RZECZPOSPOLITA POLSKA

MINISTERSTWO FINANSÓW

SZEF KRAJOWEJ ADMINISTRACJI SKARBOWEJ

DAS10.9011.15.2018.RKA.3

Sprawozdanie

Z AUDYTU LOKALNEGO SYSTEMU INFORMATYCZNEGO LSI (LS001) WYKORZYSTYWANEGO PRZY WDRAŻANIU REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA ŚLĄSKIEGO W PERSPEKTYWIE 2014-2020

CCI 2014PL 16M20P012

Warszawa, luty 2019 r.
Dokument zawiera 22 stron

Spis treści

WSTĘP

I.1. CEL SPRAWOZDANIA

Art. 127 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. *ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego rozporządzenie Rady (WE) nr 1083/2006* [dalej: rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013], nakłada na Instytucję Audytową obowiązek prowadzenia audytów systemu zarządzania i kontroli.

Zgodnie z art. 127 ust. 5 lit. a i b rozporządzenia 1303/2013 Instytucja Audytowa sporządza:

a) opinię audytową zgodnie z art. 63 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniającego rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylającego rozporządzenie (UE, Euratom) nr 966/2012;

b) sprawozdanie z kontroli, przedstawiające główne wyniki audytów przeprowadzonych zgodnie z ust. 1, w tym ustalenia dotyczące defektów stwierdzonych w systemach zarządzania i kontroli oraz proponowane i wdrożone działania naprawcze.

Zgodnie z art. 63 ust. 7 rozporządzenia finansowego dokumenty, o których mowa powyżej przekazywane są Komisji do dnia 15 lutego każdego roku budżetowego.

System zarządzania i kontroli Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020 oparty jest na przepisach rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013.

Sprawozdanie przedstawia zakres i wyniki czynności sprawdzających wykonanych przez pracowników Departamentu Audytu Środków Publicznych w Ministerstwie Finansów.

I.2. ORGAN ODPOWIEDZIALNY ZA SPORZĄDZENIE SPRAWOZDANIA

Wykonywanie zadań instytucji odpowiedzialnej za przeprowadzenie audytu systemu zostało powierzone Szefowi Krajowej Administracji Skarbowej, który pełni funkcję Instytucji Audytowej dla programów operacyjnych.

Szef Krajowej Administracji Skarbowej wykonuje swoje zadania za pośrednictwem Departamentu Audytu Środków Publicznych w Ministerstwie Finansów oraz komórek organizacyjnych zlokalizowanych w Izbach Administracji Skarbowej. Jest on również odpowiedzialny za zatwierdzenie przedmiotowego sprawozdania.

I.3. PODSUMOWANIE USTALEŃ

Audyt systemu LSI dla Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020 został przeprowadzony w Urzędzie Marszałkowskim Województwa Śląskiego, zgodnie ze strategią audytu dla Regionalnego Programu Operacyjnego Województwa Śląskiego.

Czynności sprawdzające dotyczyły kluczowego wymogu kontrolnego nr 6.

Wyniki badania kryterium oceny nr 23 (6.1) zostaną ujęte w *Sprawozdaniu z audytu głównego systemu informatycznego SL2014 wykorzystywanego przy wdrażaniu programów operacyjnych w perspektywie finansowej 2014-2020*.

Kryterium oceny nr 24 (6.2), z uwagi na fakt, iż wykorzystywany system informatyczny nie jest systemem raportującym, nie zostało objęte badaniem. Kryterium oceny nr 24 (6.2) oceniane jest w kontekście Centralnego Systemu Teleinformatycznego.

Dla kryterium oceny nr 25 (6.3) wydano łącznie 2 rekomendacje w kategorii 2. Ponadto 1 rekomendacja w kategorii 1 z lat ubiegłych pozostaje niewdrożona.

Dokonano oceny podsumowującej na poziomie poszczególnych obszarów Normy PN-ISO/IEC 27002:2014.

Oceny dla poszczególnych badanych obszarów:

Lp.	**Badane obszary**	**Liczba wydanych rekomendacji**				**Ocena podsumowująca badany obszar**
		Kategoria 1	**Kategoria 2**	**Kategoria 3**	**Kategoria 4**	
1	Polityki bezpieczeństwa informacji	-	-	-	-	1
2	Organizacja bezpieczeństwa informacji	-	-	-	-	1
3	Bezpieczeństwo zasobów ludzkich	-	-	-	-	1
4	Kontrola dostępu	-	-	-	-	1
5	Bezpieczeństwo fizyczne i środowiskowe	-	-	-	-	1
6	Bezpieczna eksploatacja	-	-	-	-	1
7	Bezpieczeństwo komunikacji	-	-	-	-	1
8	Pozyskiwanie, rozwój i utrzymanie systemów	-	-	-	-	1
9	Relacje z dostawcami	-	-	-	-	1
10	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	-	2	-	-	2
11	Zgodność	-	-	-	-	1

W związku z powyższym kluczowy wymóg kontrolny nr 6 został oceniony w **kategorii 2 – System funkcjonuje, potrzebne są jednak pewne usprawnienia,** zgodnie z wytyczną KE *Guidance for the Commission and Member States on a common methodology*

for the assessment of management and control systems in the Member States (EGESIF_14-0010-final).

Stan wdrożenia wydanych zaleceń będzie przedmiotem monitorowania w trakcie następnego audytu systemu zarządzania i kontroli.

II. METODYKA I ZAKRES PRAC AUDYTOWYCH

II.1. RAMY CZASOWE AUDYTU

Audyt przeprowadzony został od grudnia 2018 r. do stycznia 2019 r.

II.2. ZAKRES WYKONANYCH PRAC

Prace przeprowadzone zostały w Instytucji Zarządzającej Regionalnym Programem Operacyjnym Województwa Śląskiego - Urzędzie Marszałkowskim Województwa Śląskiego w Katowicach.

Celem przeprowadzonych prac było zapewnienie, iż spełniony jest kluczowy wymóg kontrolny nr 6. System oceniony został w następujących kryteriach:

- Kryterium oceny nr 23 (6.1) – Istnienie skomputeryzowanego systemu zdolnego do gromadzenia, rejestrowania i przechowywania danych w odniesieniu do każdej operacji, wymaganych w załączniku III rozporządzenia delegowanego Komisji (UE) nr 480/2014 z dnia 3 marca 2014 r. *uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013 ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego* [dalej rozporządzenia delegowanego Komisji (UE) nr 480/2014] w tym danych dotyczących wskaźników i celów pośrednich oraz danych na temat postępów programu w osiąganiu celów przekazanych przez instytucję zarządzającą na podstawie art. 125 ust. 2 lit. a) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013. Jeśli operacja jest objęta wsparciem z EFS, system musi również obejmować dane dotyczące poszczególnych uczestników oraz, jeśli jest to wymagane przez EFS, podział danych odnoszących się do wskaźników według płci.
- Kryterium oceny nr 24 (6.2) – Istnieją odpowiednie procedury, aby umożliwić agregowanie danych, gdy jest to konieczne dla celów ewaluacji, audytu, jak również w odniesieniu do wniosków o płatności i zestawień wydatków, rocznych sprawozdań podsumowujących, rocznej realizacji oraz sprawozdań końcowych, w tym sprawozdań dotyczących danych finansowych, przekazanych Komisji.
- Kryterium oceny nr 25 (6.3) – Istnieją odpowiednie procedury, aby zapewnić:
  a) zabezpieczenie i konserwację takiego skomputeryzowanego systemu, spójność danych, uwzględniając przyjęte międzynarodowe standardy jak na przykład ISO/IEC 27001:2013 i ISO/IEC 27002:2013, poufność danych, weryfikację nadawcy oraz przechowywanie dokumentów i danych, w szczególności

zgodnie z art. 122 ust. 3, art. 125 ust. 4 lit. d), art. 125 ust. 8 i art. 140 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013,

b) ochronę osób fizycznych w zakresie przetwarzania danych osobowych.

Opis audytowanego systemu:

System LSI2014 (LS001), którego właścicielem jest Urząd Marszałkowski Województwa Śląskiego w Katowicach, powstał w celu wspomagania realizacji Regionalnego Programu Operacyjnego Województwa Śląskiego w perspektywie 2014-2020. System zbudowany został w architekturze cienkiego klienta (dostęp poprzez przeglądarkę internetową) przez firmę zewnętrzną wyłonioną w drodze postępowania o udzielenia zamówienia publicznego. System LSI2014 w zakresie obsługi programu RPO w UMWSL jest systemem wspomagającym, wykorzystywanym m.in. w zakresie:

- generowania naborów po stronie użytkownika – instytucji ogłaszającej konkurs (IOK),
- przygotowania przez wnioskodawcę wniosku o dofinansowanie,
- rejestracji złożonych wniosków w systemie,
- rejestracji wyników oceny wniosków o dofinansowanie (ocena formalna i merytoryczna),
- odnotowania faktu wyboru projektu do dofinansowania oraz zawarcia umowy,
- rejestracji umowy oraz ewentualnych aneksów do zawartej mowy,
- przygotowania przez użytkownika IOK harmonogramów wniosków o płatność,
- przygotowania przez beneficjenta wniosków o płatność,
- rejestracji wyników oceny formalno-merytorycznej wniosków o płatność,
- rejestracji zatwierdzenia do wypłaty środków,
- przygotowania PEFS'a, czyli danych uczestników projektów (po stronie beneficjenta) – generator PEFS,
- automatycznego przekazania danych PEFS wraz z wnioskiem o płatność,
- rejestrowania przez beneficjenta danych personelu projektu – generator Personelu Projektu,
- rejestrowania przeprowadzonych kontroli.

System utrzymywany jest przez służby informatyczne Urzędu Marszałkowskiego Województwa Śląskiego na infrastrukturze własnej Urzędu w Data Center firmy 3S Data Center S.A. System LSI2014 zapewnia obsługę konkursów w ramach dofinansowania ze środków EFRR lub EFS. Dostępny jest dla pracowników Instytucji Zarządzającej Regionalnym Programem Operacyjnym (Urząd Marszałkowski Województwa Śląskiego), Instytucji Pośredniczących (Śląskie Centrum Przedsiębiorczości i Wojewódzki Urząd Pracy w Katowicach) oraz dla wnioskodawców/beneficjentów.
System zintegrowany jest z Centralnym Systemem Teleinformatycznym SL2014, do którego dane są eksportowane z wykorzystaniem Web Services w zakresie informacyjnym zgodnym z „*Wytycznymi w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020*".

Wykonane czynności:

Przeprowadzono analizę niżej wymienionych dokumentów:

- Uchwały nr 2057/283/V/2018 Zarządu Województwa Śląskiego z 04.09.2018 r.,
- Polityki Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego,
- Zarządzenia Marszałka Województwa Śląskiego nr 00082/18 z 19.09.2018 r.,
- Zarządzenia Marszałka Województwa Śląskiego nr 00045/18 z 11.06.2018 r.,
- Księgi Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego,
- Procedury zarządzania dostępem,
- Procedury kopii zapasowych,
- Polityki ochrony danych osobowych,
- Procedury postępowania z incydentami,
- Procedury zarządzania ciągłością działania,
- Procedury zarządzania ryzykiem,
- Procedury zarządzania zmianami IT,
- Deklaracji stosowania,
- Instrukcji użytkownika,
- Instrukcji Zarządzania Systemem Informatycznym,
- Regulaminu organizacyjnego Urzędu Marszałkowskiego Województwa Śląskiego,
- Notatek z posiedzenia Komitetu Bezpieczeństwa Urzędu,
- Raportu z przeglądu zintegrowanego systemu zarządzania za okres od 01.01.2017 r. do 31.12.2017 r.,
- Protokołu z przeglądu zintegrowanego systemu zarządzania za okres od 01.01.2017 r. do 31.12.2017 r.,
- Instrukcji użytkownika Lokalnego Systemu Informatycznego 2014 dla Wnioskodawców/Beneficjentów RPO WSL 2014-2020,
- Instrukcji dodawania i zmiany załączników we wniosku o dofinansowanie,
- Instrukcji składania wniosków, korespondencji i protestów w ramach naborów dotyczących projektów finansowanych ze środków Regionalnego Programu Operacyjnego Województwa Śląskiego 2014-2020,
- Regulaminu użytkownika Lokalnego Systemu Informatycznego Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020 (LSI2014),
- Wymagań technicznych i konfiguracji przeglądarek internetowych,
- Dokumentacji technicznej LSI (dokumentacja dla administratorów),
- Notatki służbowej z aktualizacji planów ciągłości działania z 29.12.2017 r.,
- Harmonogramu testowego odtwarzania systemów z kopii bezpieczeństwa,
- Rejestru testowego odtwarzania systemów z kopii bezpieczeństwa,
- Umów na wsparcie serwisowe,
- Umowy na kolokowanie urządzeń.

Przeprowadzono wywiady z pracownikami:

- Kierownikiem Referatu Zarządzania Lokalnym Systemem Informatycznym,
- Inspektorem Ochrony Danych,
- Kierownikiem Referatu Informatyki,
- Kierownikiem Referatu Monitoringu i Kontroli Trwałości,
- pracownikami Referatu ds. Zarządzania Bezpieczeństwem Informacji,
- pracownikami Referatu Informatyki, Zespołu sieci informatycznych i systemów serwerowych,
- pracownikiem Referatu Aplikacji i Zarządzania.

III. WYNIKI OCENY

III.1. KRYTERIUM OCENY NR 23 (6.1) KLUCZOWEGO WYMOGU KONTROLNGO NR 6

W celu uzyskania zapewnienia, że wskazany przez Komisję Europejską zakres danych dotyczący realizowanych projektów (wskazanych w załączniku III do rozporządzenia delegowanego Komisji (UE) nr 480/2014) znajduje się w systemie informatycznym oraz przedstawia prawidłowe dane, przeprowadzono test mający na celu ustalenie, czy odpowiedni zakres danych został wprowadzony do CST SL2014 i czy dane są prawidłowe. Kryterium zostanie ocenione w ramach audytu bezpieczeństwa systemu SL2014.

III.2. KRYTERIUM OCENY NR 24 (6.2) KLUCZOWEGO WYMOGU KONTROLNEGO NR 6

System LSI (LS001) jest systemem wspomagającym wykorzystywanym na etapie składania wniosków o dofinansowanie w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego. Dane z systemu eksportowane są do Centralnego Systemu Teleinformatycznego SL2014, który przechowuje i agreguje dane określone w załączniku III do rozporządzenia delegowanego Komisji (UE) nr 480/2014. Systemem raportującym, zapewniającym ścieżkę audytową dla realizowanych projektów, jest CST SL2014, w związku z powyższym ocena spełnienia kryterium nr 24 (6.2) zostanie dokonana przez Instytucję Audytową podczas audytu systemu informatycznego SL2014.

III.3. KRYTERIUM OCENY NR 25 (6.3) KLUCZOWEGO WYMOGU KONTROLNEGO NR 6

Obszar audytu Lokalnego Systemu Informatycznego (LSI) w zakresie Regionalnego Programu Operacyjnego Województwa Śląskiego w Urzędzie Marszałkowskim Województwa Śląskiego (UMWSL) został określony na podstawie analizy ryzyka, w której uwzględniono:

- Sprawozdanie z audytu bezpieczeństwa systemu LSI z 2017 r.,
- arkusz Urzędu Marszałkowskiego Województwa Śląskiego zawierający wykaz zmian w poszczególnych obszarach/domenach normy ISO/IEC27002, które stwierdzono od czasu ostatniego badania systemu,
- przegląd wstępny przeprowadzony przez audytora.

Zakres audytu stanowią następujące zagadnienia:

1. Polityki bezpieczeństwa informacji,
2. Organizacja bezpieczeństwa informacji,
3. Bezpieczeństwo zasobów ludzkich,
4. Kontrola dostępu,
5. Bezpieczeństwo fizyczne i środowiskowe,
6. Bezpieczna eksploatacja,
7. Bezpieczeństwo komunikacji,
8. Pozyskiwanie, rozwój i utrzymanie systemów,
9. Relacje z dostawcami,
10. Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
11. Zgodność.

Ustalenia opisane w dalszej części sprawozdania odzwierciedlają stan rzeczywisty zweryfikowany przez Instytucję Audytową na podstawie analizy dokumentów, wywiadów z pracownikami instytucji oraz testów potwierdzających działanie mechanizmów kontrolnych.

W wyniku przeprowadzonych prac audytowych ustalono:

1. Polityki bezpieczeństwa informacji

1.1. Kierunki bezpieczeństwa informacji określane przez kierownictwo

1.1.1. Polityki dotyczące bezpieczeństwa informacji

Polityka Zintegrowanego Systemu Zarządzania jest udokumentowana i dostępna w formie papierowej oraz w formie elektronicznej na stronie internetowej Urzędu, w Biuletynie Informacji Publicznej oraz w intranecie. Powyższe zapewnia pełną dostępność do treści dokumentu dla wszystkich zainteresowanych stron, zarówno z wewnątrz jak i zewnątrz organizacji.

Zgodnie z *Księgą Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego* (KZSZ), stanowiącą załącznik nr 1 do Zarządzenia nr 00082/18 Marszałka Województwa Śląskiego z 19.09.2018 r., w urzędzie jest wdrożony, utrzymywany i doskonalony zintegrowany system zarządzania (ZSZ) spełniający m. in. wymagania norm ISO 9001:2015 oraz ISO 27001:2017. Skuteczność zintegrowanego systemu zarządzania, w tym kontroli zarządczej zapewnia się poprzez realizację ustalonych w urzędzie procedur, rozwiązania organizacyjne i techniczne oraz wdrożenie procesu zarządzania ryzykiem. Kontrola zarządcza w Urzędzie Marszałkowskim Województwa Śląskiego (UMWSL) funkcjonująca w ramach zintegrowanego systemu zarządzania obejmuje również zarządzanie jakością oraz zarządzanie bezpieczeństwem informacji.

Podstawowe założenia i zasady obowiązujące w zintegrowanym systemie zarządzania w Urzędzie obejmują m.in:

- zastosowanie podejścia procesowego w zarządzaniu urzędem,
- zarządzanie ryzykiem, w tym ocenę ryzyka bezpieczeństwa informacji,

- zapewnienie stałego doskonalenia skuteczności funkcjonującego zintegrowanego systemu zarządzania,
- uwzględnienie bezpieczeństwa informacji i ochrony danych osobowych we wszystkich realizowanych procesach.

Dla osiągnięcia skutecznego zintegrowanego systemu zarządzania w urzędzie zdefiniowano mapę procesów, która przedstawia procesy główne, zarządcze i pomocnicze (mapa procesów stanowi załącznik nr 2 do *Księgi Zintegrowanego Systemu Zarzadzania*). Dla każdego procesu przeprowadzono analizę ryzyka. Dodatkowo analizie ryzyka poddawane są również aktywa informacyjne pod kątem zapewnienia poufności, dostępności i integralności przetwarzanych informacji. Zgodnie z pkt. 4.4.9 KZSZ, w celu skutecznego zarządzania procesami, sprawnego koordynowania zadań oraz utrzymania oczekiwanego poziomu bezpieczeństwa informacji w ramach zintegrowanego systemu zarządzania ustanowiono *Politykę Zintegrowanego Systemu Zarządzania* (PZSZ) oraz określono pozostałe procedury określające sposób realizacji zadań (w tym w zakresie zarządzania ryzykiem).

Najważniejszym dokumentem w ramach zintegrowanego systemu zarządzania jest *Polityka Zintegrowanego Systemu Zarządzania* z dnia 04.09.2018 r. Drugim dokumentem w hierarchii jest Księga Zintegrowanego Systemu Zarządzania. Ponadto do dokumentacji obejmującej swoim zakresem ZSZ należy m. in:

- *Procedura działań korygujących,*
- *Procedura audytu wewnętrznego,*
- *Polityka ochrony danych osobowych* (PODO),
- *Polityka zarządzania ciągłością działania* (PZCD),
- *Instrukcja użytkownika,*
- *Instrukcja zarządzania systemem informatycznym* (IZSI),
- *Procedura zarządzania dostępem* (PZD),
- *Procedura postępowania z incydentami* (PPI),
- *Procedura kopii zapasowych,*
- *Zasady zarządzania zmianami IT,*
- *Procedura zarządzania ryzykiem.*

Zgodnie z PZSZ, wszyscy pracownicy zostali zobowiązani do zapoznania się z Polityką ZSZ za pomocą obiegu dokumentów, poczty elektronicznej i poprzez tablice ogłoszeń w intranecie oraz zostali zobligowani do jej stosowania w trakcie wykonywania obowiązków służbowych. W trakcie audytu potwierdzono, iż pracownicy, składając podpis przy swoim nazwisku na wykazie pracowników, potwierdzili zapoznanie się z *Zarządzeniem Marszałka Województwa Śląskiego nr 00082/2018 z 19.09.2018 r. w sprawie przyjęcia dokumentacji zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego* i przyjęli do stosowania.

Nowo zatrudnieni pracownicy są zapoznawani z zakresem ZSZ, w tym polityką ZSZ w ramach procedury przygotowawczej. W trakcie audytu potwierdzono, iż nowo zatrudnieni pracownicy, składają podpis na indywidualnych *Oświadczeniach o odpowiedzialności* (załącznik nr 12 do Polityki Ochrony Danych Osobowych),

potwierdzając tym samym, że zapoznali się z treścią regulacji i obowiązków zawartych w *Księdze Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego* oraz w politykach szczegółowych, które przyjmują do stosowania.

Ponadto składają oświadczenie, że odbyli szkolenie z zakresu obowiązujących w Urzędzie Marszałkowskim Województwa Śląskiego zasad bezpieczeństwa informacji oraz ochrony danych osobowych i że znana jest im treść *Zarządzenia nr 82/2018 Marszałka Województwa Śląskiego z dnia 18.09.2018 r. w sprawie wprowadzenia Księgi Zintegrowanego Systemu Zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego.*

1.1.2. Przegląd polityki bezpieczeństwa informacji

Zgodnie z pkt 5 KZSZ w ramach monitorowania i sprawozdawczości w zakresie ZSZ raz w roku najwyższe kierownictwo UMWSL przeprowadza przegląd zintegrowanego systemu zarządzania. W ramach przeglądu analizowany jest m. in. stopień realizacji celów Polityki ZSZ, celów procesów, celów priorytetowych województwa, celów jakościowych oraz celów bezpieczeństwa informacji. Ponadto na bieżąco odbywają się spotkania najwyższego kierownictwa z kadrą kierowniczą urzędu w ramach posiedzeń Zarządu, narad i bieżących konsultacji, podczas których omawiane są postępy w realizacji celów i zadań oraz istotne problemy, ryzyka i słabości funkcjonowania urzędu.

Ponadto zgodnie z pkt 9.1.1.10 *Monitorowanie stanu bezpieczeństwa informacji* KZSZ, przegląd stanu bezpieczeństwa informacji realizowany jest kwartalnie (lub zgodnie z potrzebami) przez Komitet Bezpieczeństwa Urzędu i obejmuje następujące zagadnienia:

- zapewnienie, że ryzyka w obszarze bezpieczeństwa informacji są zarządzane, a działania, plany postępowania z ryzykiem osiągają zaplanowane rezultaty,
- przegląd rejestru zdarzań i incydentów w celu wyciagnięcia wniosków z incydentów związanych z bezpieczeństwem informacji,
- weryfikacja i zatwierdzenie planów zachowania ciągłości działania oraz wyników testów planów zachowania ciągłości działania,
- przedstawienie bieżących działań komórki ds. zarządzania bezpieczeństwem informacji IOD i GASI,
- wspieranie osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji.

Z przeglądu sporządzana jest notatka określająca stan bezpieczeństwa oraz wskazująca działania i zasoby niezbędne do realizacji celów bezpieczeństwa informacji w urzędzie. Powyższe potwierdzono na podstawie notatek z posiedzenia Komitetu Bezpieczeństwa Urzędu nr 3/2018 z 30.07.2018 r. oraz nr 4/2018 z 09.12.2018 r.

W trakcie audytu potwierdzono przeprowadzenie przeglądu zintegrowanego systemu zarządzania na podstawie *Protokołu z przeglądu zintegrowanego systemu zarządzania za okres od 01.01.2017 r. do 31.12.2017 r.* zatwierdzonego przez Marszałka Województwa w dniu 30.03.2018 r. Ponadto przedstawiono *Raport z przeglądu zintegrowanego systemu zarządzania za okres od 01.01.2017 r. do 31.12.2017 r.* zatwierdzony przez Marszałka Województwa w dniu 27.03.2018 r.

Ostatnia aktualizacja *Księgi Zintegrowanego Systemu Zarządzania* miała miejsce pod koniec III kwartału 2018 r.

2. Organizacja bezpieczeństwa informacji

2.1. Organizacja wewnętrzna

2.1.1. Role i odpowiedzialności za bezpieczeństwo informacji

Zgodnie z treścią KZSZ Komitet Bezpieczeństwa Urzędu monitoruje bieżący poziom bezpieczeństwa informacji w Urzędzie oraz dba o to, aby wymagania bezpieczeństwa były zidentyfikowane i uwzględnione w procesach i systemach teleinformatycznych funkcjonujących w Urzędzie. Skład Komitetu Bezpieczeństwa Urzędu proponowany jest przez przewodniczącego, przy czym obligatoryjnymi członkami są: Inspektor Ochrony Danych (IOD), Główny Administrator Systemu Informatycznego (GASI), osoba z komórki koordynującej zarządzanie ryzykiem w urzędzie oraz osoba odpowiedzialna za audyt w urzędzie. Sekretarz Województwa jest informowany o przebiegu prac komitetu oraz w razie potrzeby jest włączany w jego działania.

Za całość kwestii technicznych związanych z bezpieczeństwem systemów teleinformatycznych i urządzeń służących do przetwarzania danych urzędu odpowiadają właściwe komórki Wydziału ds. informatyki. W celu sprawowania skutecznego nadzoru nad systemami informatycznymi wyznaczono Głównego Administratora Systemu Informatycznego (GASI), którego role pełni dyrektor/ zastępca dyrektora Wydziału ds. informatyki lub osoba upoważniona. GASI w szczególności:

- wypełnia obowiązki związane z zarządzaniem systemami informatycznymi, wynikające z regulacji wewnętrznych, polityk szczegółowych obszaru bezpieczeństwa informacji,
- dba o bezpieczeństwo systemów teleinformatycznych urzędu oraz ich zgodność z przepisami prawa,
- pełni nadzór nad Administratorami Systemów Informatycznych (ASI),
- dba o podnoszenie wiedzy technicznej ASI,
- współpracuje z pozostałymi osobami pełniącymi funkcje w ramach systemu zarządzania bezpieczeństwem informacji oraz komórkami organizacyjnymi urzędu w zakresie związanym z bezpieczeństwem systemów teleinformatycznych urzędu,
- zapewnia prowadzenie dokumentacji, rejestrów i wykazów wymaganych przepisami prawa oraz wskazanych w politykach szczegółowych.

Każdy system informatyczny (rozumiany jako narzędzie programowe służące do przetwarzania danych, w szczególności danych osobowych) używany w urzędzie powinien mieć wyznaczonego minimum jednego Administratora Systemu Informatycznego (ASI) odpowiedzialnego za kwestie techniczne związane z danym systemem oraz zarządzanie uprawnieniami dostępu. W przypadku systemów zewnętrznych, udostępnianych przez inne instytucje, nadzór nad procesem zarządzania uprawnieniami do systemu sprawują kierownicy komórek organizacyjnych korzystających z tych systemów lub wyznacza się Administratora

Uprawnień (AU) w systemie informatycznym na podstawie zakresu obowiązków służbowych. ASI/AU w szczególności:

- wypełnia obowiązki wynikające z regulacji wewnętrznych obszaru bezpieczeństwa informacji,
- wprowadza, modyfikuje lub usuwa prawa dostępu do systemu informatycznego dla poszczególnych użytkowników zgodnie z obowiązującymi procedurami,
- zapewnia konfigurację systemu zapewniającą bezpieczeństwo informacji w nim przetwarzanych,
- dba o zgodność systemu z wymogami prawa i regulacji wewnętrznych urzędu,
- świadczy pomoc dla użytkowników z zakresu systemu oraz urządzeń służących do przetwarzania danych systemu – ze szczególną dbałością o wiedzę z zakresu bezpieczeństwa systemów i bezpiecznej pracy z systemem,
- w uzgodnieniu z GASI i IOD opracowuje i proponuje, w razie takiej potrzeby, odrębne szczegółowe instrukcje i procedury dotyczące danego systemu w celu włączenia ich do dokumentacji ZSZ.

Ponadto w urzędzie na podstawie art. 37 ust. 1 lit. a RODO wyznaczony został Inspektor Ochrony Danych (IOD). Szczegółowe zasady funkcjonowania IOD zawarte zostały w *Polityce ochrony danych osobowych* oraz w *Regulaminie organizacyjnym Urzędu Marszałkowskiego Województwa Śląskiego.* Zgodnie z §48 ww. regulaminu do zakresu działania Inspektora Ochrony Danych należą sprawy związane z bezpieczeństwem i ochroną danych osobowych, w tym w szczególności:

- wypełnianie obowiązków określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO),
- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy ww. rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych osobowych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania ww. rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym: podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

3. Bezpieczeństwo zasobów ludzkich

3.1.1. Uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji

Zgodnie z pkt 7.1.6 *Wiedza organizacji* KZSZ kierownictwo urzędu przywiązuje dużą wagę do nabywania wiedzy w drodze dokształcania pracowników w formie samokształcenia, szkoleń wewnętrznych i zewnętrznych, studiów podyplomowych, kursów językowych, udziału w warsztatach, konferencjach, spotkaniach grup roboczych, itp. Zasady dokształcania pracowników uregulowane zostały w *Zarządzeniu nr 0004/18 Marszałka Województwa Śląskiego z 11.06.2018 r. w sprawie przyjęcia procedury podnoszenia kwalifikacji zawodowych pracowników UMWSL*. Pracownicy, biorący udział w różnych formach dokształcania, przekazują zdobyta wiedzę pozostałym członkom zespołu.

Ponadto zgodnie z pkt 12.5 *Szkolenia i działania zwiększające świadomość* PODO pracownicy UMWSL odbywają szkolenia okresowo, nie rzadziej niż raz na dwa lata. Szkolenia związane są z zagadnieniami dotyczącymi bezpieczeństwa informacji i ochrony danych osobowych. Za zapewnienie szkoleń odpowiada IOD.

W PODO określono również, iż każda osoba, przetwarzająca dane osobowe na rzecz Administratora Danych ma obowiązek działania z jego upoważnienia i na jego polecenie. W związku z powyższym, osoba upoważniana potwierdza podpisem na upoważnieniu zobowiązanie do stosowania zasad bezpieczeństwa, do zachowania tajemnicy danych oraz sposobów ich zabezpieczania. Powyższe potwierdzono na podstawie *Upoważnienia do przetwarzania danych osobowych* nowo zatrudnionego pracownika z 17.01.2019 r. W przypadku osób upoważnianych po raz pierwszy (nowy pracownik), osoba upoważniana odbywa w Referacie ds. zarządzania bezpieczeństwem informacji szkolenie wstępne z zakresu zasad bezpieczeństwa informacji i ochrony danych osobowych oraz podpisuje oświadczenie (patrz pkt 1.1.1. Polityki dotyczące bezpieczeństwa informacji).

W trakcie audytu potwierdzono cykliczną realizację szkoleń z zakresu ochrony danych osobowych i bezpieczeństwa informacji. Szkolenia są planowane, a ich harmonogram dostępny jest na stronie intranetowej UM – zakładka: „Zintegrowany System Zarządzania / Szkolenia" (http://intranet.slaskie.pl/app/section/219/). Pracownicy w dniu szkolenia podpisują *Listę obecności* (np. lista obecności dotycząca szkolenia przeprowadzonego w dniu 14.12.2018 r. w zakresie bezpieczeństwa przetwarzania informacji i ochrony danych osobowych).

4. Kontrola dostępu

Rozdział 4 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

5. Bezpieczeństwo fizyczne i środowiskowe

Rozdział 5 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

6. Bezpieczna eksploatacja

6.1. Procedury eksploatacyjne i odpowiedzialność

6.1.1. Dokumentowanie procedur eksploatacyjnych

W zakresie eksploatacji oraz użytkowania systemu LSI funkcjonują m.in. następujące dokumenty:

- *Instrukcja użytkownika Lokalnego Systemu Informatycznego 2014 dla Wnioskodawców/Beneficjentów RPO WSL 2014-2020,*
- *Instrukcja dodawania i zmiany załączników we wniosku o dofinansowanie,*
- *Instrukcja składania wniosków, korespondencji i protestów w ramach naborów dotyczących projektów finansowanych ze środków Regionalnego Programu Operacyjnego Województwa Śląskiego 2014-2020,*
- *Regulamin użytkownika Lokalnego Systemu Informatycznego Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020 (LSI2014),*
- *Wymagania techniczne i konfiguracja przeglądarek internetowych.*

Instrukcje użytkowe dla wnioskodawców/beneficjentów publikowane są na stronie informacyjnej Lokalnego Systemu Informatycznego 2014 (https://rpo.slaskie.pl/czytaj/lokalny_system_informatyczny_2014/).

W ramach utrzymania oraz eksploatacji środowiska teleinformatycznego UMWSL funkcjonują właściwe procedury dedykowane użytkownikom oraz administratorom systemów. Są to m.in.:

- *Dokumentacja techniczna LSI (dokumentacja dla administratorów),*
- *Instrukcja użytkownika* (załącznik nr 7 do Zarządzenia nr 00082/2018),
- *Instrukcja zarządzania systemem informatycznym (Załącznik nr 7 do Zarządzenia nr 00082/2018),*
- *Procedura kopi zapasowych (Załącznik nr 11 do Zarządzenia nr 00082/2018),*
- *Zasady zarządzania zmianami i wydaniami IT* (załącznik nr 12 do Zarządzenia nr 00082/2018),

6.1.2. Zarządzanie zmianami

Sposób zarządzania zmianami oraz wydaniami w usługach informatycznych w UMWSL przedstawia dokument: *Zasady zarządzania zmianami IT*.

Zgodnie z ww. dokumentem źródłem zmian wprowadzanych na środowiska testowe/produkcyjne mogą być:

- zgłoszenia użytkowników,
- konieczność implementacji nowych funkcjonalności w systemach i oprogramowaniu,
- rekomendacje dostawców zewnętrznych,
- incydenty, problemy, znane błędy.

W UMWSL rozróżniane są następujące typy zmian:

- zmiana standardowa – zmiana o minimalnym ryzyku i wpływie na procesy biznesowe, zmiana nie wymaga rejestracji, akceptacji, analizy wykonalności i testowania,
- zmiana normalna dzieląca się na: zmianę małą (zmiana o małym ryzyku i wpływie na biznes, wymagająca akceptacji przez drugiego pracownika działu, posiadającego wiedzę na temat proponowanej zmiany) oraz zmianę dużą (zmiana o dużym ryzyku i wpływie na procesy biznesowe, wymagająca akceptacji dyrektora wydziału ds. informatyki),
- zmiana awaryjna – zmiana o krytycznym ryzyku, pilności i wpływie na procesy biznesowe, zmiany te wykonywane są w celu usunięcia awarii.

Każda zmiana ma przydzielony priorytet (wysoki, średni, niski), który może zostać zmieniony na każdym etapie realizacji zmiany. Zmiany podlegają testowaniu z zachowaniem zasad bezpieczeństwa.

Do obsługi zmian w aplikacji LSI wykorzystano system MantisBT, który jest zintegrowany z systemem GIT. Za zbieranie informacji na temat zmian, analizę potrzeb oraz opracowanie zgłoszeń odpowiada Zespół ds. rozwoju LSI. Ponadto do systemu MantisBT mogą trafić zgłoszenia od użytkowników systemu LSI (w tym beneficjentów). Zarządzanie procesami zmian oparte jest o strukturę SCRUM. W systemie MantisBT odnotowywane są informacje na temat zgłoszenia zmiany, realizację zmiany przez programistów, testy w pierwszej kolejności wykonane przez pracowników Referatu Zarządzania Lokalnym Systemem Informatycznym, a w drugiej kolejności przez instytucję ogłaszającą konkurs. Każdy krok odnotowywany jest w systemie przy pomocy statusów. Po przeprowadzeniu testów akceptacyjnych zmiana jest implementowana w środowisku produkcyjnym.

6.1.3. Zarządzanie pojemnością

Podrozdział 6.1.3 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

6.1.4. Oddzielenie środowisk rozwojowych, testowych i produkcyjnych

W pkt 15.3 *Rozdzielenie systemów produkcyjnych od testowych* IZSI określono ogólne zasady rozdzielenia systemów produkcyjnych, testowych i opracowywania nowych aplikacji. W tym celu ASI odpowiedzialny jest za to, że:

- oprogramowanie do opracowywania i testowania jest oddzielone,
- procesy testowania i wytwarzania aplikacji są rozdzielone,
- stosowane są różne hasła do systemów produkcyjnych, testowych i opracowywania nowych aplikacji.

Zgodnie z zawartymi informacjami w IZSI, nie wolno w UMWSL stosować danych zawierających dane identyfikujące osobę lub inne poufne dane w charakterze danych testowych. Wykorzystanie danych produkcyjnych do testów możliwe jest po zastosowaniu pseudonimizacji lub anonimizacji zgodnie z art. 4 RODO.

Za organizację przydzielenia, aktualizacji i odbierania dostępów do systemów testowych, w których nie znajdują się kopie danych produkcyjnych, odpowiadają upoważnieni pracownicy Referatu Zarządzania Lokalnym Systemem Informatycznym.

Zgodnie z dokumentacją techniczną rozróżniamy następujące wersje środowisk LSI:

- lsi-dev.slaskie.pl – wersja rozwojowa, na której tworzone są nowe moduły i funkcjonalności. Pierwszy poziom testów,
- lsi-test.slaskie.pl – bieżące i szybkie poprawki dotyczące funkcjonalności działających produkcyjnie. Obsłużone i zgłoszone do testów poprawki nie powinny pozostawać bez zatwierdzenia dłużej niż 24h,
- lsi-szkol.slaskie.pl – odpowiednik wersji produkcyjnej do celów szkoleniowych,
- lsi.slaskie.pl – wersja produkcyjna,
- lsi-raport.slaskie.pl – wersja oparta o bazę danych replikowaną z wersji produkcyjnej z uprawnieniem tylko do SELECT-a.

Urząd Marszałkowski Województwa Śląskiego utrzymuje trzy wirtualne serwery, na których pracuje system LSI 2014. Na jednym serwerze (LSI) zainstalowana jest wersja produkcyjna i szkoleniowa, na drugim (LSI test) wersja deweloperska i testowa, (aplikacja i baza danych pracuje na jednym serwerze), na trzecim LSI-raport.

6.2. Ochrona przed szkodliwym oprogramowaniem

Podrozdział 6.2 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

6.3. Kopie zapasowe

Podrozdział 6.3 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

6.4. Rejestrowanie zdarzeń i monitorowanie

6.4.1. Rejestrowanie zdarzeń

Rozliczalność w systemach teleinformatycznych, zgodnie z IZSZ, podlega dokumentowaniu w dziennikach systemów (logach). Obligatoryjnie w dziennikach odnotowuje się:

- dostęp do systemu z uprawnieniami administracyjnymi,

- dostęp do konfiguracji systemu, w tym konfiguracji zabezpieczeń,
- dostęp do danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

Dodatkowo zaleca się, aby w dziennikach były odnotowywane:

- działania użytkowników nieposiadających uprawnień administracyjnych,
- zdarzenia systemowe o mniejszym znaczeniu dla funkcjonowania systemu,
- zdarzenia i parametry środowiska w którym eksploatowany jest system.

Zgodnie z IZSI informacje w dziennikach przechowywane są od dnia zapisu przez dwa lata lub zgodnie z obowiązującymi dany system szczegółowymi przepisami prawa. Zapisy do plików systemowych (logowanie zdarzeń) odbywa się automatycznie. Administratorzy techniczni nie mają możliwości ingerencji w dzienniki zdarzeń. Zgodnie z uzyskanymi informacjami w trakcie audytu, logi nie są usuwane z systemu LSI. W trakcie audytu potwierdzono, że pierwsze logi datowane są na czerwiec 2015 r.

7. Bezpieczeństwo komunikacji

Rozdział 7 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

8. Pozyskiwanie, rozwój i utrzymanie systemów

Rozdział 8 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

9. Relacje z dostawcami

9.1. Bezpieczeństwo informacji w relacjach z dostawcami

9.1.1. Polityka bezpieczeństwa informacji w relacjach z dostawcami

Zgodnie z pkt *18 Uwzględnienie bezpieczeństwa w relacjach z dostawcami IZSI,* w umowach zawieranych z wykonawcami należy uwzględniać kwestie związane z bezpieczeństwem informacji, szczególnie dotyczące:

- zachowania poufności,
- informacji podlegających ochronie, w tym danych osobowych,
- spełniania wymogów prawnych,
- praw własności intelektualnej i prawa autorskiego,
- zasad informowania o naruszeniach.

Monitorowanie umów związanych z bezpieczeństwem informacji realizowane jest przez osoby wskazane przez kierownika komórki organizacyjnej odpowiedzialnej za daną umowę. Monitorowanie odbywa się co najmniej raz w roku.

Licencje, własność kodów i praw własności intelektualnej, jak i kwestie bezpiecznego projektowania, kodowania i stosowanych praktyk testowania każdorazowo uregulowane są w załącznikach do umowy w zakresie tworzenia i zakupywania nowych aplikacji/systemów.

Z uzyskanych w trakcie audytu informacji wynika, iż obecnie nie obowiązują umowy zawarte z podmiotami zewnętrznymi w zakresie funkcjonowania systemu LSI. Prace rozwojowe nad systemem LSI w UMWSL realizowane są własnymi siłami urzędu.

Umowy z podmiotami zewnętrznymi zostały zawarte w ramach wsparcia serwisowego:

- umowa nr 3105/2R/2016 z 08.12.2016 r. zawarta pomiędzy Województwem Śląskim a Infonet Projekt S.A. – przedmiotem umowy jest świadczenie asysty technicznej dla macierzy (dyskowych), w której m. in. określono sposób i warunki kontaktu pomiędzy UMWSL a wykonawcą umowy i serwisem, sposób i warunki realizacji umowy (w tym m.in. sposób zgłoszenia awarii, czas usunięcia awarii) oraz zasady realizacji zmian postanowień zawartej umowy,
- umowa nr 2122/2R/2015 z 08.09.2015 r. pomiędzy Województwem Śląskim a COIG S.A. – przedmiotem umowy jest dostawa fabrycznie nowych serwerów, w której m. in. określono warunki gwarancji, sposób postępowania z dyskiem twardym z uwagi na bezpieczeństwo danych oraz zasady realizacji zmian postanowień zawartej umowy.

Ponadto, na usługę kolokowania urządzeń oraz dostęp do punktu wymiany ruchu sieciowego dla UMWSL zawarto umowę nr 4794/OR/2018 z 17.10.2018 r. pomiędzy Województwem Śląskim a Konsorcjum (3S DataCenter S.A., 3S S.A.). Zgodnie z zapisami umowy, wykonawca nie jest uprawniony do przetwarzania, wykorzystywania, czy jakiejkolwiek ingerencji w dane (w tym dane osobowe) przetwarzane przez zamawiającego w Centrum Przetwarzania Danych. Ponadto oświadcza, że realizuje politykę bezpieczeństwa opartą o aktualne normy w zakresie bezpieczeństwa informacji, zgodną z obowiązującymi przepisami prawa. W załączniku nr 1 do umowy określone zostały parametry SLA (Service Level Agreement) dla usług łącza transmisji danych.

9.1.2. Uwzględnienie bezpieczeństwa w porozumieniach z dostawcami

Zgodnie z pkt *15.1 Cykl życia systemów informatycznych IZSI*, Systemy informatyczne, które mają być wprowadzane w urzędzie podlegają formalnemu procesowi planowania ich wyboru i wdrożenia. Przeprowadzana jest analiza ryzyka oraz identyfikowane są wymagania funkcjonalne i pozafunkcjonalne dla systemów informatycznych, w tym wymagania związane z bezpieczeństwem informacji przetwarzanych w tym systemie. Wdrażanie systemów informatycznych realizowane jest każdorazowo, zgodnie z zapisami umowy o opracowanie i uruchomienie danego systemu.

Dla systemów informatycznych funkcjonujących w urzędzie, o ile to uzasadnione, utrzymywane są umowy wsparcia, w szczególności w zakresie dostarczana

poprawek bezpieczeństwa oraz zapewniania zgodności z przepisami obowiązującego prawa.

9.2. Zarządzanie usługami świadczonymi przez dostawców

9.2.1. Monitorowanie i przegląd usług świadczonych przez dostawców

Zgodnie z pkt 15.1 *Cykl życia systemów informatycznych IZSI*, w przypadku, gdy utrzymanie systemu/serwis techniczny realizowane jest przez dostawców zewnętrznych, wyznacza się parametry SLA podlegające monitorowaniu, np. czas na reakcję, czas na usunięcie awarii, dostępność systemu. System LSI 2014 utrzymywany jest na sprzęcie własnym Urzędu Marszałkowskiego i siłami własnymi urzędu. Umowy opisane w pkt 9.1.1. są świadczone przez wyłonionego na drodze postępowania przetargowego wykonawcę zewnętrznego. W umowach znajdują się zapisy regulujące zasady współpracy, które obowiązują strony. Podstawą wypłaty wynagrodzenia jest przekazanie przez wykonawcę protokołu odbiorczego lub protokołu zdawczo-odbiorczego.

9.2.2. Zarządzanie zmianami w usługach świadczonych przez dostawców

Zgodnie z pkt 15.1 *Cykl życia systemów informatycznych IZSI* zmiany w ramach systemów informatycznych już funkcjonujących w Urzędzie realizowane są zgodnie z procedurą *Zasady zarządzania zmianami IT*. Wycofywanie systemów z eksploatacji realizowane jest w oparciu o wniosek, który przesyłany jest przez kierownika komórki organizacyjnej, w której system funkcjonuje do Wydziału ds. Informatyki.

Zarządzanie zmianami w usługach świadczonych przez dostawców jest regulowane w poszczególnych umowach z podmiotami zewnętrznymi.

Proces w zakresie zasad zarządzania zmianami w LSI został szerzej opisane w punkcie w pkt. 6.1.2 – *Zarządzania zmianami*.

10. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Rozdział 10 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

11. Zgodność

11.1. Zgodność z wymaganiami prawnymi i umownymi

11.1.1. Określenie stosowanych wymagań prawnych i umownych

Zgodnie z pkt 2 *Powołania normatywne* KZSZ zintegrowany system zarządzania przyjęty w Urzędzie Marszałkowskim Województwa Śląskiego jest zgodny z:

- mającymi zastosowanie wymogami normy ISO 9001:2015 oraz normy ISO 27001:2017,

- Ustawą z dnia 27 sierpnia 2009 r. o finansach publicznych oraz komunikatem nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych,
- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. U. UE. L. 119 z 4 maja 2016 r. (RODO),
- Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (UODO),
- Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
- Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Ponadto do najważniejszych aktów prawnych regulujących działalność urzędu należy wymienić m.in.:

- Ustawę z dnia 5 czerwca 1998 r. o samorządzie województwa,
- Ustawę z dnia 21 listopada 2008 r. o pracownikach samorządowych,
- Ustawę z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego,
- Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych,
- Statut Województwa Śląskiego,
- Statut Urzędu Marszałkowskiego Województwa Śląskiego,
- Regulamin Organizacyjny Urzędu Marszałkowskiego Województwa Śląskiego,
- Wewnętrzne regulaminy organizacyjne komórek organizacyjnych Urzędu.

11.1.2. Prywatność i ochrona danych identyfikujących osobę

Polityka ochrony danych osobowych (PODO) stanowiąca *Załącznik nr 5 do Zarządzenia nr 00082/2018 Marszałka Województwa Śląskiego z 19.09.2018 r.* określa specyficzne kwestie związane z realizacja obowiązków Administratora Danych i dotyczy przetwarzania danych osobowych w Urzędzie Marszałkowskim Województwa Śląskiego. Zgodnie z ww. wszelkie czynności przetwarzania danych osobowych odbywać się będą z poszanowaniem określonych w art. 5 Rozporządzenia 2016/679 (RODO) zasad tj.:

- zgodności z prawem, rzetelności i przejrzystości,
- ograniczenia celu,
- minimalizacji danych,
- prawidłowości danych,
- ograniczenia przechowywania,

- integralności i poufności,
- rozliczalności Administratora Danych z przestrzegania przepisów.

Ponadto Administrator Danych oraz wszystkie osoby przetwarzające dane osobowe osób fizycznych na jego rzecz, w ramach odpowiedzialności za przetwarzanie danych osobowych, są zobowiązani do przestrzegania przepisów prawa i wykazywania ich przestrzegania w ramach zasady rozliczalności.

W UMWSL funkcjonuje Inspektor Ochrony Danych, który zgodnie z PODO prowadzi i na bieżąco aktualizuje *Rejestr czynności przetwarzania danych osobowych* oraz *Rejestr kategorii czynności przetwarzania podmiotu przetwarzającego*. Obydwa rejestry (potwierdzono w trakcie audytu) prowadzone są w formie elektronicznej i udostępniane są komórkom organizacyjnym urzędu za pomocą narzędzia elektronicznego eORG. Każda zmiana w eORG dotycząca obydwu rejestrów jest odnotowana w systemie.

Ponadto zgodnie z PODO z przetwarzaniem danych osobowych wiążą się ryzyka naruszenia praw lub wolności osób. Analiza ryzyka powinna odbywać się:

- systematycznie dla istniejących procesów przetwarzania danych osobowych,
- na etapie projektowania nowych procesów przetwarzania danych osobowych,
- w razie wystąpienia istotnych zmian w procesie przetwarzania danych lub zidentyfikowania nowych zagrożeń.

Sposób postępowania z ryzykiem określa *Procedura zarządzania ryzykiem w Urzędzie Marszałkowskim Województwa Śląskiego* (*Załącznik do Zarządzenia nr 00084/2018 Marszałka Województwa Śląskiego z dnia 19.09.2018 r*.). Ponadto patrz pkt 11.2 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami.

12. Audyt stanu wdrożenia rekomendacji otwartych z lat ubiegłych

Rozdział 12 usunięto na podstawie art. 5 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330)
Wyłączenie w zakresie danych dotyczących sposobów zabezpieczeń w systemie LSI.

Usunięcia dokonał: Łukasz Zmuda

Zatwierdził: Małgorzata Staś, Dyrektor Wydziału Rozwoju Regionalnego

Z upoważnienia
Szefa Krajowej Administracji Skarbowej

Paweł Cybulski

Zastępca Szefa Krajowej Administracji Skarbowej
/podpisano kwalifikowanym podpisem elektronicznym/