podległych urzędach;
4. Do zakresu zadań **Zespołu Infrastruktury Sieciowej i Serwerowej oraz Planowania i Logistyki Informatycznej (RPN2IIS)** należy, w szczególności:
- a. administrowanie serwerowniami i sprzętem serwerowym,
 - b. administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - c. utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - d. planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - e. zarządzanie kopiami bezpieczeństwa,
 - f. planowanie rozwoju podległej infrastruktury informatycznej,

- g. planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w izbie i podległych urzędach,
 - h. udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
 - i. efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
 - j. wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowe;
5. Do zakresu zadań **Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej oraz Planowania i Logistyki Informatycznej (RPN2IIP)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Bydgoszczy urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - 5) administrowanie serwerowniami i sprzętem serwerowym,
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - 9) zarządzanie kopiami bezpieczeństwa,
 - 10) planowanie rozwoju podległej infrastruktury informatycznej,
 - 11) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Bydgoszczy i podległych izbie urzędach,
 - 12) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
 - 13) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
 - 14) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowe;
6. Do zakresu zadań **Pierwszego Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej oraz Systemów Centralnych (RPN2IIW1)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,

- inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- 3) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej w Bydgoszczy i podległych izbie urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - 5) administrowanie serwerowniami i sprzętem serwerowym,
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - 9) zarządzanie kopiami bezpieczeństwa,
 - 10) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania,
 - 11) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - 12) prowadzenie analiz systemowych dla usług informatycznych,
 - 13) projektowanie usług informatycznych,
 - 14) implementacja usług informatycznych,
 - 15) weryfikowanie jakości dostarczanych usług informatycznych,
 - 16) administrowanie techniczne komponentami usług informatycznych.
7. Do zakresu zadań **Drugiego Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej oraz Systemów Centralnych (RPN2IIW2)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,

- inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- 3) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej w Bydgoszczy i podległych izbie urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - 5) administrowanie serwerowniami i sprzętem serwerowym,
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - 9) zarządzanie kopiami bezpieczeństwa,
 - 10) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - 11) implementacja usług informatycznych,
 - 12) weryfikowanie jakości dostarczanych usług informatycznych,
 - 13) administrowanie techniczne komponentami usług informatycznych.
8. Do zakresu zadań **Trzeciego Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RPN2IIW3)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - 3) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej w Bydgoszczy i podległych izbie urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - 5) administrowanie serwerowniami i sprzętem serwerowym,
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,

- 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - 9) zarządzanie kopiami bezpieczeństwa,
 - 10) zapewnienie wsparcia od strony informatycznej dla Centrum Kompetencyjnego Rozliczeń;
9. Do zakresu zadań **Czwartego Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RPN2IIW4)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - 3) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej w Bydgoszczy i podległych izbie urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - 5) administrowanie serwerowniami i sprzętem serwerowym,
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - 9) zarządzanie kopiami bezpieczeństwa;
10. Do zakresu zadań **Piątego Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RPN2IIW5)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - 3) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej w Bydgoszczy i podległych izbie urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,

- zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,
- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - 5) administrowanie serwerowniami i sprzętem serwerowym,
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - 9) zarządzanie kopiami bezpieczeństwa;

III. Oddział Zarządzania Regionem Pomorskim (RPN3)

1. Do zadań **Sekcji Bezpieczeństwa Informatycznego (RPN3IID)** należy, w szczególności:
 - 1) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - 2) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 3) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - a) instalowanie nowych wydań i poprawek systemu,
 - b) instalowanie kluczy licencyjnych,
 - c) zapewnienie sprawności technicznej systemu informatycznego,
 - d) zapewnienie odpowiedniej wydajności systemu,
 - e) administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - f) utrzymanie systemowej bazy uprawnień użytkowników,
 - g) zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - h) opracowanie procedur dotyczących administrowania systemem,
 - i) monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
 - 4) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia;
 - 5) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
 - 6) współpraca z Pierwszym Działem Bezpieczeństwa i Ochrony Informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Gdańsku;
 - 7) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji.
2. Do zadań **Zespołu Infrastruktury Sieciowej i Serwerowej (RPN3IIS)** należy, w szczególności:
 - 1) administrowanie serwerowniami i sprzętem serwerowym;
 - 2) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 3) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 4) planowanie rozbudowy i modyfikacji podległej infrastruktury;

- 5) zarządzanie kopiami bezpieczeństwa i administrowanie systemami pamięci masowych;
 - 6) zarządzanie kontami domeny i urządzeń sieciowych na poziomie lokalnych i regionalnym;
 - 7) administrowanie systemami informatycznymi na poziomie infrastruktury serwerowej, systemów operacyjnych w podległych jednostkach, w tym zarządzanie parametrami środowiskowymi serwerowni, warstwą serwerową, warstwą SO;
 - 8) dostarczanie usług z obszaru platformy wirtualizacji;
 - 9) udział w procesie realizacji procesu zakupów sprzętu komputerowego, usług i oprogramowania;
 - 10) udział w uruchamianiu i realizacji inicjatyw informatycznych w zakresie opiniowania i ustalania architektury rozwiązań;
 - 11) planowanie rozwoju i wdrażanie zmian środowisk serwerów aplikacji i oprogramowania, w szczególności poprzez prowadzenie analizy projektowania, testowania i implementacji nowych rozwiązań i technologii sieciowej;
 - 12) współpraca z usługodawcami zewnętrznymi w zakresie serwisu oraz dostaw oprogramowania;
 - 13) obsługa systemu wydruków centralnych;
 - 14) administrowanie systemami monitorującymi infrastrukturę teleinformatyczną;
 - 15) monitorowanie warunków środowiskowych węzłów teleinformatycznych.
3. Do zadań **Zespołu Systemów Centralnych, Lokalnych i Bazy Wiedzy (RPN3IIC)** należy, w szczególności:
- 1) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
 - a) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - b) prowadzenie analiz systemowych dla usług informatycznych,
 - c) projektowanie usług informatycznych,
 - d) implementacja usług informatycznych,
 - e) weryfikowanie jakości dostarczanych usług informatycznych,
 - f) administrowanie techniczne komponentami usług informatycznych;
 - 2) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
 - 3) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Gdańsku i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
 - 4) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
 - 5) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
 - 6) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
 - 7) prowadzenie dokumentacji usług informatycznych;
 - 8) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-ej linii wsparcia, regionalnie i lokalnie;
 - 9) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
 - 10) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
 - 11) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;

- 12) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy;
 - 13) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów.
4. Do zadań **Zespołu Helpdesk (RPN3IIIH)** należy, w szczególności:
- 1) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo, w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) informowanie użytkowników o stanie realizacji zgłoszenia,
 - e) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Gdańsku i podległymi urządzeniami oraz wykonawcami zewnętrznymi,
 - f) monitorowanie postępów prac nad zgłoszeniami;
 - 2) optymalizacja jakości świadczonych usług informatycznych przez:
 - a) utrzymywanie funkcji ServiceDesk,
 - b) monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - c) realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - d) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - 4) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
 - 5) określanie poza funkcjonalnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej w Gdańsku i podległych urządzeniach.
5. Do zadań **Pierwszego Zespołu Wsparcia Informatycznego (RPN3IIW1)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Gdańsku urządzeniach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,

- g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 5) obsługa wideokonferencji oraz obsługa systemów VoIP;
6. Do zadań **Drugiego Zespołu Wsparcia Informatycznego (RPN3IIW2)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) administrowanie lokalnymi systemami informatycznymi w podległych urządzeniach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
7. Do zadań **Zespołu Planowania i Logistyki Informatycznej (RPN3IIP)** należy, w szczególności:
- 1) planowanie rozwoju podległej infrastruktury informatycznej;
 - 2) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Gdańsku i podległych urządzeniach;
 - 3) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania;
 - 4) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
 - 5) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej.

IV. Oddział Zarządzania Regionem Warmińsko – Mazurskim (RPN4)

1. Do zadań **Sekcji Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPN4IID)** należy, w szczególności:
- 1) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - 2) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 3) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - a) instalowanie nowych wydań i poprawek systemu,
 - b) instalowanie kluczy licencyjnych,
 - c) zapewnienie sprawności technicznej systemu informatycznego,
 - d) zapewnienie odpowiedniej wydajności systemu,

- e) administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - f) utrzymanie systemowej bazy uprawnień użytkowników,
 - g) zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - h) opracowanie procedur dotyczących administrowania systemem,
 - i) monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
- 4) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia;
 - 5) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
 - 6) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Olsztynie;
 - 7) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji;
 - 8) administrowanie serwerowniami i sprzętem serwerowym;
 - 9) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 10) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 11) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - 12) zarządzanie kopiami bezpieczeństwa.
2. Do zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy, Helpdesk, Systemów Centralnych (RPN4IIL)** należy, w szczególności:
- 1) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
 - 2) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Olsztynie i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
 - 3) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
 - 4) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
 - 5) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
 - 6) prowadzenie dokumentacji usług informatycznych;
 - 7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-jej linii wsparcia, regionalnie i lokalnie;
 - 8) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
 - 9) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
 - 10) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;
 - 11) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy;
 - 12) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów;
 - 13) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,

- c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) informowanie użytkowników o stanie realizacji zgłoszenia,
 - e) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Olsztynie i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - f) monitorowanie postępów prac nad zgłoszeniami;
- 14) optymalizacja jakości świadczonych usług informatycznych przez:
- a) utrzymywanie funkcji ServiceDesk,
 - b) monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - c) realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - d) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 15) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
- 16) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
- 17) określanie pozafunkcjonalnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej w Olsztynie i podległych urzędach;
- 18) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
- a) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - b) prowadzenie analiz systemowych dla usług informatycznych,
 - c) projektowanie usług informatycznych,
 - d) implementacja usług informatycznych,
 - e) weryfikowanie jakości dostarczanych usług informatycznych,
 - f) administrowanie techniczne komponentami usług informatycznych;
- 19) realizowanie zadań scentralizowanych w zakresie utrzymania i rozwoju Systemu Ewidencja Kontroli (EWIKON).
3. Do zadań **Pierwszego (RPN4I IW1) i Drugiego (RPN4I IW2) Zespołu Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Olsztynie urzędach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;

- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 5) administrowanie serwerowniami i sprzętem serwerowym;
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - 9) zarządzanie kopiami bezpieczeństwa.
4. Do zadań **Trzeciego Zespołu Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPN4IIW3)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Olsztynie urządach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie i regionalnie;
 - 5) administrowanie serwerowniami i sprzętem serwerowym;
 - 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 8) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - 9) zarządzanie kopiami bezpieczeństwa;
 - 10) utrzymanie systemów granicznych, w tym:
 - a) utrzymanie systemu łączności VoIP,
 - b) administracja systemami bezpieczeństwa obiektów na przejściach granicznych,
 - c) opiniowanie projektów inwestycji oraz nadzór nad ich realizacją, w tym prowadzenie spraw z zakresu planowania i wykonywania inwestycji dotyczących przejść granicznych, ich modernizacji w zakresie informatyki, elektronicznych systemów ochrony obiektów i teletechniki,
 - d) prowadzenie pierwszej linii wsparcia systemów granicznych dla użytkowników regionu,
 - e) utrzymanie i administrowanie Systemów Odpraw Celnych (SOC) w ramach CAIFS 2 w Izbie,
 - f) wdrażanie systemów granicznych,
 - g) integrowanie systemów granicznych z innymi systemami,
 - h) wykonywanie czynności analitycznych zagadnień zgodnie ze specjalizacją w obszarze systemów granicznych;

- 11) administrowanie i zapewnienie ciągłości pracy systemów granicznych (SO).
5. Do zadań **Czwartego Zespołu Wsparcia Informatycznego, Planowania i Logistyki Informatycznej (RPN4IIW4)** należy, w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Olsztynie urządach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 5) planowanie rozwoju podległej infrastruktury informatycznej;
 - 6) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Olsztynie i podległych urządach;
 - 7) udział w realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania;
 - 8) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
 - 9) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej.

V. Oddział Zarządzania Regionem Zachodniopomorskim (RPN5)

1. Do zadań **Zespołu Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Planowania i Logistyki Informatycznej (RPN5IID)** należy:
- 1) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - 2) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 3) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;

- 4) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia;
- 5) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
- 6) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Szczecinie;
- 7) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji;
- 8) planowanie rozwoju podległej infrastruktury informatycznej;
- 9) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Szczecinie i podległych urządach;
- 10) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania;
- 11) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
- 12) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej;
- 13) administrowanie serwerowniami i sprzętem serwerowym na poziomie regionalnym;
- 14) planowanie rozbudowy i modyfikacji podległej infrastruktury serwerowej;
- 15) zarządzanie kopiami bezpieczeństwa;
- 16) nadzór nad zadaniami obsługi i weryfikacji na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych.

2. Do zadań **Zespołu Systemów Lokalnych i Bazy Wiedzy oraz Systemów Centralnych (RPN5IIL)** należy:

- 1) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
- 2) współpraca z komórkami organizacyjnymi Izby i podległymi urządami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
- 3) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
- 4) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
- 5) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
- 6) prowadzenie dokumentacji usług informatycznych;
- 7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-ej linii wsparcia, regionalnie i lokalnie;
- 8) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych w zakresie systemów lokalnych i Bazy Wiedzy;
- 9) wsparcie obsługi i weryfikacji na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
- 10) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;
- 11) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy;
- 12) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów, nie zastrzeżonych do realizacji w innych komórkach;
- 13) w zakresie systemów centralnych: dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
 - wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - prowadzenie analiz systemowych dla usług informatycznych,
 - projektowanie usług informatycznych,

- implementacja usług informatycznych,
- weryfikowanie jakości dostarczanych usług informatycznych,
- administrowanie techniczne komponentami usług informatycznych.

3. Do zadań **Sekcji Helpdesk (RPN5IIIH)** należy:

1) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:

- rejestrowanie i obsługa zgłoszeń od użytkowników,
- analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
- przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
- informowanie użytkowników o stanie realizacji zgłoszenia,
- identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Szczecinie i podległymi urzędami oraz wykonawcami zewnętrznymi,
- monitorowanie postępów prac nad zgłoszeniami;

2) optymalizacja jakości świadczonych usług informatycznych, poprzez:

- utrzymywanie funkcji ServiceDesk,
- monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
- realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
- inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;

3) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);

4) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;

5) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej w Szczecinie i podległych urzędach;

6) prowadzenie dokumentacji usług informatycznych;

7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-ej linii wsparcia, regionalnie i lokalnie.

4. Do zadań **Pierwszego (RPN5IIW1), Drugiego (RPN5IIW2) i Trzeciego (RPN5IIW3) Zespołu Wsparcia Informatycznego** należy:

1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;

2) optymalizacja jakości świadczonych usług informatycznych, przez:

- monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
- inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;

3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Szczecinie urzędach, w tym:

- utrzymanie ciągłości działania systemów informatycznych,
- zapewnienie odpowiedniej wydajności systemów,
- instalowanie nowych wydań i poprawek,
- zarządzanie kontami użytkowników oraz uprawnieniami,
- zarządzanie kopiami awaryjnymi systemów i bazy danych,

- przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej w podległych Izbie Administracji Skarbowej w Szczecinie jednostkach;
- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 5) współpraca z komórką bezpieczeństwa informatycznego, infrastruktury serwerowej oraz planowania i logistyki informatycznej w zakresie planowania rozwoju lokalnej infrastruktury oraz wydatków na rozwój i jej utrzymanie;
- 6) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów;
- 7) administrowanie serwerowniami i sprzętem serwerowym na poziomie lokalnym
5. Do zadań **Zespołu Systemów Centralnych (RPN5IIC)** należy: dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
- 1) wsparcie Centrum Kompetencyjnego Egzekucji Administracyjnej Izby Administracji Skarbowej w Szczecinie w zakresie: tworzenia, utrzymania i rozwijania narzędzi informatycznych wspomagających egzekucję,
 - 2) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych;
 - 3) prowadzenie analiz systemowych dla usług informatycznych;
 - 4) projektowanie usług informatycznych;
 - 5) implementacja usług informatycznych;
 - 6) weryfikowanie jakości dostarczanych usług informatycznych;
 - 7) administrowanie techniczne komponentami usług informatycznych.
6. Do zadań **Zespołu Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RPN5IIS)** należy:
- 1) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 2) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 3) planowanie rozbudowy i modyfikacji podległej infrastruktury sieciowej;
 - 4) zarządzanie kopiami bezpieczeństwa (w zakresie infrastruktury sieciowej);
 - 5) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 6) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 7) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Szczecinie urządzeniach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - 8) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;

- 9) współpraca z komórką bezpieczeństwa informatycznego, infrastruktury serwerowej, planowania i logistyki informatycznej w zakresie planowania rozwoju lokalnej infrastruktury oraz wydatków na rozwój i jej utrzymanie;
- 10) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów.

§ 31.

Departament Zarządzania Regionem Zachodnim (RZA)

I. Do zakresu zadań **Biura Wsparcia (RZA1BW)** należy, w szczególności:

- 1) wsparcie osób zarządzających departamentem zarządzania regionem w zakresie obsługi biurowej,
- 2) wsparcie w zapewnieniu dyscypliny pracy w podległych komórkach organizacyjnych,
- 3) wsparcie w skutecznym przepływie informacji wewnątrz regionu,
- 4) wsparcie w procesie planowania budżetu rzeczowo-finansowego regionu w zakresie właściwości podległych komórek organizacyjnych,
- 5) obsługa obiegu dowodów finansowo-księgowych dotyczących zakupów realizowanych na potrzeby podległych komórek organizacyjnych.

II. Oddział Zarządzania Regionem Wielkopolskim (RZA2)

1. Do zadań **Zespołu Planowania i Logistyki Informatycznej oraz Bezpieczeństwa Informatycznego (RZA2WIIP)** należy w szczególności:
 - 1) planowanie rozwoju podległej infrastruktury informatycznej;
 - 2) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Poznaniu i podległych urzędach;
 - 3) udział w realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania;
 - 4) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
 - 5) wsparcie osób zarządzających Pionem Informatyki w zakresie obsługi biurowej;
 - 6) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - 7) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 8) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - a) instalowanie nowych wydań i poprawek systemu,
 - b) instalowanie kluczy licencyjnych,
 - c) zapewnienie sprawności technicznej systemu informatycznego,
 - d) zapewnienie odpowiedniej wydajności systemu,
 - e) administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - f) utrzymanie systemowej bazy uprawnień użytkowników,
 - g) zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - h) opracowanie procedur dotyczących administrowania systemem,
 - i) monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
 - 9) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia;
 - 10) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
 - 11) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Poznaniu;

- 12) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji.
2. Do zadań **Zespołu Infrastruktury Sieciowej i Serwerowej (RZA2WIIS)** należy w szczególności:
 - 1) administrowanie serwerowniami i sprzętem serwerowym;
 - 2) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 3) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 4) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - 5) zarządzanie kopiami bezpieczeństwa.
3. Do zadań **Zespołu Helpdesk oraz Systemów Lokalnych i Bazy Wiedzy (RZA2WIIH)** należy w szczególności:
 - 1) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) informowanie użytkowników o stanie realizacji zgłoszenia,
 - e) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Poznaniu i podległymi Urzędami oraz wykonawcami zewnętrznymi,
 - f) monitorowanie postępów prac nad zgłoszeniami;
 - 2) optymalizacja jakości świadczonych usług informatycznych przez:
 - a) utrzymywanie funkcji ServiceDesk,
 - b) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - c) realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - d) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - 4) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
 - 5) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej w Poznaniu i podległych Urzędach;
 - 6) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
 - 7) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Poznaniu i podległymi Urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
 - 8) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
 - 9) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
 - 10) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
 - 11) prowadzenie dokumentacji usług informatycznych;

- 12) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-jej linii wsparcia, regionalnie i lokalnie;
- 13) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
- 14) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
- 15) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;
- 16) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy;
- 17) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów.

1) Do zadań **Pierwszego Zespołu Wsparcia Informatycznego (RZA2WIIW1)**, **Drugiego Zespół Wsparcia Informatycznego (RZA2WIIW2)**, **Trzeciego Zespół Wsparcia Informatycznego (RZA2WIIW3)**, **Czwartego Zespół Wsparcia Informatycznego (RZA2WIIW4)** i **Piątego Urzędach**, w tym:

- a) utrzymanie ciągłości działania systemów informatycznych,
- b) zapewnienie odpowiedniej wydajności systemów,
- c) instalowanie nowych wydań i poprawek,
- d) zarządzanie kontami użytkowników oraz uprawnieniami,
- e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
- f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
- g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;

2) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;

3) wsparcie techniczne zadań związanych z informatyką śledczą.

Piąty Zespół Wsparcia Informatycznego (RZA2WIIW5) wspiera Zespół Systemów Centralnych (RZA2WIIC) w wykonaniu realizacji scentralizowanego zadania budowy, administrowania i wsparcia dla ogólnopolskiego systemu informatycznego RAPEX umożliwiającego dostarczanie informacji dotyczących bezpieczeństwa produktów wprowadzanych na obszar celny UE oraz ogólnopolskiego systemu informatycznego P44 umożliwiającego dostarczanie informacji dotyczących obowiązujących dokumentów dla wypełnienia pola 44 SAD.

4. Do zadań **Zespołu Systemów Centralnych (RZA2WIIC)** należy w szczególności:

- 1) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
 - a) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - b) prowadzenie analiz systemowych dla usług informatycznych,
 - c) projektowanie usług informatycznych,
 - d) implementacja usług informatycznych,
 - e) weryfikowanie jakości dostarczanych usług informatycznych,
 - f) administrowanie techniczne komponentami usług informatycznych;
- 2) pełnienie roli Centrum Kompetencyjnego Systemu Hurtowni Danych (ARIADNA2), w tym:
 - a) wspieranie komórki Ministerstwa właściwej do spraw analiz w zakresie utrzymania i rozwoju Systemu Hurtowni Danych (ARIADNA2),
 - b) projektowanie i wdrażanie zmian w systemie,
 - c) prowadzenie bieżących działań analitycznych, w tym analiz obsługiwanych w systemach procesów oraz definiowanie wniosków dotyczących optymalizacji systemu,

- d) bieżąca parametryzacja eksploatowanego systemu,
 - e) projektowanie i opracowywanie koncepcji realizacji zmian biznesowych w systemie oraz rekomendowanie sposobu realizacji funkcjonalności w zakresie wymagań biznesowych,
 - f) współpraca z Komisją Europejską, DG Taxud w zakresie wpływu regulacji unijnych na system informatyczny oraz prowadzone projekty informatyczne,
 - g) budowanie i utrzymywanie szczegółowej mapy procesów w ramach domeny biznesowej,
 - h) przygotowanie scenariuszy testowych i planów testów, wykonywanie testów jednostkowych projektowanych systemów informatycznych, prowadzenie testów aplikacji, odbiorów oprogramowania,
 - i) przygotowywanie i przeprowadzanie szkoleń dla użytkowników systemu,
 - j) wsparcie w zakresie II-iej linii wsparcia dla użytkowników wewnętrznych oraz zewnętrznych (monitoring i obsługa incydentów, w tym na poziomie międzynarodowym);
- 3) realizacja zadań scentralizowanych w zakresie:
- a) budowy, administrowania i wsparcia dla ogólnopolskiego systemu informatycznego Centralny Rejestr Operacyjny CeRO,
 - b) budowy, administrowania i wsparcia dla ogólnopolskiego systemu informatycznego RAPEX umożliwiającego dostarczanie informacji dotyczących bezpieczeństwa produktów wprowadzanych na obszar celny UE oraz ogólnopolskiego systemu informatycznego P44 umożliwiającego dostarczanie informacji dotyczących obowiązujących dokumentów dla wypełnienia pola 44 SAD,
 - c) współpracy administracyjnej i integracyjnej w ramach HARF w zakresie ogólnopolskiej bazy danych uwierzytelniania i autoryzacji System Zdalnego Dostępu RSA.
5. Do zadań **Zespołu Wsparcia Rejestracji Obsługi Wniosków (RZA2WIIR)**, jako Centrum Kompetencyjnego wspierającego komórkę Ministerstwa właściwą do spraw ceł w zakresie utrzymania i rozwoju Systemu Zintegrowanej Rejestracji Przedsiębiorców i Obsługi Wniosków (SZPROT), należy w szczególności:
- 1) wsparcie właściciela biznesowego w zakresie utrzymania, rozwoju i wdrażania zmian w obszarze biznesowym rejestrowania użytkowników zewnętrznych (podmiotów gospodarczych, partnerów KAS) w domenie celnej i akcyzowej, w ramach systemów informatycznych Skarbowo-Celnych;
 - 2) wsparcie merytoryczne służb informatycznych resortu finansów w zakresie utrzymania, rozwoju i wdrażania rozwiązań informatycznych w obszarze rejestrowania użytkowników zewnętrznych (podmiotów gospodarczych, partnerów KAS) w domenie celnej i akcyzowej, w ramach systemów informatycznych Skarbowo-Celnych;
 - 3) współudział w projektowaniu rozwiązań biznesowych dotyczących rejestrowania użytkowników zewnętrznych (podmiotów gospodarczych, partnerów KAS) w domenie celnej i akcyzowej;
 - 4) prowadzenie bieżących działań analitycznych, w tym analiz obsługiwanych w systemach procesów oraz definiowanie wniosków dotyczących optymalizacji systemów i integracji danych;
 - 5) opracowywanie biznesowej koncepcji realizacji zmian w systemach informatycznych oraz rekomendowanie sposobu realizacji funkcjonalności w zakresie wymagań biznesowych;
 - 6) współudział w procesie wdrażania zmian w systemie SZPROT, w tym także testowanie systemów pod względem funkcjonalnym po wprowadzeniu zmian;
 - 7) analiza funkcjonalna systemu SZPROT oparta na:
 - a) przepisach prawnych i ich zmianach w zakresie merytorycznym realizowanym

- przez ten system,
- b) zmieniających się potrzebach biznesowych,
 - c) błędach zdiagnozowanych w trakcie ich eksploatacji zarówno na poziomie krajowym jak i międzynarodowym;
- 8) rekomendowanie właścicielowi biznesowemu kierunków rozwoju funkcjonalności systemu SZPROT (projektowanie nowych funkcjonalności biznesowych, uzgadnianie procesów oraz ich modyfikacja i opisywanie);
 - 9) nadzór nad aktualnością, kompletnością i jakością danych wprowadzanych do systemu SZPROT, a także monitorowanie terminowości wprowadzania danych;
 - 10) wsparcie właściciela biznesowego w budowaniu, rozbudowywaniu, pielęgnowaniu i publikowaniu mapy procesów w ramach domeny biznesowej w zakresie rejestrowania użytkowników zewnętrznych (podmiotów gospodarczych, partnerów KAS) w domenie celnej i akcyzowej;
 - 11) wsparcie właściciela biznesowego w tworzeniu, pielęgnowaniu, utrzymywaniu aktualności i publikowaniu modeli danych w ramach określonej domeny biznesowej w zakresie rejestrowania użytkowników zewnętrznych (podmiotów gospodarczych, partnerów KAS) w domenie celnej i akcyzowej;
 - 12) realizacja zadań drugiej linii wsparcia systemu SZPROT, wsparcie dla użytkowników wewnętrznych i zewnętrznych, organizacja i zarządzanie krajową komórką wsparcia, współpraca z innymi II Liniami Wsparcia Systemu Informacyjnego Skarbowo-Celnego, z III Linią Wsparcia, z wykonawcami umów na wsparcie systemów, w tym w szczególności:
 - a) sprawowanie merytorycznego nadzoru nad funkcjonowaniem pierwszej linii wsparcia Systemu Informacyjnego Skarbowo-Celnego,
 - b) świadczenie usług eksperckiego wsparcia w zakresie bieżących potrzeb użytkowników, udzielanie pomocy w zakresie wykraczającym poza dostępną bazę wiedzy i ustalone procedury, wymagające podjęcia działań analitycznych,
 - c) obsługa zgłoszeń od użytkowników,
 - d) bieżąca parametryzacja i konfiguracja w zakresie parametrów biznesowych,
 - e) zarządzanie kontami i uprawnieniami definiowanie w systemie ról biznesowych odpowiadających potrzebom użytkowników,
 - f) weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - g) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - h) informowanie użytkowników o stanie realizacji zgłoszenia,
 - i) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami wewnętrznymi, komórkami organizacyjnymi oraz wykonawcami zewnętrznymi,
 - j) monitorowanie postępów prac nad zgłoszeniami,
 - k) opracowywanie rozwiązań zastępczych dla problemów, dla których nie opracowano rozwiązań standardowych/informatycznych;
 - 13) udzielanie wsparcia dla struktur regionalnych zarządzania systemem SZPROT oraz udzielanie pomocy w zakresie wykraczającym poza dostępną bazę wiedzy i ustalone procedury, wymagającej podjęcia działań analitycznych oraz tworzenie nowych procedur;
 - 14) udział w przygotowywaniu planów i scenariuszy testowych oraz przeprowadzanie testów produktów, w szczególności wykonywanie testów funkcjonalnych, akceptacyjnych, testów gotowości operacyjnej;
 - 15) testowanie zmian funkcjonalnych systemu SZPROT, z uwzględnieniem zmian komponentów informatycznych współpracujących z tymi systemami w ramach Systemu Informacyjnego Skarbowo-Celnego;
 - 16) aktualizacja instrukcji dla użytkowników wewnętrznych (po stronie KAS) oraz dla

- podmiotów gospodarczych, składających dokumenty elektronicznie za pośrednictwem w/w systemów;
- 17) organizowanie i prowadzenie szkoleń i zajęć warsztatowych w obszarze wsparcia merytorycznego aplikacji, centralnych rozwiązań (zgodnie ze zgłaszanym zapotrzebowaniem użytkowników systemów na rzecz wszystkich izb administracji skarbowej) oraz cykliczne spotkania z trenerami, koordynatorami, liderami i administratorami biznesowymi zarządzanych systemów;
 - 18) współdziałanie w analizie wpływu regulacji prawnych, w tym unijnych na system SZPROT oraz prowadzone projekty;
 - 19) prowadzenie analizy danych w obszarze związanym z wykrywaniem przestępczości celno-skarbowej, w tym współpraca z innymi instytucjami (np. organami Policji, prokuratury, sądami, ABW), przekazywanie informacji na podstawie danych zawartych w systemie SZPROT;
 - 20) współdziałanie w procesie monitorowania działania rozwiązań i aplikacji wdrażanych centralnie w zakresie systemu SZPROT;
 - 21) współdziałanie w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - 22) współdziałanie w określaniu zasad utrzymania ciągłości działania dla systemów i procesów na możliwie najwyższym poziomie, związanych ze świadczeniem usług w tym wymagań biznesowych SLA;
 - 23) eskalowanie/alarmowanie przypadków niedotrzymania parametrów SLA dla systemu SZPROT;
 - 24) wsparcie właścicieli biznesowych w opracowywaniu w ramach postępowań o zamówienie publiczne projektów umów dotyczących rozwoju i utrzymania systemów w zakresie przygotowania opisów przedmiotów zamówienia, określania funkcjonalności systemów oraz wsparcie służb informatycznych resortu finansów i właścicieli biznesowych w nadzorze nad realizacją w/w umów;
 - 25) opracowywanie i aktualizacji dokumentacji bezpieczeństwa informacji w zakresie właściwych systemów oraz dokumentacji związanej z zasadami przetwarzania danych (w tym danych osobowych);
 - 26) przegląd i weryfikacja dokumentacji projektowej oraz powykonawczej systemów, aktualizowanej wraz z kolejnymi wersjami dostarczanych produktów;
 - 27) analiza i opiniowanie dokumentacji opracowanych na zlecenie właściciela biznesowego systemów oraz Komisji Europejskiej;
 - 28) reprezentowanie właściciela biznesowego na wskazanych przez niego spotkaniach, konferencjach, seminariach w kraju i zagranicą, w tym także udział w pracach zespołów powołanych przez Komisję Europejską.
- Do innych zadań **Zespołu Wsparcia Rejestracji Obsługi Wniosków (RZA2WIIR)** należy w szczególności:
- 1) administrowanie systemem SZPROT;
 - 2) utrzymanie i rozwój usługi e-Klient i e-Decyzje;
 - 3) współpraca z Departamentem Bezpieczeństwa MF w zakresie ochrony informacji przetwarzanych przez system SZPROT, w tym danych osobowych;
 - 4) współpraca z koordynatorami systemu SZPROT;
 - 5) przygotowywanie danych i opracowanie analiz w zakresie właściwości komórki.

III. Oddział Zarządzania Regionem Dolnośląskim (RZA3)

Wydział Systemów Centralnych i Lokalnych, Bazy Wiedzy, Help Desk, Bezpieczeństwa i Licencji oraz Infrastruktury Sieciowej i Serwerowej (RZA3IIT-1)

1. Zespół Bezpieczeństwa Informatycznego (RZA3DIID)

Do zadań komórki należy w szczególności:

- 1) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
- 2) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 3) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - a) instalowanie nowych wydań i poprawek systemu,
 - b) instalowanie kluczy licencyjnych,
 - c) zapewnienie sprawności technicznej systemu informatycznego,
 - d) zapewnienie odpowiedniej wydajności systemu,
 - e) administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - f) utrzymanie systemowej bazy uprawnień użytkowników,
 - g) zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - h) opracowanie procedur dotyczących administrowania systemem,
 - i) monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
- 4) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,
- 5) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
- 6) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej we Wrocławiu;
- 7) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji.

2. Zespół Systemów Lokalnych i Bazy Wiedzy oraz Help Desk (RZA3DIIL)

Do zadań komórki należy w szczególności:

- 1) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
- 2) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej we Wrocławiu i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
- 3) administrowanie i monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
- 4) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
- 5) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
- 6) prowadzenie dokumentacji usług informatycznych;
- 7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie;
- 8) obsługa i weryfikacja wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie administrowanych aplikacji;
- 9) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;
- 10) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów;
- 11) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy , w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) informowanie użytkowników o stanie realizacji zgłoszenia,

- e) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej we Wrocławiu i podległymi urzędami oraz wykonawcami zewnętrznymi,
- f) monitorowanie postępów prac nad zgłoszeniami;
- 12) optymalizacja jakości świadczonych usług informatycznych przez:
 - a) utrzymywanie funkcji ServiceDesk,
 - b) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - c) zarządzanie i monitorowanie uaktualniania Baz Wiedzy,
 - d) realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - e) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 13) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
- 14) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
- 15) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej we Wrocławiu i podległych urzędach;
- 16) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
- 17) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie;
- 18) udział w pozyskiwaniu danych z systemów eksploatowanych przez Izbę Administracji Skarbowej we Wrocławiu i w podległych urzędach.

3. Zespół Systemów Centralnych (RZA3DIIC)

Do zadań komórki należy w szczególności:

- 1) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS w tym:
 - a) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - b) prowadzenie analiz systemowych dla usług informatycznych,
 - c) projektowanie usług informatycznych,
 - d) implementacja usług informatycznych,
 - e) weryfikowanie jakości dostarczanych usług informatycznych,
 - f) administrowanie techniczne komponentami usług informatycznych,
 - g) udział w pracach rozwojowych i tworzenie oprogramowania w systemie WRO-SYSTEM oraz innych systemach wsparcia analizy i kontroli obszaru podatkowego;
- 2) utrzymania i administrowania Systemem Analizy Zgłoszeń Celnych ALINA;
- 3) wsparcie, utrzymanie i rozwijanie Systemu Ewidencja Outsourcing Ulgi, WRO-SYSTEM i innych aplikacji służących do obsługi Jednolitego Pliku Kontrolnego (JPK);
- 4) utrzymanie, administrowanie oraz wsparcie merytoryczne i techniczne Systemu Zarządzania Pojazdami i Kontroli Kosztów AutoManager;
- 5) utrzymanie oraz wsparcie merytoryczne i techniczne Systemu Elektronicznych Zamknięć Urzędowych i Systemu Wirtualizacji i Backupu (SWB);
- 5a) utrzymanie oraz wsparcie merytoryczne i techniczne Systemu Wirtualizacji i Backupu (SWB);
- 6) utrzymanie i rozwój modułu gromadzącego i przetwarzającego dane geolokalizacyjne SENT-GEO w ramach Systemu Elektronicznego Nadzoru Transportu (SENT);
- 7) współpraca z Instytutem Łączności w zakresie utrzymania i rozwoju systemów SENT-GEO oraz Systemu Elektronicznych Zamknięć Urzędowych;

- 8) współpraca z właściwymi departamentami MF w zakresie utrzymania i rozwoju Systemu Elektronicznych Zamknięć Urzędowych, Systemu Wirtualizacji i Backupu (SWB), Systemu Analizy Zgłoszeń Celnych ALINA oraz Systemu Międzynarodowej Pomocy Administracyjnej w Sprawach Celnych (SMPA) i Systemu Geoinfo;
- 9) kontrola urządzeń zawierających dane informatyczne oraz systemów informatycznych w zakresie prawidłowości użytkowania środków technicznych systemu monitorowania przewozów towarów;
- 10) współpraca z innymi jednostkami KAS, służbami i organami w zakresie przeciwdziałania i zwalczania przestępczości w zakresie systemu monitorowania przewozów towarów;
- 11) realizacja czynności nadzoru w ramach monitorowania wykorzystania plomb elektronicznych przez jednostki organizacyjne KAS;
- 12) udzielanie wsparcia merytorycznego i technicznego funkcjonariuszom pełniącym zadania kontrolne w systemie monitorowania przewozu towarów z zastosowaniem elektronicznych zamknięć urzędowych;
- 13) utrzymanie i rozwój Zintegrowanego Systemu Zarządzania Zasobami Ludzkimi (HERMES2);
- 14) utrzymanie i rozwój Centralnego i zintegrowanego systemu zarządzania uprawnieniami autoryzacyjnymi użytkowników wewnętrznych (SASISC);
- 15) wykonywanie zadań określonych dla Centrum w „Procedurze stosowania elektronicznego zamknięcia urzędowego w ramach systemu monitorowania drogowego przewozu towarów”;
- 16) utrzymania i rozwoju Systemu Zarządzania Organizacją KAS (SZOKAS).

4. Zespół Infrastruktury Sieciowej i Serwerowej (RZA3DIIS)

Do zadań komórki należy w szczególności:

- 1) administrowanie serwerowniami i sprzętem serwerowym;
- 2) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
- 3) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
- 4) planowanie rozbudowy i modyfikacji podległej infrastruktury;
- 5) zarządzanie kopiami bezpieczeństwa;
- 6) uczestnictwo w badaniu u przedsiębiorcy, warunków i kryteriów w związku z wnioskiem o przyznanie świadectwa upoważnionego przedsiębiorcy (AEO) i pozwolenia na stosowanie procedury uproszczonej oraz monitorowanie, czy spełniane są wymagane warunki i kryteria.

5. Sekcja Planowania i Logistyki Informatycznej (RZA3DIIP)

Do zadań komórki należy w szczególności:

- 1) planowanie rozwoju podległej infrastruktury informatycznej;
- 2) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej we Wrocławiu i podległych urzędach;
- 3) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania;
- 4) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
- 5) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej.

Wydział Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIT-2)

1. Pierwszy Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW1)

Do zadań komórki należy w szczególności:

- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 3) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej we Wrocławiu i podległych urzędach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 4) administrowanie serwerowniami i sprzętem serwerowym;
- 5) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
- 6) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 7) wsparcie techniczne zadań związanych z informatyką śledczą.

2. Drugi Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW2)

Do zadań komórki należy w szczególności:

- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 3) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 5) wsparcie techniczne zadań związanych z informatyką śledczą;
- 6) uczestnictwo w badaniu u przedsiębiorcy, warunków i kryteriów w związku z wnioskiem o przyznanie świadectwa upoważnionego przedsiębiorcy (AEO) i pozwolenia

na stosowanie procedury uproszczonej oraz monitorowanie, czy spełniane są wymagane warunki i kryteria;

7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie.

3. Trzeci Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW3)

Do zadań komórki należy w szczególności:

1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;

2) optymalizacja jakości świadczonych usług informatycznych, przez:

a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,

b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;

3) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:

a) utrzymanie ciągłości działania systemów informatycznych,

b) zapewnienie odpowiedniej wydajności systemów,

c) instalowanie nowych wydań i poprawek,

d) zarządzanie kontami użytkowników oraz uprawnieniami,

e) zarządzanie kopiami awaryjnymi systemów i bazy danych,

f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,

g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo–programowej;

4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;

5) wsparcie techniczne zadań związanych z informatyką śledczą;

6) uczestnictwo w badaniu u przedsiębiorcy, warunków i kryteriów w związku z wnioskiem o przyznanie świadectwa upoważnionego przedsiębiorcy (AEO) i pozwolenia na stosowanie procedury uproszczonej oraz monitorowanie, czy spełniane są wymagane warunki i kryteria;

7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie.

4. Czwarty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW4)

Do zadań komórki należy w szczególności:

1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;

2) optymalizacja jakości świadczonych usług informatycznych, przez:

a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,

b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;

3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej we Wrocławiu urzędach, w tym:

a) utrzymanie ciągłości działania systemów informatycznych,

b) zapewnienie odpowiedniej wydajności systemów,

c) instalowanie nowych wydań i poprawek,

d) zarządzanie kontami użytkowników oraz uprawnieniami,

- e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
- f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
- g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 5) wsparcie techniczne zadań związanych z informatyką śledczą;
- 6) uczestnictwo w badaniu u przedsiębiorcy, warunków i kryteriów w związku z wnioskiem o przyznanie świadectwa upoważnionego przedsiębiorcy (AEO) i pozwolenia na stosowanie procedury uproszczonej oraz monitorowanie, czy spełniane są wymagane warunki i kryteria;
- 7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-ej linii wsparcia, regionalnie i lokalnie.

5. Piąty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW5)

Do zadań komórki należy w szczególności:

- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej we Wrocławiu urządach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 5) wsparcie techniczne zadań związanych z informatyką śledczą;
- 6) uczestnictwo w badaniu u przedsiębiorcy, warunków i kryteriów w związku z wnioskiem o przyznanie świadectwa upoważnionego przedsiębiorcy (AEO) i pozwolenia na stosowanie procedury uproszczonej oraz monitorowanie, czy spełniane są wymagane warunki i kryteria;
- 7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-ej linii wsparcia, regionalnie i lokalnie.

6. Szósty Zespół Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA3DIIW6)

Do zadań komórki należy w szczególności:

- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- 2) optymalizacja jakości świadczonych usług informatycznych, przez:

- a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
- b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej we Wrocławiu urządach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 5) wsparcie techniczne zadań związanych z informatyką śledczą;
- 6) uczestnictwo w badaniu u przedsiębiorcy, warunków i kryteriów w związku z wnioskiem o przyznanie świadectwa upoważnionego przedsiębiorcy (AEO) i pozwolenia na stosowanie procedury uproszczonej oraz monitorowanie, czy spełniane są wymagane warunki i kryteria;
- 7) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie.

IV. Oddział Zarządzania Regionem Łódzkim (RZA4)

Do zadań **Zespołu Help Desk oraz Systemów Lokalnych i Bazy Wiedzy (RZA4LIH)** należy w szczególności:

- 1) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) informowanie użytkowników o stanie realizacji zgłoszenia,
 - e) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Łodzi i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - f) monitorowanie postępów prac nad zgłoszeniami;
- 2) optymalizacja jakości świadczonych usług informatycznych przez:
 - a) utrzymywanie funkcji ServiceDesk,
 - b) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - c) realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - d) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 3) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
- 4) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;

- 5) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej w Łodzi i podległych urzędach;
- 6) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych;
- 7) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Łodzi i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej;
- 8) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii;
- 9) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
- 10) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie;
- 11) prowadzenie dokumentacji usług informatycznych;
- 12) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-iej linii wsparcia, regionalnie i lokalnie;
- 13) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
- 14) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych;
- 15) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie;
- 16) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy;
- 17) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów;
- 18) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 19) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej.

Do zadań **Zespołu Planowania i Logistyki Informatycznej, Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RZA4LIIP)** należy w szczególności:

- 1) planowanie rozwoju podległej infrastruktury informatycznej;
- 2) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Łodzi i podległych urzędach;
- 3) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania;
- 4) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
- 5) administrowanie serwerowniami i sprzętem serwerowym;
- 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
- 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
- 8) planowanie rozbudowy i modyfikacji podległej infrastruktury;
- 9) zarządzanie kopiami bezpieczeństwa;
- 10) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- 11) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- 12) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Łodzi urzędach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,

- b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 13) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 14) zapewnienie wsparcia informatycznego dla Wydziału Centrum Kompetencyjne Usług Elektronicznych;
- 15) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Łodzi urzędach.

Do zadań **Zespołu Bezpieczeństwa Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RZA4LIID)** należy w szczególności:

- 1) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
- 2) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 3) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - a) instalowanie nowych wydań i poprawek systemu,
 - b) instalowanie kluczy licencyjnych,
 - c) zapewnienie sprawności technicznej systemu informatycznego,
 - d) zapewnienie odpowiedniej wydajności systemu,
 - e) administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - f) utrzymanie systemowej bazy uprawnień użytkowników,
 - g) zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - h) opracowanie procedur dotyczących administrowania systemem,
 - i) monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
- 4) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia;
- 5) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
- 6) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Łodzi;
- 7) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji;
- 8) administrowanie serwerowniami i sprzętem serwerowym;
- 9) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
- 10) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
- 11) planowanie rozbudowy i modyfikacji podległej infrastruktury;
- 12) zarządzanie kopiami bezpieczeństwa;
- 13) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;

- 14) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- 15) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 16) wsparcie techniczne zadań związanych z informatyką śledczą;
- 17) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Łodzi urzędach.

Do zadań **Pierwszego Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA4LIIW-1) i Drugiego Zespołu Wsparcia Informatycznego oraz Infrastruktury Sieciowej i Serwerowej (RZA4LIIW-2)** należy w szczególności:

- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Łodzi urzędach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- 5) administrowanie serwerowniami i sprzętem serwerowym;
- 6) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
- 7) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
- 8) planowanie rozbudowy i modyfikacji podległej infrastruktury;
- 9) zarządzanie kopiami bezpieczeństwa;

- 10) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Łodzi urzędach.

V. Oddział Zarządzania Regionem Lubuskim (RZA4)

- 1) w ramach **Pierwszego Zespołu Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej, Bezpieczeństwa Informatycznego, Systemów Lokalnych i Bazy Wiedzy, Helpdesk, Planowania i Logistyki Informatycznej** (RZA5FIIW-1) – zadania wykonywane dla Izby Administracji Skarbowej w Zielonej Górze:
- a) administrowanie warstwą aplikacyjną usług informatycznych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - udział w opracowaniu procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
 - b) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia we współpracy z Zespołem Bezpieczeństwa Informatycznego, Helpdesk, Infrastruktury Sieciowej i Serwerowej, Planowania i Logistyki Informatycznej,
 - c) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
 - d) wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
 - e) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,
 - f) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Zielonej Górze i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
 - g) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
 - h) rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
 - i) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
 - j) prowadzenie dokumentacji usług informatycznych,
 - k) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-jej linii wsparcia, regionalnie i lokalnie,
 - l) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych,
 - m) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji zarządzanych w ramach działu,
 - n) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,

- o) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,
- p) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
- r) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Zielonej Górze podległymi urządzeniami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami;
- s) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- t) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
- u) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
- w) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej w Zielonej Górze i podległych urządzeniach,
- y) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
- z) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- za) administrowanie lokalnymi systemami informatycznymi w Izbie Administracji Skarbowej w Zielonej Górze, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- zb) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
- zc) administrowanie serwerowniami i sprzętem serwerowym,
- zd) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,

- ze) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
- zf) zarządzanie kopiami bezpieczeństwa,
- zg) planowanie rozwoju podległej infrastruktury informatycznej,
- zh) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Zielonej Górze i podległych urzędach,
- zi) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
- zj) wsparcie osób zarządzających Oddziałem Zarządzania Regionem Lubuskim w zakresie obsługi biurowej,
- zk) realizacja zadań z zakresu IT, we współpracy z komórką Ministerstwa Finansów właściwą do spraw informatyzacji;

2) w ramach **Drugiego Zespołu Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej, Bezpieczeństwa Informatycznego, Systemów Lokalnych i Bazy Wiedzy, Helpdesk, Planowania i Logistyki Informatycznej (RZA5FIIW-2)** – zadania wykonywane dla urzędów skarbowych województwa lubuskiego i dla Lubuskiego Urzędu Celno-Skarbowego:

- a) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - udział w opracowaniu procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
- b) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia we współpracy z Zespołem Bezpieczeństwa Informatycznego, Helpdesk, Infrastruktury Sieciowej i Serwerowej, Planowania i Logistyki Informatycznej,
- c) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
- d) wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
- e) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,
- f) współpraca z komórkami organizacyjnymi Izby Administracji Skarbowej w Zielonej Górze i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
- g) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
- h) rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
- i) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
- j) prowadzenie dokumentacji usług informatycznych,
- k) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów

- informatycznych na poziomie II-jej linii wsparcia, regionalnie i lokalnie,
- l) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych,
 - m) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych,
 - n) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
 - o) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,
 - p) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
 - r) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Zielonej Górze i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami;
 - s) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - t) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
 - u) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
 - w) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w izbie i podległych urzędach,
 - y) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
 - z) optymalizacja jakości świadczonych usług informatycznych, przez:
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - za) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Zielonej Górze urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach

- bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - zb) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - zba) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Zielonej Górze urządach,
 - zc) wsparcie techniczne zadań związanych z informatyką śledczą,
 - zd) administrowanie serwerowniami i sprzętem serwerowym,
 - ze) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
 - zf) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
 - zg) zarządzanie kopiami bezpieczeństwa,
 - zh) planowanie rozwoju podległej infrastruktury informatycznej,
 - zi) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Zielonej Górze i podległych urządach,
 - zj) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
 - zk) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
 - zl) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej,
 - zm) realizacja zadań z zakresu IT, we współpracy z komórką Ministerstwa Finansów właściwą do spraw informatyzacji;
- 3) w ramach **Zespołu Systemów Centralnych, Systemów Lokalnych i Bazy Wiedzy, Bezpieczeństwa Informatycznego, Helpdesk, Infrastruktury Sieciowej i Serwerowej (RZA5FIIC)** – dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
- a) realizacja zadań scentralizowanych w zakresie utrzymania, administrowania i rozwoju systemów oraz usług centralnych i lokalnych,
 - b) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - c) prowadzenie analiz systemowych dla usług informatycznych,
 - d) projektowanie usług informatycznych,
 - e) implementacja usług informatycznych,
 - f) weryfikowanie jakości dostarczanych usług informatycznych,
 - g) administrowanie techniczne komponentami usług informatycznych,
 - h) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania,
 - i) udział w testach i odbiorach systemów informatycznych realizowanych regionalnie i centralnie,
 - j) udział w opracowaniu wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych w zakresie wdrożenia powierzonych do utrzymania systemów centralnych,
 - k) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
 - l) utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
 - m) rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
 - n) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II-ej linii wsparcia, regionalnie i lokalnie,
 - r) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji centralnych,
 - s) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,

- t) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Zielonej Górze i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami;
 - u) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - w) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
 - y) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
 - z) administrowanie serwerowniami i sprzętem serwerowym,
 - za) planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - zb) zarządzanie kopiami bezpieczeństwa,
 - zc) realizacja zadań z zakresu IT, we współpracy z komórką Ministerstwa Finansów właściwą do spraw informatyzacji;
- 4) w ramach **Zespołu Bezpieczeństwa Informatycznego, Helpdesk, Infrastruktury Sieciowej i Serwerowej, Planowania i Logistyki Informatycznej (RZA5FIID)** – realizowanie i koordynowanie działań związanych z zapewnieniem bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa w KAS, w tym:
- a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania w zakresie bezpieczeństwa teleinformatycznego,
 - b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
 - c) administrowanie warstwą aplikacyjną usług informatycznych w zakresie bezpieczeństwa teleinformatycznego oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - zarządzanie kluczami licencyjnymi,
 - wskazywanie środków i celów konfiguracyjnych zapewniających odpowiednią wydajności systemu,
 - administracja oprogramowaniem systemowym w regionie w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - administrowanie systemami i narzędziami bezpieczeństwa środowiska teleinformatycznego
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - udział w opracowaniu procedur dotyczących administrowania systemem,

- monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
- d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,
- e) udział w opracowywaniu dokumentacji związanej z bezpieczeństwem teleinformatycznym,
- f) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie wsparcia zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Zielonej Górze,
- g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
- h) obsługa incydentów bezpieczeństwa teleinformatycznego dotyczących systemów informatycznych oraz lokalnej infrastruktury teleinformatycznej,
- i) efektywne zarządzanie licencjami i nadzór nad ich wykorzystaniem,
- j) monitorowanie procesów przetwarzania informacji w systemach informatycznych, w kontekście bezpieczeństwa teleinformatycznego,
- k) udział w procesie realizacji procesu zakupów sprzętu komputerowego, usług i oprogramowania,
- l) realizacja zgłoszeń wsparcia użytkowników w zakresie zdarzeń i incydentów bezpieczeństwa teleinformatycznego na poziomie II-ej linii wsparcia,
- m) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi izby i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami;
- n) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- o) administrowanie serwerowniami i sprzętem serwerowym,
- p) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,
- r) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa,
- s) realizacja zadań z zakresu IT, we współpracy z komórką Ministerstwa Finansów właściwą do spraw informatyzacji.

§ 32.

Departament Zarządzania Regionem Południowym (RPD)

- I. Do zadań Biuro Wsparcia (RPD1BW) należy w szczególności:

- 1) wsparcie osób zarządzających departamentem zarządzania regionem w zakresie obsługi biurowej,
- 2) wsparcie w zapewnieniu dyscypliny pracy w podległych komórkach organizacyjnych
- 3) wsparcie w skutecznym przepływie informacji wewnątrz regionu
- 4) wsparcie w procesie planowania budżetu rzeczowo-finansowego regionu w zakresie właściwości podległych komórek organizacyjnych;
- 5) obsługa obiegu dowodów finansowo-księgowych dotyczących zakupów realizowanych na potrzeby podległych komórek organizacyjnych

II. Oddział Zarządzania Regionem Śląskim (RPD2)

1. Do zadań **Wydziału Helpdesk, Systemów Centralnych, Bezpieczeństwa, Programowania oraz Planowania i Logistyki Informatycznej (RPD2SIIHCDP)** należą sprawy realizowane przez:

- 1) Zespół Helpdesk oraz Systemów Lokalnych i Bazy Wiedzy (RPD2SIIHL) realizujący I linię wsparcia dla Izby Administracji Skarbowej w Katowicach i podległych jej jednostek organizacyjnych (dalej „IAS w Katowicach”) oraz II linię wsparcia aplikacyjnego, do którego zadań należy w szczególności:
 - a) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów , w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi w IAS w Katowicach oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami,
 - b) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
 - c) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
 - d) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
 - e) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w IAS w Katowicach,
 - f) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,
 - g) współpraca z komórkami organizacyjnymi w IAS w Katowicach w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
 - h) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,

- i) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
 - j) prowadzenie dokumentacji usług informatycznych,
 - k) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II linii wsparcia, regionalnie i lokalnie,
 - l) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych,
 - m) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych,
 - n) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
 - o) zarządzanie i monitorowanie uaktualnienia Bazy Wiedzy;
- 2) Zespół **do Spraw** Programowania (RPD2SIIPR), do którego zadań należy w szczególności:
- a) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
 - b) współpraca w zakresie realizacji projektów centralnych w obszarze budowy oraz modernizacji oprogramowania,
 - c) tworzenie aplikacji regionalnych wraz z ich utrzymaniem, dostosowaniem do wymagań prawnych,
 - d) rozwój systemów lokalnych i regionalnych i ich wersjonowanie;
- 3) Zespół Systemów Centralnych (RPD2SIIC), do którego zadań należy w szczególności:
- a) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
 - wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - prowadzenie analiz systemowych dla usług informatycznych,
 - projektowanie usług informatycznych,
 - implementacja usług informatycznych,
 - weryfikowanie jakości dostarczanych usług informatycznych,
 - administrowanie techniczne komponentami usług informatycznych,
 - b) w zakresie administrowania i utrzymania systemów SSP i SZD, w szczególności:
 - aktualizacja dokumentów opisujących standardy i procesy związane z utrzymaniem i aktualizacją oprogramowania,
 - wykonywanie czynności administracyjnych na wszystkich środowiskach,
 - aktualizacja oprogramowania aplikacyjnego (wgrywanie poprawek) na środowiskach testowym i produkcyjnym zgodnie z przyjętymi standardami,
 - kontrolowanie czasu przetwarzania i liczby deklaracji wprowadzanych do systemu,
 - wykonywanie zleconych zapytań SQL na bazach danych środowisk,
 - współpraca z innymi administratorami Resortu Finansów oraz zespołami Wykonawców zewnętrznych w zakresie zapewnienia działania usług i rozwiązywania incydentów,
 - monitorowanie realizacji działań utrzymaniowych i administracyjnych zgodnie z obowiązującymi SLA dla każdej z usług,
 - weryfikacja planów wdrożenia nowych lub modyfikowanych usług oraz uczestnictwo we wdrożeniach,

- przeprowadzanie przeglądów jakości i odbiorów dotyczących obszaru działania, w tym Pakietu Kodów Źródłowych, Pakietu instalacyjnego oraz Dokumentacji,
 - udział w testach akceptacyjnych nowych i poprawionych wersji usług,
 - pozyskiwanie wiedzy technicznej z zakresu wdrożonych i wdrażanych usług,
 - raportowanie zidentyfikowanych ryzyk i zagadnień z obszaru utrzymania i administracji,
- c) realizacja zadań administracyjnych i utrzymaniowych w zakresie usług:
- Twój e-PIT,
 - e-Urząd,
 - e-Podatki (SSP, Konto podatnika - Portal Podatkowy, PUE),
- d) instalowanie nowych wydań i poprawek oraz wykonywanie kopii zabezpieczających na serwerach systemów centralnych,
- e) wykonywanie obowiązków służbowych w systemie całodobowym w sytuacjach tego wymagających, zgodnie z opracowanym przez kierującego zespołem harmonogramem pracy;
- 4) Sekcja **do Spraw** Bezpieczeństwa Informatycznego (RPD2SIID), do którego zadań należy w szczególności:
- a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania,
- b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
- c) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
- instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania,
- d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,
- e) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
- f) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w IAS w Katowicach,
- g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji;
- 5) Sekcja **do Spraw** Planowania i Logistyki Informatycznej (RPD2SIIP), do której zadań należy w szczególności:
- a) planowanie rozwoju podległej infrastruktury informatycznej,
- b) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w IAS w Katowicach,
- c) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
- d) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,

- e) wsparcie osób zarządzających Regionem Śląskim w zakresie obsługi biurowej,
 - f) realizacja zadań związanych z koordynacją procedowania wniosków budżetowych i zakupowych z obszaru informatycznego Resortu Finansów, w zakresie:
 - koordynacji przebiegu wniosków dotyczących zwiększenia budżetu IT na zakup środków trwałych lub usług z katalogu wydatków IT oraz zmiany ich przeznaczenia,
 - koordynacji wniosków o zgody na wydatkowanie kwot budżetowych w ramach progów ustalanych przez Centrum,
 - koordynacji przebiegu informacji o planowanych postępowaniach zakupowych powyżej progów kwotowych ustalanych przez Centrum,
 - prowadzenia rejestru obsługiwanych wniosków z możliwością ich monitorowania oraz raportowania,
 - opracowywania wniosków rekomendacyjnych dla Centrum.
2. Do zadań Pierwszego Zespołu Wsparcia Informatycznego (RPD2SIIW-01), Drugiego Zespołu Wsparcia Informatycznego (RPD2SIIW-02), Trzeciego Zespołu Wsparcia Informatycznego (RPD2SIIW-03), Czwartego Zespołu Wsparcia Informatycznego (RPD2SIIW-04) oraz Piątego Zespołu Wsparcia Informatycznego (RPD2SIIW-05), z zastrzeżeniem ust.3-7, należy w szczególności:
- 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydentem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Katowicach jednostek organizacyjnych, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek oraz wykonywanie kopii bezpieczeństwa, z wyłączeniem tych działań na serwerach systemów centralnych,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 5) wsparcie techniczne zadań związanych z informatyką śledczą;
 - 6) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Katowicach urzędach.
3. Pierwszy Zespół Wsparcia Informatycznego (RPD2SIIW-01), realizuje zadania wymienione w ust. 2 w lokalizacjach: I US w Bielsku-Białej, II US w Bielsku-Białej, US w Cieszynie, US w Czechowicach-Dziedzicach, US w Pszczynie, US w Żywcu, II Śląskiego US w Bielsku-Białej, Oddziału Celnego w Żywcu, Izby i UCS w Cieszynie, UCS w Chotěbuz, budynku UCS w Bielsku Białej przy ul. Regera 32 i Traugutta 2a, Oddziału Celnego w Czechowicach – Dziedzicach.

4. Drugi Zespół Wsparcia Informatycznego (RPD2SIIW-02), realizuje zadania wymienione w ust. 2 w lokalizacjach: US w Będzinie, US w Dąbrowie Górniczej, US w Jaworznie, I US w Katowicach, US w Mysłowicach, US w Sosnowcu, I Śląskiego US w Sosnowcu, Oddziału Celnego w Sławkowie.
5. Trzeci Zespół Wsparcia Informatycznego (RPD2SIIW-03), realizuje zadania wymienione w ust. 2 w lokalizacjach: US w Bytomiu, US w Chorzowie, I US w Gliwicach, II US Gliwicach, US w Piekarach Śląskich, US w Rudzie Śląskiej, US w Siemianowicach Śląskich, US w Tarnowskich Górach, US w Zabrze, Oddziału Celnego w Chorzowie, Oddziału Celnego w Gliwicach, Oddziału Celnego Poczтового w Zabrze.
6. Czwarty Zespół Wsparcia Informatycznego (RPD2SIIW-04), realizuje zadania wymienione w ust. 2 w lokalizacjach: I US w Częstochowie, II US w Częstochowie, US w Kłobucku, US w Lublińcu, US w Myszkowie, US w Zawierciu, budynku UCS w Częstochowie przy ul. Rejtana 9 i Rydza-Śmigłego 26, Oddziału Celnego w Częstochowie oraz w budynku Izby w Częstochowie przy ul. Rejtana 9.
7. Piąty Zespół Wsparcia Informatycznego (RPD2SIIW-05), realizuje zadania wymienione w ust. 2 w lokalizacjach: US w Jastrzębiu Zdroju, US w Mikołowie, US w Raciborzu, US w Rybniku, US w Tychach, US w Wodzisławiu Śląskim, US w Żorach, Oddziału Celnego w Raciborzu, Oddziału Celnego w Tychach, budynku UCS w Rybniku przy ul. Kłokocińska 51.
8. Zespoły Wsparcia Informatycznego świadczą wsparcie informatyczne dla pracowników innych jednostek Ministerstwa, realizujących zadania w lokalizacjach wymienionych w ust. 3-7, chyba że przepisy szczególne stanowią inaczej.
9. Do zadań Zespołu Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RPD2SIISW), należy w szczególności:
 - 1) administrowanie serwerowniami i sprzętem serwerowym;
 - 2) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 3) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 4) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - 5) zarządzanie kopiami bezpieczeństwa;
 - 6) wykonywanie czynności wymienionych w ust.2.
10. Zespół Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RPD2SIISW) realizuje:
 - 1) zadania wymienione w ust. 2 pkt 1 – 5 w IAS w Katowicach;
 - 2) zadania wymienione w ust.2 pkt 6 w lokalizacjach: głównej siedziby IAS w Katowicach przy ul. Damrota 25, budynku IAS/UCS w Katowicach przy ul. Paderewskiego 32b, głównej siedziby UCS w Katowicach przy ul. Słonecznej 34, budynku UCS w Katowicach przy ul. Plac Grunwaldzki 8-10, Oddziałów Celnych w Pyrzowicach.
11. Zespół Infrastruktury Sieciowej i Serwerowej oraz Wsparcia Informatycznego (RPD2SIISW) świadczy wsparcie informatyczne dla pracowników innych jednostek Ministerstwa, realizujących zadania we wskazanych w ust.10 pkt 2 lokalizacjach, chyba że przepisy szczególne stanowią inaczej.

III. Oddział Zarządzania Regionem Opolskim (RPD3)

- 1) do zadań **Zespołu Bezpieczeństwa Informatycznego, Systemów Centralnych, Lokalnych i Bazy Wiedzy, Planowania i Logistyki Informatycznej oraz Helpdesk (RPD3OILL)** należy, w szczególności:
 - a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie,

- regionalnie i centralnie;
- c) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - instalowanie nowych wydań i poprawek systemu,
 - instalowanie kluczy licencyjnych,
 - zapewnienie sprawności technicznej systemu informatycznego,
 - zapewnienie odpowiedniej wydajności systemu,
 - administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - utrzymanie systemowej bazy uprawnień użytkowników,
 - zarządzanie kopiami awaryjnymi systemu i bazy danych,
 - opracowanie procedur dotyczących administrowania systemem,
 - monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania,
 - d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,
 - e) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,
 - f) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Katowicach,
 - g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,
 - h) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,
 - i) współpraca z komórkami organizacyjnymi Izby i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
 - j) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
 - k) rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
 - l) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
 - m) prowadzenie dokumentacji usług informatycznych,
 - n) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie,
 - o) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych,
 - p) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych,
 - r) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
 - s) zarządzanie i monitorowanie uaktualnieniami Baz Wiedzy,
 - t) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
 - u) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,

- informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izbie Administracji Skarbowej w Katowicach i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami;
- w) optymalizacja jakości świadczonych usług informatycznych przez:
- utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- y) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
- z) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
- za) określanie poza funkcjonalnych wymagań dla lokalnych systemów informatycznych w Izbie i podległych urzędach) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
- wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - prowadzenie analiz systemowych dla usług informatycznych,
 - projektowanie usług informatycznych,
 - implementacja usług informatycznych,
 - weryfikowanie jakości dostarczanych usług informatycznych,
 - administrowanie techniczne komponentami usług informatycznych,
- zb) planowanie rozwoju podległej infrastruktury informatycznej,
- zc) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie i podległych urzędach,
- zd) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
- ze) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
- zf) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej;
- 2) do zadań **Pierwszego Zespołu Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej (RPD3OIIW-1)** należy, w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- b) optymalizacja jakości świadczonych usług informatycznych, przez:
- monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- c) administrowanie lokalnymi systemami informatycznymi w podległych urzędach, w tym:
- utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,

- przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- e) wsparcie techniczne zadań związanych z informatyką śledczą;
- f) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Katowicach urządach;
- g) administrowanie serwerowniami i sprzętem serwerowym;
- h) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
- i) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
- j) planowanie rozbudowy i modyfikacji podległej infrastruktury;
- k) zarządzanie kopiami bezpieczeństwa.
- 3) do zadań **Drugiego Zespołu Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej** (RPD3OIIW-2) należy, w szczególności:
- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
- b) optymalizacja jakości świadczonych usług informatycznych, przez:
- monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- c) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Katowicach urządach, w tym:
- utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
- d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
- e) wsparcie techniczne zadań związanych z informatyką śledczą;
- f) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Katowicach urządach;
- g) administrowanie serwerowniami i sprzętem serwerowym;
- h) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
- i) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
- j) planowanie rozbudowy i modyfikacji podległej infrastruktury;
- k) zarządzanie kopiami bezpieczeństwa.

IV. Oddział Zarządzania Regionem Małopolskim (RPD4)

1. W ramach Wydziału Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Bezpieczeństwa Informatycznego, Planowania i Logistyki Informatycznej (RPD4IIW) do zadań Pierwszego (RPD4IIW-1), Drugiego (RPD4IIW-2), Trzeciego (RPD4IIW-3), Czwartego (RPD4IIW-4) i Piątego (RPD4IIW-5) Zespołu Wsparcia Informatycznego, Infrastruktury Sieciowej i Serwerowej oraz Bezpieczeństwa Informatycznego, Planowania i Logistyki Informatycznej należy, w szczególności:
 - 1) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych;
 - 2) optymalizacja jakości świadczonych usług informatycznych, przez:
 - a) monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) administrowanie lokalnymi systemami informatycznymi w urzędach, w tym:
 - a) utrzymanie ciągłości działania systemów informatycznych,
 - b) zapewnienie odpowiedniej wydajności systemów,
 - c) instalowanie nowych wydań i poprawek,
 - d) zarządzanie kontami użytkowników oraz uprawnieniami,
 - e) zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - f) przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - g) monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej;
 - 4) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie;
 - 5) wsparcie techniczne zadań związanych z informatyką śledczą;
 - 6) administrowanie serwerowniami i sprzętem serwerowym;
 - 7) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi;
 - 8) utrzymywanie infrastruktury sieciowej zgodnie z zasadami i standardami bezpieczeństwa;
 - 9) planowanie rozbudowy i modyfikacji podległej infrastruktury;
 - 10) zarządzanie kopiami bezpieczeństwa;
 - 11) planowanie rozwoju podległej infrastruktury informatycznej;
 - 12) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Krakowie i w urzędach;
 - 13) udział w procesie realizacji procesu zakupów sprzętu komputerowego, usług i oprogramowania;
 - 14) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami;
 - 15) wsparcie osób zarządzającym pionem informatyki w zakresie obsługi biurowej;
 - 16) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania;
 - 17) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:
 - a) instalowanie nowych wydań i poprawek systemu,
 - b) instalowanie kluczy licencyjnych,
 - c) zapewnienie sprawności technicznej systemu informatycznego,
 - d) zapewnienie odpowiedniej wydajności systemu,
 - e) administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
 - f) utrzymanie systemowej bazy uprawnień użytkowników,
 - g) zarządzanie kopiami awaryjnymi systemu i bazy danych,

- h) opracowanie procedur dotyczących administrowania systemem,
 - i) monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania;
- 18) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia;
 - 19) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
 - 20) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Krakowie;
 - 21) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji.
2. Do zadań Zespołu Systemów Centralnych (RPD4IIC) należy, w szczególności:
- 1) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych i centralnych systemów informatycznych;
 - a) wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - b) prowadzenie analiz systemowych dla usług informatycznych,
 - c) projektowanie usług informatycznych,
 - d) implementacja usług informatycznych,
 - e) weryfikowanie jakości dostarczanych usług informatycznych,
 - f) administrowanie techniczne komponentami usług informatycznych;
 - 2) realizacja zawartych umów w zakresie zarządzanych centralnych systemów informatycznych zgodnie z pełnionymi rolami;
 - 3) monitorowanie działania i kontrola poprawności pracy centralnych systemów i aplikacji;
 - 4) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych w ramach zarządzanych centralnych systemów informatycznych;
 - 5) zarządzanie procesami wsparcia użytkowników w zakresie obsługi centralnych systemów informatycznych na poziomie II-jej linii wsparcia w tym:
 - a) świadczenie usług eksperckiego wsparcia w zakresie bieżących potrzeb użytkowników zarządzanych systemów, w tym udzielanie pomocy w zakresie wykraczającym poza dostępną bazę wiedzy i ustalone procedury, wymagające podjęcia działań analitycznych,
 - b) obsługa zgłoszeń od użytkowników,
 - c) weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - d) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - e) informowanie użytkowników o stanie realizacji zgłoszenia,
 - f) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami wewnętrznymi, komórkami organizacyjnymi oraz wykonawcami zewnętrznymi,
 - g) monitorowanie postępów prac nad zgłoszeniami,
 - h) aktualizacja instrukcji dla użytkowników wewnętrznych (po stronie KAS) oraz dla podmiotów gospodarczych, składających dokumenty elektronicznie za pośrednictwem centralnych systemów informatycznych;
 - 6) optymalizacja jakości świadczonych usług informatycznych, poprzez:
 - a) monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - b) inicjowanie i prowadzenie działań mających na celu podniesienie wydajności i stabilności centralnych systemów informatycznych,

- c) zarządzanie i monitorowanie uaktualniania Baz Wiedzy,
 - d) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
- 7) prowadzenie szkoleń w obszarze aplikacji, systemów informatycznych i obsługi urządzeń komputerowych oraz cykliczne spotkania z trenerami, koordynatorami, liderami i administratorami zarządzanych systemów informatycznych;
 - 8) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - 9) projektowanie nowych funkcjonalności biznesowych, uzgadnianie procesów oraz ich modyfikacja i opisywanie;
 - 10) prowadzenie analizy danych w obszarze związanym z wykrywaniem przestępczości celno-skarbowej, w tym współpraca z organami policji, prokuratury, sądami, ABW, przekazywanie informacji na podstawie danych zawartych w centralnych systemach informatycznych;
 - 11) zarządzanie komponentami środowiska produkcyjnego i testowego centralnych systemów informatycznych poprzez:
 - a) techniczne utrzymywanie i administrowanie centralnymi systemami,
 - b) opracowywanie i wdrażanie czynności administracyjnych dla centralnych systemów przywozu i wywozu dla potrzeb warstwy centralnej i lokalnej,
 - c) koordynowanie zadań związanych z utrzymaniem i administrowaniem centralnymi systemami w izbach administracji skarbowej,
 - d) monitorowanie poprawności działania systemów centralnych systemów,
 - e) obsługa administracyjna i zarządzanie konfiguracją;
 - 12) organizowanie i obsługiwanie wsparcia technicznego dla ogólnopolskich użytkowników centralnych systemów na poziomie eksperckim;
 - 13) monitorowanie spójności w implementacji centralnych systemów we wszystkich jednostkach organizacyjnych KAS;
 - 14) zapewnienie ciągłości działania systemów informatycznych w zakresie administrowania merytorycznego poprzez ustalenie zasad bezpieczeństwa i ciągłości działania SLA systemów;
 - 15) monitorowanie i analizowanie wartości parametrów SLA dla systemów informatycznych obsługiwanych w komórce;
 - 16) eskalowanie/alarmowanie przypadków niedotrzymania parametrów SLA dla centralnych systemów informatycznych;
 - 17) przygotowywanie planów i scenariuszy testowych, środowiska testowego oraz przeprowadzanie testów produktów w szczególności wykonywanie testów jednostkowych i integracyjnych zarządzanych systemów;
 - 18) przygotowywanie danych, procedur, wytycznych, opracowań i analiz dla potrzeb i na zlecenie Kierownictwa KAS, IAS, Ministerstwa Finansów oraz innych instytucji upoważnionych, w oparciu o dostępne bazy danych;
 - 19) budowa procedur, zasad i postanowień dotyczących polityki bezpieczeństwa centralnych systemów, ich realizacja oraz nadzór nad ich przestrzeganiem;
 - 20) opracowywanie dokumentacji i udział w postępowaniach przetargowych dotyczących zakupów usług, oprogramowania itp. dla potrzeb centralnych systemów informatycznych obsługiwanych w komórce;
 - 21) obsługa administracyjna i zarządzanie konfiguracją zarządzanych centralnych systemów informatycznych;
 - 22) utrzymywanie technicznego środowiska analitycznego centralnych systemów;
 - 23) utrzymywanie technicznego środowiska Centrum CBT;
 - 24) utrzymywanie archiwalnych baz danych w obszarze danych rozrachunkowych;

- 25) analizowanie i przedkładanie potrzeb oraz zagrożeń związanych z rozwojem bazy sprzętowej, sieci teleinformatycznej i zakupów gotowego oprogramowania dla potrzeb utrzymania centralnych systemów informatycznych;
 - 26) identyfikowanie potrzeb w zakresie zarządzanych systemów oraz przygotowanie założeń do Planu Budżetu;
 - 27) projektowanie, budowa i wdrażanie autorskich systemów dedykowanych dla potrzeb zarządzania, monitoringu i sprawowania kontroli w obszarze technicznej eksploatacji systemów, w tym prowadzenie prac programistycznych i implementacyjnych;
 - 28) wytwarzanie dokumentacji w tym projektowej oraz wdrożeniowej i powykonawczej;
 - 29) udział w reagowaniu kryzysowym i realizacja zadań wynikających z planu zarządzania kryzysowego.
3. Do zadań Zespołu Helpdesk, Systemów Lokalnych i Bazy Wiedzy (RPD4IIH) należy, w szczególności:
- 1) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo Finansów, w tym:
 - a) rejestrowanie i obsługa zgłoszeń od użytkowników,
 - b) analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - c) przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - d) informowanie użytkowników o stanie realizacji zgłoszenia,
 - e) identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami wewnętrznymi, komórkami organizacyjnymi oraz wykonawcami zewnętrznymi,
 - f) monitorowanie postępów prac nad zgłoszeniami;
 - 2) optymalizacja jakości świadczonych usług informatycznych, poprzez:
 - a) utrzymywanie funkcji Servicedesk,
 - b) monitorowanie procesów: zarządzanie incydemem, zarządzanie wnioskami i zarządzanie problemem,
 - c) realizacja i publikacja raportów z obsługi w Servicedesk zgłoszeń, incydentów, wniosków,
 - d) inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego;
 - 3) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement);
 - 4) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych;
 - 5) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie Administracji Skarbowej w Krakowie i urzędach;
 - 6) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
 - 7) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikacje lub odebranie uprawnień użytkowników użytkownikom w zakresie aplikacji centralnych,
 - 8) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych;
 - 9) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,

- a) współpraca z komórkami organizacyjnymi w Izbie Administracji Skarbowej w Krakowie i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
- b) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
- c) gromadzenie dokumentacji usług informatycznych,
- d) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych realizowanych na poziomie II-iej linii wsparcia, regionalnie i lokalnie,
- e) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
- f) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,
- g) obsługa organizacyjna zamówień na informacje/zestawienia/raporty z systemów informatycznych.

V. Oddział Zarządzania Regionem Świętokrzyskim (RPD5)

1) Do zadań **Pierwszego Zespołu Wsparcia Informatycznego** (RPD5TIIW-1)

należy:

- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
- b) optymalizacja jakości świadczonych usług informatycznych przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,
- c) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Kielcach urzędach, w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - zapewnienie odpowiedniej wydajności systemów,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
 - monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo–programowej,
- d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,
- e) wsparcie techniczne zadań związanych z informatyką śledczą,
- f) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Kielcach urzędach;

2) Do zadań **Drugiego Zespołu Wsparcia Informatycznego** (RPD5TIIW-2) należy:

- a) zarządzanie i realizacja procesu bezpośredniego wsparcia użytkowników usług informatycznych,
- b) optymalizacja jakości świadczonych usług informatycznych przez:
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,

c) administrowanie lokalnymi systemami informatycznymi w podległych Izbie Administracji Skarbowej w Kielcach urządach, w tym:

- utrzymanie ciągłości działania systemów informatycznych,
- zapewnienie odpowiedniej wydajności systemów,
- instalowanie nowych wydań i poprawek,
- zarządzanie kontami użytkowników oraz uprawnieniami,
- zarządzanie kopiami awaryjnymi systemów i bazy danych,
- przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
- monitorowanie i utrzymanie warunków technicznych infrastruktury sprzętowo-programowej,

d) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,

e) wsparcie techniczne zadań związanych z informatyką śledczą,

f) zadanie scentralizowane w zakresie utrzymania centralnego systemu wideokonferencji,

g) zapewnienie stanowisk komputerowych z dostępem do udostępnionych podatnikom systemów teleinformatycznych, w szczególności Portalu Podatkowego, Portalu Usług Elektronicznych Skarbowo-Celnych w podległych Izbie Administracji Skarbowej w Kielcach urządach;

3) Do zadań **Zespołu Infrastruktury Sieciowej i Serwerowej, Bezpieczeństwa Informatycznego oraz Planowania i Logistyki Informatycznej** (RPD5TIIS) należy:

a) udział w opracowywaniu i utrzymaniu standardów dotyczących oprogramowania,

b) udział w testach i odbiorach systemów informatycznych realizowanych lokalnie, regionalnie i centralnie,

c) administrowanie warstwą aplikacyjną usług informatycznych oraz warstwą aplikacyjną systemów niejawnych, w tym:

- instalowanie nowych wydań i poprawek systemu,
- instalowanie kluczy licencyjnych,
- zapewnienie sprawności technicznej systemu informatycznego,
- zapewnienie odpowiedniej wydajności systemu,
- administracja oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
- utrzymanie systemowej bazy uprawnień użytkowników,
- zarządzanie kopiami awaryjnymi systemu i bazy danych,
- opracowanie procedur dotyczących administrowania systemem,
- monitorowanie przetwarzania informacji w systemie informatycznym, w kontekście bezpieczeństwa procesu przetwarzania,

d) utrzymanie wzorców konfiguracyjnych stacji roboczych lub sesji terminalowych oraz badanie ich podatności na zagrożenia,

e) udział w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego,

f) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym w Izbie Administracji Skarbowej w Kielcach,

g) projektowanie, wdrażanie oraz utrzymanie zabezpieczeń danych i systemów teleinformatycznych zgodnie z polityką bezpieczeństwa informacji,

h) administrowanie serwerowniami i sprzętem serwerowym,

i) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi,

j) utrzymywanie infrastruktury sieciowej, zgodnie z zasadami i standardami bezpieczeństwa,

k) planowanie rozbudowy i modyfikacji podległej infrastruktury,

l) zarządzanie kopiami bezpieczeństwa;

- m) planowanie rozwoju podległej infrastruktury informatycznej,
- n) planowanie wydatków na utrzymanie i rozwój informatyki lokalnej w Izbie Administracji Skarbowej w Kielcach i podległych urzędach,
- o) udział w procesie realizacji procesu zakupu sprzętu komputerowego, usług i oprogramowania,
- p) efektywne zarządzanie oprogramowaniem komputerowym oraz licencjami,
- q) wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej;
- 4) Do zadań **Zespołu Systemów Centralnych, Lokalnych i Bazy Wiedzy oraz Helpdesk (RPD5TIIC)** należy:
 - a) przygotowywanie, wdrażanie i administrowanie nowych lokalnych i regionalnych systemów informatycznych,
 - b) współpraca z komórkami organizacyjnymi Izby i podległymi urzędami w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych systemów informatycznych, w tym dokumentacji technicznej,
 - c) monitorowanie działania lokalnych i regionalnych systemów informatycznych i koordynowanie działań związanych z usunięciem awarii,
 - d) rozwój systemów lokalnych i regionalnych i ich wersjonowanie,
 - e) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług informatycznych pozyskiwanych regionalnie i lokalnie,
 - f) prowadzenie dokumentacji usług informatycznych,
 - g) zarządzanie procesami wsparcia użytkowników w zakresie obsługi systemów informatycznych na poziomie II–ej linii wsparcia, regionalnie i lokalnie,
 - h) organizowanie i prowadzenie zajęć warsztatowych w obszarze aplikacji lokalnych, regionalnych i centralnych,
 - i) obsługa i weryfikacja na poziomie regionalnym wniosków o założenie kont, nadanie, modyfikację lub odebranie uprawnień użytkownikom w zakresie aplikacji centralnych,
 - j) monitorowanie działania aplikacji wdrażanych regionalnie i centralnie,
 - k) zarządzanie i monitorowanie uaktualnienia Baz Wiedzy,
 - l) obsługa zamówień na informacje/zestawienia/raporty z systemów informatycznych przez formułowanie zapytań do baz danych, tworzenie skryptów,
 - m) zarządzanie procesem wsparcia użytkowników usług informatycznych oraz zewnętrznych użytkowników eksploatujących informatyczne systemy wdrażane przez Ministerstwo, w tym:
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom,
 - przekazywanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi Izby Administracji Skarbowej w Kielcach i podległymi urzędami oraz wykonawcami zewnętrznymi,
 - monitorowanie postępów prac nad zgłoszeniami,
 - n) optymalizacja jakości świadczonych usług informatycznych przez:
 - utrzymywanie funkcji ServiceDesk,
 - monitorowanie procesów: zarządzanie incydem, zarządzanie wnioskami i zarządzanie problemem,
 - realizacja i publikacja raportów z obsługi w ServiceDesk zgłoszeń, incydentów, wniosków,
 - inicjowanie i prowadzenie działań mających na celu podniesienie efektywności wsparcia informatycznego,

- o) udział w tworzeniu porozumień SLA (Service Level Agreement) oraz OLA (Operational Level Agreement),
- p) identyfikowanie obszarów wymagających poprawy jakości świadczonych usług informatycznych,
- q) określanie pozafunkcyjnych wymagań dla lokalnych systemów informatycznych w Izbie i podległych urzędach,
- r) dostarczanie, wdrażanie, rozwój i utrzymanie usług informatycznych dla KAS, w tym:
 - wspieranie jednostek organizacyjnych KAS w optymalizacji działalności przy wykorzystaniu usług informatycznych,
 - prowadzenie analiz systemowych dla usług informatycznych,
 - projektowanie usług informatycznych,
 - implementacja usług informatycznych,
 - weryfikowanie jakości dostarczanych usług informatycznych,
 - administrowanie techniczne komponentami usług informatycznych.

VI. Oddział Zarządzania Krajową Informacją Skarbową (RPD6)

1. Do zadań **Pierwszego Zespołu Informatyki (RPD6KLI1)** należy w szczególności:

- 1) zarządzanie eksploatacją i utrzymaniem systemów informatycznych;
- 2) obsługa zgłoszeń użytkowników eksploatowanych systemów;
- 3) zarządzanie infrastrukturą IT;
- 4) udział w projektach informatycznych realizowanych na szczeblu centralnym i lokalnym;
- 5) prowadzenie szkoleń w obszarze aplikacji i systemów informatycznych oraz obsługi urządzeń komputerowych;
- 6) określanie pozafunkcyjnych wymagań dla systemów informatycznych i teleinformatycznych KIS oraz udział w testach i odbiorach rozwiązań IT realizowanych centralnie i lokalnie;
- 7) planowanie wydatków na utrzymanie i rozwój usług informatycznych;
- 8) realizacja zadań związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych i cyberbezpieczeństwa;
- 9) współpraca z komórką Ministerstwa właściwą do spraw bezpieczeństwa;
- 10) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym i cyberbezpieczeństwa;
- 11) dostarczanie usług informatycznych oraz zarządzanie ich eksploatacją;
- 12) prowadzenie ewidencji sprzętu i oprogramowania informatycznego;
- 13) weryfikacja potrzeb użytkowników w zakresie sprzętu komputerowego i oprogramowania;
- 14) wnioskowanie w sprawach zakupów informatycznych;
- 15) techniczny odbiór dostaw i usług związanych z zakupem sprzętu komputerowego i oprogramowania.

2. Do zadań **Drugiego Zespołu Informatyki (RPD6KLI2)** należy w szczególności:

- 1) zarządzanie infrastrukturą IT;
- 2) udział w projektach informatycznych realizowanych na szczeblu centralnym i lokalnym;
- 3) prowadzenie szkoleń w obszarze aplikacji i systemów informatycznych oraz obsługi urządzeń komputerowych;
- 4) określanie pozafunkcyjnych wymagań dla systemów informatycznych i teleinformatycznych KIS oraz udział w testach i odbiorach rozwiązań IT realizowanych centralnie i lokalnie;

- 5) zarządzanie eksploatacją i utrzymaniem Systemu Informacji Telefonicznej;
- 6) zarządzanie systemami komunikacji elektronicznej;
- 7) administrowanie lokalną siecią komputerową i urządzeniami sieciowymi w KIS;
- 8) realizacja zadań związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych i cyberbezpieczeństwa;
- 9) współpraca z komórką Ministerstwa właściwą do spraw bezpieczeństwa;
- 10) współpraca z komórką bezpieczeństwa i ochrony informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym i cyberbezpieczeństwa.

VII. Oddział Zarządzania Krajową Szkołą Skarbowości (RPD7)

Do zadań realizowanych przez Zespół Zarządzania Wsparciem Informatycznym, Bezpieczeństwem Informatycznym, Infrastrukturą Sieciową i Serwerową (RPD7ZWI) obejmujący wszystkie siedziby/ Filie Krajowej Szkoły Skarbowości należą w szczególności:

1. przestrzeganie zasad bezpieczeństwa określonych w politykach bezpieczeństwa i instrukcjach zarządzania systemami,
2. zarządzanie eksploatacją i utrzymanie systemów informatycznych w tym:
 - utrzymanie ciągłości działania systemów informatycznych,
 - administrowanie serwerowniami i sprzętem serwerowym,
 - administrowanie i monitorowanie lokalnych sieci komputerowych i urządzeń sieciowych,
 - monitorowanie, zapewnienie odpowiedniej wydajności systemów i koordynowanie działań związanych z usunięciem awarii,
 - instalowanie nowych wydań i poprawek,
 - zarządzanie kopiami awaryjnymi systemów i bazy danych,
 - zarządzanie kontami użytkowników oraz uprawnieniami,
 - zarządzanie oprogramowaniem komputerowym oraz licencjami,
 - zarządzanie systemami komunikacji elektronicznej,
 - wsparcie osób zarządzających pionem informatyki w zakresie obsługi biurowej,
 - wsparcie osób zarządzających szkoleniami informatycznymi;
3. obsługa zgłoszeń użytkowników eksploatowanych systemów, ;
 - rejestrowanie i obsługa zgłoszeń od użytkowników,
 - analizowanie, weryfikowanie i rozwiązywanie zgłoszeń oraz udzielanie konsultacji użytkownikom, na poziomie II-ej i III-ej linii wsparcia, regionalnie i lokalnie;
 - eskalowanie nierozwiązanych zgłoszeń do kolejnych linii wsparcia,
 - informowanie użytkowników o stanie realizacji zgłoszenia,
 - identyfikowanie złożonych problemów wymagających rozwiązań, we współpracy z komórkami organizacyjnymi KSS, podległymi Filiami oraz wykonawcami zewnętrznymi,
4. zarządzanie infrastrukturą IT;
 - planowanie wydatków na utrzymanie i rozwój usług informatycznych,
 - planowanie rozbudowy i modyfikacji podległej infrastruktury,
 - dostarczanie usług informatycznych oraz zarządzanie ich eksploatacją,
 - prowadzenie ewidencji sprzętu i oprogramowania informatycznego,
 - współpraca z filiami KSS w zakresie identyfikacji i weryfikacji potrzeb informatycznych: sprzętu komputerowego, oprogramowania oraz dokumentacji technicznej,
 - wnioskowanie w sprawach zakupów informatycznych;
 - techniczny odbiór dostaw i usług związanych z zakupem sprzętu komputerowego i oprogramowania.
5. udział w projektach informatycznych realizowanych na szczeblu centralnym i lokalnym;
6. prowadzenie szkoleń w obszarze aplikacji i systemów informatycznych oraz obsługi urządzeń komputerowych;

7. realizacja zadań związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych i cyberbezpieczeństwa;
8. współpraca z komórką Ministerstwa właściwą do spraw bezpieczeństwa;
9. współpraca z komórką KSS odpowiedzialną za bezpieczeństwo i ochronę informacji w zakresie zarządzania bezpieczeństwem teleinformatycznym i cyberbezpieczeństwa;
10. wsparcie techniczne zadań związanych z informatyką dla:
 - Filia w Białobrzegach, Filia w Krakowie, Filia w Jastrzębiej Górze, Filia w Muszynie, Filia w Otwocku, Filia w Przemysłu, Filia we Wrocławiu

§ 33.

Departament Bezpieczeństwa IT (DBIT)

Do zakresu zadań **Wydziału Administrowania Systemami do Przetwarzania Informacji Niejawnych oraz Zabezpieczeń Aplikacji (DBIT1)** należy w szczególności:

- 1) administrowanie systemami teleinformatycznymi przeznaczonymi do przetwarzania informacji niejawnych, z wyłączeniem systemów informatycznych do obsługi GIIF, we współpracy z Pełnomocnikiem do spraw ochrony informacji niejawnych, w szczególności poprzez:
 - a) zapewnienie funkcjonowania systemów teleinformatycznych oraz przestrzegania zasad i wymagań bezpieczeństwa dla tych systemów,
 - b) uczestniczenie w procesie zarządzania ryzykiem bezpieczeństwa w systemach teleinformatycznych, poprzez realizację procesów:
 - szacowania ryzyka dla bezpieczeństwa informacji niejawnych,
 - postępowania z ryzykiem,
 - akceptacji ryzyka,
 - przeglądu, monitorowania i informowania o ryzyku,
 - c) uczestniczenie w opracowywaniu dokumentacji bezpieczeństwa dla systemów niejawnych,
 - d) wykonywanie okresowych testów bezpieczeństwa,
 - e) prowadzenie szkoleń użytkowników w zakresie:
 - procedur bezpiecznej eksploatacji,
 - oprogramowania użytkowego,
 - f) prowadzenie ewidencji użytkowników i ich uprawnień oraz odbytych przez nich szkoleń,
 - g) prowadzenie ewidencji sprzętu komputerowego i urządzeń, na których przetwarzane są informacje niejawne,
 - h) tworzenie i przechowywanie rejestru zdarzeń,
 - i) prowadzenie dzienników administratora odrębnie dla poszczególnych systemów teleinformatycznych;
- 2) instalowanie, aktualizowanie i konfigurowanie systemów operacyjnych i oprogramowania użytkowego w zakresie właściwości komórki organizacyjnej;
- 3) instalowanie i konfigurowanie szyfratorów oraz instalowanie certyfikatów krypto w urządzeniach i aplikacjach szyfrujących;
- 4) przygotowywanie dokumentacji przetargowych, w tym zakupów usług i sprzętu, we współpracy z komórką organizacyjną właściwą do spraw zakupów;
- 5) koordynowanie działań związanych z zapewnieniem bezpieczeństwa teleinformatycznego w systemach utrzymywanych w Ministerstwie Finansów i resorcie finansów, w zakresie inicjowania aktualizacji zapisów Polityki Bezpieczeństwa Informacji Resortu Finansów;
- 6) współpraca z Departamentem Informacji Finansowej w Ministerstwie Finansów w zakresie spraw związanych z bezpieczeństwem systemów informatycznych do obsługi GIIF;

- 7) planowanie, monitorowanie i weryfikowanie stosowania zabezpieczeń danych i systemów informatycznych;
- 8) administrowanie centralnymi systemami bezpieczeństwa;
- 9) identyfikowanie potrzeb oraz inicjowanie i projektowanie rozwiązań w zakresie systemów bezpieczeństwa teleinformatycznego;
- 10) wyznaczanie kierunków i zlecanie działań w zakresie bezpieczeństwa teleinformatycznego poprzez wdrażanie procedur i standardów bezpieczeństwa funkcjonujących w ramach resortu finansów;
- 11) współpraca z komórkami organizacyjnymi i nadzór nad realizowanymi przez nie działaniami w zakresie bezpieczeństwa teleinformatycznego;
- 12) realizowanie działań w zakresie zapewnienia w Ministerstwie Finansów oraz resorcie finansów bezpieczeństwa cyberprzestrzeni, w tym w szczególności:
 - a) współpraca z Pełnomocnikiem do spraw bezpieczeństwa cyberprzestrzeni w zakresie realizowania zadań wynikających z Polityki Bezpieczeństwa Cyberprzestrzeni RP, w tym m.in.:
 - opracowywanie i utrzymanie procedur reagowania na incydenty bezpieczeństwa teleinformatycznego dotyczących systemów informatycznych Ministerstwa Finansów oraz centralnej infrastruktury teleinformatycznej,
 - identyfikowanie i prowadzenie cyklicznych analiz ryzyka w obszarze bezpieczeństwa teleinformatycznego,
 - zapewnienie obsługi incydentów bezpieczeństwa teleinformatycznego dotyczących systemów informatycznych Ministerstwa Finansów oraz centralnej infrastruktury teleinformatycznej,
 - opracowanie procedur zapewniających informowanie właściwych zespołów CERT o wystąpieniu incydentów bezpieczeństwa teleinformatycznego dotyczących systemów informatycznych Ministerstwa Finansów oraz centralnej infrastruktury teleinformatycznej,
 - b) współpraca z Departamentem Bezpieczeństwa i Ochrony Informacji w Ministerstwie Finansów w zakresie opracowania i utrzymania Strategii ochrony cyberprzestrzeni w obszarze Ministerstwa Finansów i resortu finansów;
 - c) współpraca z resortem finansów w zakresie realizacji zadań wynikających z Polityki Bezpieczeństwa Cyberprzestrzeni RP w zakresie właściwości komórki organizacyjnej;
- 13) współpraca z Wydziałem Zarządzania Usługami IT w zakresie przeprowadzania testów RTO (Recovery Time Objective) i RPO (Recovery Point Objective);
- 14) współpraca z Departamentem Bezpieczeństwa i Ochrony Informacji w Ministerstwie Finansów w zakresie realizowania spraw obronnych, zarządzania kryzysowego, ciągłości działania Ministerstwa Finansów;
- 15) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 34.

Wydział Systemów Kadrowo-Płacowych Resortu Finansów (SKP)

Do zakresu zadań **Wydziału Systemów Kadrowo-Płacowych Resortu Finansów (SKP)** należy w szczególności:

- 1) przygotowywanie, wdrażanie i administrowanie centralnych rozwiązań IT w obszarze podatków, budżetu, logistyki i kadr, w tym systemu informatycznego Sykap;
- 2) współpraca z komórkami organizacyjnymi izb administracji skarbowej, urzędami skarbowymi oraz urzędami skarbowo-celnymi w zakresie identyfikacji potrzeb dostawy nowych lokalnych i regionalnych oraz centralnych rozwiązań IT w obszarze podatków, budżetu, logistyki i kadr w tym opracowywanie dokumentacji;
- 3) monitorowanie działania regionalnych i centralnych rozwiązań i koordynowanie działań związanych z usunięciem niedostępności;

- 4) wsparcie właściciela biznesowego w zakresie projektowania, wdrażania, utrzymania i doskonalenia centralnych rozwiązań w obszarze podatków, budżetu, logistyki i kadr;
- 5) współpraca z komórkami organizacyjnymi w zakresie identyfikacji potrzeb dostarczenia nowych centralnych rozwiązań w tym opracowywanie dokumentacji;
- 6) koordynowanie dostarczania, wdrażania, rozwoju i utrzymania usług biznesowych;
- 7) prowadzenie dokumentacji rozwiązań;
- 8) zarządzanie procesami wsparcia użytkowników w zakresie obsługi na poziomie III-ej linii wsparcia;
- 9) monitorowanie działania centralnych aplikacji wdrażanych;
- 10) monitorowanie działania rozwiązań i usług biznesowych;
- 11) projektowanie nowych funkcjonalności biznesowych, uzgadnianie procesów oraz ich modyfikacja i opisywanie;
- 12) przygotowanie informacji/zestawień/raportów z baz danych na podstawie otrzymanych zleceń;
- 13) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.

§ 35.

Wydział Prawny (PR)

Do zakresu zadań **Wydziału Prawnego (PR)** należy w szczególności:

- 1) realizowanie zadań związanych z projektami aktów wewnętrznych, w szczególności:
 - a) opracowywanie projektów aktów wewnętrznych,
 - b) prowadzenie uzgodnień wewnętrznych projektów aktów wewnętrznych,
 - c) opiniowanie oraz zapewnienie poprawności pod względem prawnym, legislacyjnym i redakcyjnym projektów aktów wewnętrznych opracowanych przez inne komórki organizacyjne Centrum;
- 2) prowadzenie rejestru aktów wewnętrznych wydawanych przez Dyrektora Centrum;
- 3) zapewnienie poprawności formalnoprawnej tekstów jednolitych aktów wewnętrznych;
- 4) uzgadnianie i opiniowanie projektów pełnomocnictw i upoważnień;
- 5) świadczenie obsługi prawnej;
- 6) reprezentowanie Centrum przed organami orzekającymi;
- 7) prowadzenie rejestru oraz terminarza spraw sądowych, w których stroną jest Centrum;
- 8) sporządzanie opinii prawnych oraz porady i konsultacje w zakresie stosowania prawa;
- 9) sygnalizowanie zapowiedzi nowych lub zmian obowiązujących przepisów związanych z funkcjonowaniem Centrum, poprzez bieżące informowanie o ww. zmianach;
- 10) udzielanie wyjaśnień i informacji pracownikom, w kwestiach prawnych związanych z wykonywanymi obowiązkami na poszczególnych stanowiskach służbowych;
- 11) wsparcie prawne w zakresie przeprowadzanych w Centrum kontroli, w tym opiniowanie lub sporządzanie pism kierowanych do organów uprawnionych do przeprowadzenia kontroli, przygotowywanie zastrzeżeń do protokołów kontroli i wystąpień pokontrolnych;
- 12) realizowanie zadań związanych z projektami pism oraz projektów innych dokumentów (umów, porozumień, aneksów), w szczególności:
 - a) opracowywanie projektów pism oraz projektów innych dokumentów,
 - b) prowadzenie uzgodnień wewnętrznych projektów pism oraz projektów innych dokumentów,
 - c) opiniowanie oraz zapewnienie poprawności pod względem prawnym, legislacyjnym i redakcyjnym projektów pism oraz projektów innych dokumentów opracowanych przez inne komórki organizacyjne Centrum;
- 13) wykonywanie innych zadań w zakresie właściwości komórki organizacyjnej.