RZECZPOSPOLITA POLSKA

MINISTERSTWO FINANSÓW

SZEF KRAJOWEJ ADMINISTRACJI SKARBOWEJ

DAS10.9011.16.2019.3.GUXC

Sprawozdanie

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

CCI2014PL16M2OP012

Spis treści

I. 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.

Dokumenty, o których mowa powyżej przekazywane są Komisji do dnia 15 lutego kolejnego roku budżetowego.

System zarządzania i kontroli Regionalnego Programu Operacyjnego Województwa Śląskiego w perspektywie finansowej 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.

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 (Departament DAS) w Ministerstwie Finansów oraz właściwych komórek organizacyjnych Izb Administracji Skarbowej. Jest on również odpowiedzialny za zatwierdzenie przedmiotowego sprawozdania.

I.3. PODSUMOWANIE USTALEŃ

Audyt systemu dla Regionalnego Programu Operacyjnego Województwa Śląskiego 2014-2020 został przeprowadzony zgodnie ze *Strategią audytu Regionalnego Programu Operacyjnego Województwa Śląskiego 2014-2020* w oparciu o *Program audytu.*

Czynności sprawdzające dotyczyły kluczowego wymogu kontrolnego nr 6.

Wyniki badania kryterium oceny nr 23 (6.1) zostaną ujęte w *Sprawozdaniu z audytu bezpieczeństwa 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 głównego systemu teleinformatycznego SL2014.

Dla kryterium oceny nr 25 (6.3) wydano łącznie 6 rekomendacji w kategorii 1. Ponadto, 2 rekomendacje w kategorii 2 z lat ubiegłych pozostają niewdrożone.

Dokonano oceny podsumowującej na poziomie poszczególnych obszarów Normy PN-ISO/IEC 27002:2017.

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	2	0	0	0	1
2.	Bezpieczeństwo zasobów ludzkich	0	0	0	0	1
3.	Kontrola dostępu	2	0	0	0	1
4.	Kryptografia	0	0	0	0	1
5.	Bezpieczeństwo fizyczne i środowiskowe	0	0	0	0	1
6.	Bezpieczna eksploatacja	2	0	0	0	1
7.	Bezpieczeństwo komunikacji	0	0	0	0	1
8.	Pozyskiwanie, rozwój i utrzymanie systemów	0	0	0	0	1
9.	Relacje z dostawcami	0	0	0	0	1
10.	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	0	0	0	0	1
11.	Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	0	0	0	0	1
12.	Zgodność	0	0	0	0	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 w lipcu 2019 r.

II.2. ZAKRES WYKONANYCH PRAC

Prace przeprowadzone zostały w Instytucji Zarządzającej Regionalnym Programem Operacyjnym Województwa Śląskiego 2014-2020 – w Urzędzie Marszałkowskim Województwa Śląskiego.

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 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* [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 płatność 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 27001:2017 i ISO/IEC 27002:2017, 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 LSI (dalej: LSI2014, LS001), którego właścicielem jest Urząd Marszałkowski Województwa Śląskiego w Katowicach (dalej: UMWSL), 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 udzielenie 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 umowy,
- 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, czyli danych uczestników projektów (po stronie beneficjenta) – generator PEFS,
- automatycznego przekazania danych PEFS wraz z wnioskiem o płatność,
- rejestrowania przez beneficjenta danych personelu projektu,
- rejestrowania przeprowadzonych kontroli.

Za utrzymanie systemu odpowiada Wydział Cyfryzacji i Informatyki Urzędu Marszałkowskiego Województwa Śląskiego. System utrzymywany jest na infrastrukturze własnej urzędu, w Data Center firmy 3S Data Center S.A. System zapewnia obsługę konkursów dofinansowanych ze środków EFRR i EFS. Dostępny jest dla:

- pracowników Instytucji Urzędu Marszałkowskiego Województwa Śląskiego pełniącego funkcję Instytucji Zarządzającej Regionalnym Programem Operacyjnym,
- pracowników Śląskiego Centrum Przedsiębiorczości pełniącego funkcję Instytucji Pośredniczącej,

- pracowników Wojewódzkiego Urzędu Pracy w Katowicach pełniącego funkcję Instytucji Pośredniczącej,
- 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 dokumentów m.in:

- Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013;
- Uchwały nr 2057/283/V/2018 Zarządu Województwa Śląskiego z 04.09.2018 r. w sprawie przyjęcia Polityki Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego;
- Zarządzenia nr 00082/18 z dnia 19.09.2018 r. Marszałka Województwa Śląskiego w sprawie przyjęcia Polityki Zintegrowanego Systemu Zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego wraz z załącznikami:
  - Księgą Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego;
  - Procedurą działań korygujących;
  - Procedurą auditu wewnętrznego;
  - Deklaracją stosowania;
  - Polityką ochrony danych osobowych;
  - Instrukcją zarządzania systemem informatycznym;
  - Instrukcją użytkownika;
  - Procedurą zarządzania dostępem;
  - Procedurą postepowania z incydentami;
  - Polityką zarządzania ciągłością działania;
  - Procedurą kopii zapasowych;
  - Zasadami zarządzania zmianami IT.
- Zarządzenia Marszałka Województwa Śląskiego nr 00084/18 z dnia 19.09.2018 r. w sprawie wprowadzenia Procedury zarządzania ryzykiem w Urzędzie Marszałkowskim Województwa Śląskiego;
- Uchwały nr 1514/53/VI/2019 Zarządu Województwa Śląskiego z dnia 03.07.2019 r. w sprawie Regulaminu organizacyjnego Urzędu Marszałkowskiego Województwa Śląskiego wraz z załącznikami;
- Uchwały nr 550/28/VI/2019 Zarządu Województwa Śląskiego z dnia 20.03.2019 r. w sprawie przyjęcia Polityki Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego;
- Porozumienia nr 8/RR/2015 z dnia 16.03.2015 r. zawartego ze Śląskim Centrum Przedsiębiorczości w sprawie realizacji RPO WSL na lata 2014-2020 wraz z aneksem nr 5 z dnia 25.03.2019 r.;

- Porozumienia nr 13/RR/2015 z dnia 17.03.2015 r. (tekst jednolity) zawartego z Wojewódzkim Urzędem Pracy w Katowicach;
- Notatki z dnia 26.04.2019 r. z posiedzenia Komitetu Bezpieczeństwa Urzędu wraz z załącznikami;
- Raportu na przegląd zintegrowanego systemu zarządzania za okres od 01.01.2018 r. do 31.12.2018 r.;
- Protokołu z przeglądu zintegrowanego systemu zarządzania za okres od 01.01.2018 r. do 31.12.2018 r.;
- Notatek ze spotkań grupy LSI;
- Zasad zarządzania LSI 2014 w ramach RPO WSL 2014-2020;
- Instrukcji użytkownika Lokalnego Systemu Informatycznego 2014 dla Wnioskodawców/Beneficjentów RPO WSL 2014-2020;
- Instrukcji dodawania i zmiany załączników we wniosku o dofinansowanie;
- Instrukcji wypełniania Karty oceny formalno-merytorycznej oraz merytorycznej dla Oceniających w ramach Lokalnego Systemu Informatycznego RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,
- Instrukcji obsługi wniosku o płatność w ramach Lokalnego Systemu Informatycznego 2014 dla operatorów RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,
- Instrukcji obsługi modułu korekt zatwierdzania wniosku o płatność dla operatorów w ramach Lokalnego Systemu Informatycznego 2014 RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,
- Instrukcji operatora Lokalnego Systemu Informatycznego LSI 2014 moduł – kontrole projektu,
- Instrukcji obsługi KOP dla operatorów w ramach Lokalnego Systemu Informatycznego 2014 RPO WSL 2014-2020 w części dotyczącej współfinansowania,
- Instrukcji wypełniania modułów nabory, projekty, wnioski o dofinansowanie, Umowy w ramach Lokalnego Systemu Informatycznego 2014 dla operatorów RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,
- Instrukcji obejmującej zmiany w module kontroli w ramach Lokalnego Systemu Informatycznego 2014 dla operatorów RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,
- 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 (LSI 2014);
- Wymagań technicznych i konfiguracji przeglądarek internetowych dla systemu LSI2014;
- Dokumentacji technicznej LSI (dokumentacja dla administratorów);
- Notatki służbowej z aktualizacji planów ciągłości działania z 18.12.2018 r.;
- Harmonogramu testów planów ciągłości działania na 2019 r.;

- Protokołów z testów planów ciągłości działania z dnia 18.12.2018 r.;
- Listy scenariuszy i planów ciągłości działania;
- Harmonogramu testowego odtwarzania systemów z kopii bezpieczeństwa wraz z załącznikiem: Rejestr testowego odtwarzania systemów z kopii bezpieczeństwa;
- Umowy z dnia 30.10.2018 r. zawartej z firmą SITEL Sp. z o.o. na świadczenie usługi stałego szerokopasmowego dostępu do Internetu;
- Umowy z dnia 17.10.2018 r. zawartej z firmą 3S Data Center S.A. na usługę kolokacji;
- Umowy z dnia 03.11.2017 r. zawartej z firmą 3S S.A. na dzierżawę łączy światłowodowych;
- Umowy z dnia 10.09.2018 r. zawartej z firmą Intaris Sp. z o.o. na dostawę sprzętu komputerowego;
- Protokołów z przeglądu systemów wspomagających w serwerowni: klimatyzacji, gaszenia gazem, UPS;
- Przykładowego zgłoszenia incydentu bezpieczeństwa;
- Dwóch arkuszy: Cząstkowa ocena podatności (słabości) lub incydentu bezpieczeństwa informacji z dnia 08.07.2019 r;
- Notatki służbowej Referatu Systemów Informatycznych - Wydziału Organizacyjnego z dnia 05.07.2019 r.;
- Końcowej oceny podatności (słabości) lub incydentu bezpieczeństwa informacji z dnia 08.07.2019 r.;
- Zgłoszenia naruszenia ochrony danych osobowych przekazanego do PUODO;
- Listy obecności ze szkolenia wewnętrznego „Bezpieczeństwo przetwarzania informacji, ochrona danych osobowych" z dnia 14.06.2019 r.;
- Oświadczeń pracowników o odbyciu szkoleń z zakresu obowiązujących w UMWSL zasad bezpieczeństwa informacji oraz zasad ochrony danych osobowych;
- Oświadczeń pracowników o odpowiedzialności w zakresie przepisów prawa;
- Kart obiegowych dla wybranych pracowników urzędu;
- Potwierdzenia realizacji służby przygotowawczej dla wybranych pracowników Urzędu;
- Potwierdzeń zapoznania się pracowników z zarządzeniem Marszałka Województwa Śląskiego nr 00082/2018 z dnia 19.09.2018 r.;
- Rejestru czynności (procesów) przetwarzania danych osobowych administratora danych;
- Ewidencji upoważnień do przetwarzania danych osobowych;
- Harmonogramu szkoleń na 2019 r. z bezpieczeństwa informacji i ochrony danych osobowych;
- Raportów z okresowego przeglądu uprawnień systemu LSI za I i II kwartał 2019 r.;
- Raportu z aktywności użytkowników systemu LSI, wygenerowanego z systemu eORG;
- Przykładowych maili w zakresie nadania, odebrania, modyfikacji uprawnień użytkowników;

- Wniosków dla pracowników o nadanie uprawnień w systemie informatycznym;
- Wniosków o nadanie uprawnień w systemie LSI;
- Wniosku o założenie konta dla członka KOP;
- Upoważnień do przetwarzania danych osobowych;
- Certyfikatów zgodności na drzwi (serwerownia i kolokacja);
- Certyfikatu systemu zarządzania dla 3S Data Center S.A.;
- Oświadczenia firmy 3S Data Center z dnia 28.01.2019 r.;
- Protokołu naprawy sprzętu (dysku) z dnia 03.06.2019 r.;
- Raportu z wypożyczeń klucza do pomieszczeń serwerowni;
- Raportu z dnia 21.12.2015 r. z przeglądu, konserwacji systemu SSWiN, kontroli stanu pomieszczenia;
- Raportu z dnia 16.02.2018 r. z wykonania przeglądu i konserwacji systemu SSWiN, AKPiA, CCTV (System sygnalizacji włamań i napadu, aparatura kontrolna pomiarowa i automatyka, telewizja przemysłowa);
- Zrzutów ekranu obrazujących blokowanie stron internetowych;
- Zrzutów ekranu z systemu Zabbix;
- Zrzutu ekranu telefonu z komunikatem z systemu Zabbix;
- Zrzutów ekranu z systemu GitLab;
- Zrzutów ekranu systemu MantisBT;
- Zrzutów ekranu z testu protokołu TLS;
- Zrzutów ekranu korelatora logów OSSIM;
- Zrzutów ekranu z systemu Palo Alto;
- Zrzutów ekranu z testowania (przeglądu) systemu LSI 2014;
- Zrzutów ekranu z systemu antywirusowego Kaspersky i ClamAV;
- Zrzutów ekranu z systemu eORG;
- Zrzutów ekranu z systemu eHR;
- Zrzutów ekranu z Intranetu UMWSL;
- Zrzutów ekranu z systemu Magik Info;
- Zrzutu ekranu z testu protokołu TLS;
- Zrzutu ekranu obrazującego synchronizację czasu;
- Zrzutu ekranu z systemu monitoringu serwerowni przy ul. Dąbrowskiego 23 – zrzut z obecności audytorów w serwerowni.

Przeprowadzono wywiady z pracownikami:

- Inspektorem ochrony danych (IOD);
- Pracownikami Referatu ds. zarządzania systemem bezpieczeństwa informacji w Wydziale Zarządzania i Organizacji Urzędu;
- Kierownikiem i pracownikami Referatu zarządzania infrastrukturą teleinformatyczną w Wydziale Cyfryzacji i Informatyki;

- Kierownikiem Referatu projektowania i rozwoju systemów informatycznych w Wydziale Cyfryzacji i Informatyki;
- Pracownikiem Referatu analiz systemu realizacji RPO WSL w Wydziale Rozwoju Regionalnego;
- Kierownikiem Referatu naboru i rozwoju pracowników w Wydziale Kadr i Płac;
- Pracownikami Referatu kadr w Wydziale Kadr i Płac;
- Kierownikiem Referatu monitoringu i kontroli trwałości w Wydziale Europejskiego Funduszu Rozwoju Regionalnego;
- Pracownikiem Referatu Lokalnego Systemu Informatycznego i nadzoru w Wydziale Europejskiego Funduszu Społecznego.

Przeprowadzono następujące testy:

- dokonano weryfikacji funkcjonowania procedur wymienionych w pkt. II.2,
- dokonano weryfikacji umów wymienionych w pkt. II.2,
- sprawdzono wyposażenie i zabezpieczenia pomieszczeń serwerowni,
- sprawdzono ustawienia domenowe serwera systemu Windows w zakresie polityki kont i haseł,
- sprawdzono ustawienia i zapisy aktywności oprogramowania antywirusowego,
- sprawdzono ustawienia firewalla,
- sprawdzono ustawienia aplikacji backupu,
- przeprowadzono testy mechanizmów kontrolnych systemu LSI 2014.

Przeprowadzono wizyty w:

- Urzędzie Marszałkowskim Województwa Śląskiego w Katowicach,
- Centrum Danych 3S Data Center S.A. zlokalizowanym przy ul. Gospodarczej 12 w Katowicach,
- Serwerowni Urzędu Marszałkowskiego Województwa Śląskiego zlokalizowanej przy ul. Dąbrowskiego 23 w Katowicach.

III. WYNIKI OCENY

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

W celu uzyskania zapewnienia, że wskazany przez Komisję Europejską zakres danych dotyczący realizowanych projektów (ujęty w załączniku III rozporządzenia delegowanego Komisji (UE) nr 480/2014) znajduje się w systemie informatycznym oraz przedstawia prawidłowe dane, zostanie przeprowadzony 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 jest systemem wspomagającym wykorzystywanym na etapie składania wniosków o dofinansowanie, zawierania umów oraz składania wniosków o płatność w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego 2014-2020. Dane z systemu eksportowane są do Centralnego Systemu Teleinformatycznego SL2014, który przechowuje i agreguje dane wskazane w załączniku III 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 oceny nr 24 (6.2) zostanie dokonana przez Instytucję Audytową podczas audytu bezpieczeństwa głównego systemu teleinformatycznego 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, opisany poniżej, stanowią następujące zagadnienia:

1. Polityki bezpieczeństwa informacji,
2. Bezpieczeństwo zasobów ludzkich,
3. Kontrola dostępu,
4. Kryptografia,
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. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania,
12. 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 przeprowadzonego audytu ustalono:

1. Polityki bezpieczeństwa informacji

1.1. Kierunki bezpieczeństwa informacji określane przez kierownictwo

1.1.1. Polityki dotyczące bezpieczeństwa informacji

W UMSL obowiązuje *Księga Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego* (dalej: KZSZ). Dokument został wprowadzony Zarządzeniem nr 00082/18 Marszałka Województwa Śląskiego z dnia 19.09.2018 r. Zgodnie z zapisami pkt 4.3 KZSZ, w urzędzie wdrożony, utrzymywany i doskonalony jest zintegrowany system zarządzania (dalej: ZSZ), spełniający wymagania norm ISO 9001:2015 i ISO27001:2017 oraz wymagania prawne, w tym w zakresie kontroli zarządczej.

Dokumentacja ZSZ obejmuje m. in.:

- *Politykę Zintegrowanego Systemu Zarządzania* (dalej: PZSZ),
- *Księgę Zintegrowanego Systemu Zarządzania* wraz z załącznikami,
- *Deklarację stosowania,*
- Udokumentowane procedury, w tym:
  - *Procedurę działań korygujących,*
  - *Procedurę audytu wewnętrznego,*
  - *Politykę ochrony danych osobowych (dalej: PODO),*
  - *Politykę zarządzania ciągłością działania (dalej: PZCD),*
  - *Instrukcję Użytkownika (dalej: IU),*
  - *Instrukcję Zarządzania Systemem Informatycznych (dalej: IZSI),*
  - *Procedurę zarządzania dostępem (dalej: PZD),*
  - *Procedurę postępowania z incydentami,*
  - *Procedurę kopii zapasowych,*
  - *Zasady zarządzania zmianami IT.*

W toku audytu ustalono:

Ustalenie nr 1	W treści procedur, które obejmuje dokumentacja ZSZ, występują odwołania do załączników. Z uwagi na fakt, iż procedury nie zawierają wykazu załączników, jak również załączniki nie stanowią integralnej części procedur, nie można stwierdzić, która wersja załącznika jest obowiązująca i aktualna.
Kategoria	Kategoria 1 – System funkcjonuje prawidłowo. Nie są potrzebne żadne lub potrzebne są tylko niewielkie usprawnienia.
Rekomendacja	Zaleca się, aby załączniki do procedur wchodzących w skład ZSZ stanowiły jej integralną część.
Stanowisko IZ	Księga oraz Procedury podstawowe ZSZ tj. Procedura działań korygujących oraz Procedura auditu wewnętrznego zawierała i w nowym wydaniu zawiera spis załączników, które stanowią integralną część procedur.

	Zgodnie z aktualnym brzmieniem pkt 7.5.2 ppkt 8 Księgi: "W przypadku konieczności wprowadzenia zmian w treści Księgi ZSZ, Deklaracji stosowania lub procedur, o których mowa w podrozdziale pkt 7.5. pkt 1 ust. 1 pkt 4 zaleca się opracowanie w całości nowego dokumentu z oznaczeniem kolejnego numeru wydania". W tej sytuacji ograniczona jest możliwość wprowadzenia nowego wydania załącznika do procedury bez nowego wydania samej procedury. Przyjęty sposób ewidencjonowania wydań odnosi się również do samych procedur a nie załączników do nich, zgodnie z poniższym zapisem pkt 7.5.2 ppkt 9 Księgi: „Komórka ds. zintegrowanego zarządzania prowadzi ewidencję dokumentacji ZSZ, o której mowa w podrozdziale 7.5. pkt 1 ust. 1 pkt 2 do 4 Księgi z odpowiednim oznaczeniem aktualnych i nieaktualnych wydań".
Stanowisko Instytucji Audytowej	**Rekomendacja podtrzymana. Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up.** IZ powinna wdrożyć rekomendację w ciągu 6 miesięcy.

Dokumentem określającym cele wdrożenia zintegrowanego systemu zarządzania jest *Polityka Zintegrowanego Systemu Zarządzania.* W dokumencie określona została misja Urzędu Marszałkowskiego Województwa Śląskiego, deklaracja Zarządu Województwa Śląskiego co do spełnienia wymagań norm ISO9001:2015 i ISO 27001:2017 oraz cele urzędu, którymi są:

- analizowanie potrzeb klientów i stałe doskonalenie świadczonych usług,
- zapewnienie poufności, integralności i dostępności informacji przetwarzanych w urzędzie, ze szczególnym uwzględnieniem obszaru ochrony danych osobowych,
- prowadzenie przejrzystej polityki informacyjnej,
- doskonalenie metod zarządzania zasobami ludzkimi, polepszanie warunków organizacyjnych i technicznych oraz stanu infrastruktury i środowiska pracy,
- utrzymanie i doskonalenie zintegrowanego systemu zarządzania w urzędzie.

Dokumentem uzupełniającym ww. politykę jest KZSZ. W załączniku nr 1 do KZSZ - *Słownik pojęć zintegrowanego systemu zarządzania* zdefiniowano bezpieczeństwo informacji jako zachowanie poufności, integralności, dostępności i rozliczalności informacji. 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.

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.

Zgodnie z PZSZ, wszyscy pracownicy urzędu zostali zobowiązani do zapoznania się z ww. polityką, która udostępniana jest za pomocą systemu obiegu dokumentacji (dalej: SOD), poczty elektronicznej i/lub tablic ogłoszeń w intranecie. Pracownicy ponadto zostali zobligowani do jej stosowania w trakcie wykonywania obowiązków służbowych.

W trakcie audytu potwierdzono, iż pracownicy urzędu poprzez złożenie podpisu 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 te regulacje do stosowania.

Nowo zatrudnieni pracownicy zapoznają się z zakresem ZSZ, w tym polityką ZSZ w ramach procedury przygotowawczej. Nowo zatrudnieni pracownicy składają podpis na indywidualnych *Oświadczeniach o odpowiedzialności* (wzór stanowi załącznik nr 12 do PODO), 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, pracownicy składają oświadczenie (wg załącznika nr 11 do PODO), potwierdzające, 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.*

Na podstawie losowo wybranej próby pracowników UMWSL potwierdzono:

- złożenie oświadczeń potwierdzających realizację szkolenia z zasad bezpieczeństwa i ochrony danych osobowych (np. oświadczenie z dnia 01.07.2019 r.),
- złożenie oświadczeń o odpowiedzialności (np. oświadczenie z dnia 01.07.2019 r.).

W intranecie urzędu, w zakładce *zintegrowany system zarządzania,* udostępniona została dla pracowników urzędu dokumentacja składająca się na zintegrowany system zarządzania.

Zgodnie z zapisami pkt. 5.3 KZSZ, w urzędzie funkcjonuje Komitet Bezpieczeństwa Urzędu (dalej: KBU). Zadaniem ww. komitetu jest bieżący monitoring poziomu bezpieczeństwa informacji w urzędzie oraz dbanie o to, aby wymagania bezpieczeństwa były zidentyfikowane i uwzględnione w procesach i systemach teleinformatycznych funkcjonujących w urzędzie. Przewodniczącym KBU jest Dyrektor urzędu (osoba zatrudniona na stanowisku Dyrektora Wydział Administracji). Obligatoryjnymi członkami Komitetu są: IOD, główny administrator systemu informatycznego (dalej: GASI), osoba z komórki koordynującej zarządzanie ryzykiem w urzędzie oraz osoba odpowiedzialna za audyt w urzędzie. KBU zbiera się

cyklicznie, raz na kwartał lub zgodnie z bieżącymi potrzebami. KBU pełni kluczową rolę w procesie zarządzania ciągłością działania urzędu – patrz pkt 11.1.1 niniejszego sprawozdania.

Zespołowi audytowemu przedłożono notatkę z ostatniego posiedzenia KBU nr 2/2019 z dnia 19.04.2019 r. wraz z załącznikami:

- załącznikiem nr 1 – zestawienie zdarzeń bezpieczeństwa informacji za I kwartał 2019 r.,
- załącznikiem nr 2 – zestawienie zadań do realizacji w wyniku obrad Komitetu Bezpieczeństwa Informacji.

W toku audytu ustalono:

Ustalenie nr 2	W urzędzie Uchwałą nr 1514/53/VI/2019 Zarządu Województwa Śląskiego z dnia 03.07.2019 r. przyjęty został zmieniony *Regulamin organizacyjny UMWSL*, wprowadzający szereg zmian w strukturze organizacyjnej urzędu. Zgodnie z ww. regulaminem, w pionie Inspektora ochrony danych powstaje Zespół IOD oraz powołano zastępcę IOD. Rozszerzono ponadto zakres pomieszczeń o podwyższonym poziomie ochrony, m. in. o pomieszczenia pracowników helpdesku oraz sieci informatycznych. Powyższe zmiany nie zostały uwzględnione w dokumentacji składającej się na ZSZ.
Kategoria	Kategoria 1 – System funkcjonuje prawidłowo. Nie są potrzebne żadne lub potrzebne są tylko niewielkie usprawnienia.
Rekomendacja	Zaleca się przeprowadzenie przeglądu dokumentacji ZSZ pod kątem wprowadzonych w dokumentach pobocznych zmian, w tym m.in. w obszarze struktury organizacyjnej oraz wyznaczenia nowych obszarów o podwyższonym poziomie ochrony.
Stanowisko IZ	Dokumentacja ZSZ została zaktualizowana, uwzględniając zmiany organizacyjne, w tym rozszerzyła opisy dotyczące nowych obszarów o podwyższonym poziomie ochrony. Zmiany zostały przyjęte Zarządzeniami Marszałka z dnia 19 sierpnia 2019 r.
Stanowisko Instytucji Audytowej	**Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up.**

1.1.2. Przegląd polityki bezpieczeństwa informacji

Zgodnie z zapisami pkt 9.1.1.10 *Monitorowanie stanu bezpieczeństwa informacji,* KBU w kwartalnych cyklach lub zgodnie z potrzebami realizuje przegląd stanu bezpieczeństwa informacji i obejmuje następujące zagadnienia:

- zapewnienie, że ryzyka w obszarze bezpieczeństwa informacji za zarządzane,

- przegląd rejestru zdarzeń i incydentów w celu wyciągnięcia wniosków z incydentów związanych z bezpieczeństwem informacji,
- weryfikacja i zatwierdzanie 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.

W trakcie audytu, na podstawie *Notatki z posiedzenia KBU nr 2/2019* z dnia 19.04.2019 r., potwierdzono powyższe zapisy.

Zgodnie z zapisami pkt 5 *Przywództwo* KZSZ, w ramach monitorowania i sprawozdawczości w zakresie ZSZ, raz w roku kierownictwo 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 urzędu 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.

W toku audytu potwierdzono dokonanie przeglądu zintegrowanego systemu zarządzania. Powyższe udokumentowano w:

- *Protokole z przeglądu zintegrowanego systemu zarządzania za okres od 01.01.2018 r. do 31.12.2018 r.* z marca 2019 r.,
- *Raporcie na przegląd zintegrowanego systemu zarządzania za okres od 01.01.2018 r. do 31.12.2018 r.* z marca 2019 r.

Ostatnia pełna aktualizacja dokumentacji składającej się na zintegrowany system zarządzania została wprowadzona Zarządzeniem nr 00082/18 Marszałka Województwa Śląskiego z dnia 19.09.2018 r. W roku 2019 Uchwałą nr 550/28/VI/2019 Zarządu Województwa Śląskiego z dnia 20.03.2019 r. zaktualizowano *Politykę Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego* (treść dokumentu nie została zmieniona, aktualizacja w związku ze zmianą na stanowisku Marszałka Województwa Śląskiego).

2. Bezpieczeństwo zasobów ludzkich

2.1. Podczas zatrudnienia

2.1.1. Uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji

Nowo zatrudnieni pracownicy są przygotowywani do należytego wykonywania obowiązków m.in. w ramach szkoleń wstępnych oraz w formie służby

przygotowawczej, która przeprowadzana jest na podstawie zarządzenia Marszałka i kończy się egzaminem.

Zgodnie z uzyskanymi informacjami, zakres szkolenia wstępnego obejmuje zagadnienia związane z ochroną danych osobowych oraz bezpieczeństwem informacji. Przeprowadzenie szkolenia wstępnego potwierdzane jest złożeniem podpisu na karcie obiegowej nowozatrudnionego pracownika przez osoby upoważnione w komórkach merytorycznych UMWSL. Ponadto, nowozatrudnieni pracownicy składają oświadczenia, w których m.in. oświadczają, że odbyli szkolenia z zakresu obowiązujących w UMWSL zasad bezpieczeństwa informacji oraz zasad ochrony danych osobowych. Powyższe potwierdzono na przykładzie losowo wybranych osób zatrudnionych w UMWSL od 1 lipca 2019 r.

Dodatkowo nowy pracownik zgodnie z powyższym zapisem zobowiązany jest odbyć służbę przygotowawczą. Obowiązek odbycia służby przygotowawczej wynika z ustawy o pracownikach samorządowych z dnia 21 listopada 2008 r. Szkolenie kończy się egzaminem. Pozytywny wynik egzaminu jest warunkiem niezbędnym do przedłużenia umowy o pracę w UMWSL. W trakcie prac audytowych w Referacie naboru i rozwoju pracowników potwierdzono odbycie służby przygotowawczej na przykładzie dokumentacji losowo wybranego pracownika UMWSL na podstawie:

- *Skierowania nr 02/2019 do odbycia służby przygotowawczej* z 15.01.2019 r.,
- *Wyboru opiekuna ds. adaptacji* z 15.01.2019 r.,
- *Harmonogramu służby przygotowawczej*,
- *Skierowania nr 02/2019 na egzamin pisemny kończący służbę przygotowawczą* z dnia 15.01.2019 r.,
- *Skierowania nr 02/2019 na egzamin ustny kończący służbę przygotowawczą* z dnia 15.01.2019 r.,
- *Protokołu z egzaminu ustnego kończącego służbę przygotowawcza w UMWSL w Katowicach* z 07.02.2019 r.,
- *Zaświadczenia o odbyciu służby* przygotowawczej *w UMWSL oraz złożeniu egzaminu końcowego z wynikiem pozytywnym* z 08.02.2019 r.

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 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 w zakładce *zintegrowany system zarządzania/szkolenia*. W 2019 r. ww. szkolenia odbyły się: 30 stycznia, 25 lutego, 26 marca, 25 kwietnia, 31 maja oraz 14 czerwca. Pracownicy w dniu szkolenia podpisują listę obecności, co potwierdzono na podstawie listy obecności dotyczącej szkolenia wewnętrznego przeprowadzonego w dniu 14.06.2019 r. w zakresie bezpieczeństwa przetwarzania informacji i ochrony danych osobowych.

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 zatrudnionych pracowników z 01.07.2019 r. oraz 04.07.2019 r. W UMWSL do prowadzenia ewidencji upoważnień do przetwarzania danych osobowych wykorzystuje się system informatyczny eORG.

potwierdzono stosowanie opisanych powyżej [illegible]

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:

- dla beneficjentów/wnioskodawców:
  - *Instrukcja użytkownika Lokalnego Systemu Informatycznego 2014 dla wnioskodawców/beneficjentów RPO WSL 2014-2020* wersja 1.4.1,
  - *Instrukcja dodawania i zmiany załączników we wniosku o dofinansowanie,*
  - *Regulamin użytkownika Lokalnego Systemu Informatycznego Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020 (LSI2014),*
  - *Wymagania techniczne i konfiguracja przeglądarek internetowych.*

- *Instrukcja jak wybrać mocne hasło i jak je chronić,*
- *Instrukcja chcę odzyskać dostęp do systemu,*
- *Instrukcja chcę dać dostęp do mojego profilu: wspólnikowi, współpracownikowi, firmie konsultingowej.*

– dla pracowników i ekspertów – instrukcje przygotowywane są w ramach kompetencji IOK dot. EFS, np.:

- *Instrukcja wypełniania karty oceny formalno-merytorycznej oraz merytorycznej dla oceniających w ramach Lokalnego Systemu Informatycznego RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,*
- *Instrukcja obsługi wniosku o płatność w ramach Lokalnego Systemu Informatycznego 2014 dla operatorów RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,*
- *Instrukcja obsługi modułu korekt zatwierdzania wniosku o płatność dla operatorów w ramach Lokalnego Systemu Informatycznego 2014 RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,*
- *Instrukcja operatora Lokalnego Systemu Informatycznego LSI 2014 moduł – kontrole projektu,*
- *Instrukcja obsługi KOP dla operatorów w ramach Lokalnego Systemu Informatycznego 2014 RPO WSL 2014-2020 w części dotyczącej współfinansowania,*
- *Instrukcja wypełniania modułów nabory, projekty, wnioski o dofinansowanie, umowy w ramach Lokalnego Systemu Informatycznego 2014 dla operatorów RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,*
- *Instrukcja obejmująca zmiany w module kontroli w ramach Lokalnego Systemu Informatycznego 2014 dla operatorów RPO WSL 2014-2020 w części dotyczącej współfinansowania z EFS,*

Szczegółowe informacje dotyczące systemu znajdują się w dokumentacji umieszczonej na stronie: https://rpo.slaskie.pl/czytaj/lokalny_system_informatyczny 2014.

6.1.2. Zarządzanie zmianami

W załączniku nr 12 *Zasady zarządzania zmianami IT* do Zarządzenia nr 00082/2018 Marszałka Województwa Śląskiego z dnia 19.09.2018 r. opisano sposób zarządzania zmianami oraz wydaniami w usługach informatycznych w UMWSL.

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 w UMWSL wykorzystuje się system MantisBT, który jest zintegrowany z systemem GIT. Za zbieranie informacji na temat zmian, analizę potrzeb oraz opracowanie zgłoszeń (w tym zgłoszeń użytkowników/ beneficjentów) odpowiada Referat projektowania i rozwoju systemów informatycznych. Zgodnie z uzyskanymi informacjami zarządzanie procesami zmian oparte jest o strukturę SCRUM. Rozwój planowanej zmiany podzielony jest na trwające jeden tydzień iteracje, zwane sprintami. W uzasadnionych przypadkach (np. okres wakacyjny), okres pomiędzy sprintami może zostać wydłużony. Po każdym sprincie (co do zasady w każdy poniedziałek) sporządzana jest *Notatka ze spotkania cyklicznego grupy roboczej ds. LSI*. Powyższe IA potwierdziła na przykładzie notatki z 12.05.2019 r., notatki z 24.06.2019 r., notatki z 08.07.2019 r. W systemie MantisBT odnotowywane są informacje na temat zgłoszenia zmiany, realizację zmiany przez programistów. Testy w pierwszej kolejności wykonane przez pracowników Referatu projektowania i rozwoju systemów, 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.

9. Relacje z dostawcami

9.1. Zarządzanie usługami świadczonymi przez dostawców

9.1.1. 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 (ang. Service Level Agreement) podlegające monitorowaniu, np. czas na reakcję, czas na usunięcie awarii, dostępność systemu. Z uzyskanych informacji wynika, iż obecnie system LSI utrzymywany jest siłami własnymi urzędu.

W ramach usług świadczonych przez dostawców zawarto następujące umowy:

- *Umowę nr 5019/OR/2018* z dnia 30.10.2018 r. zawartą z SITEL Spółka z o.o. na świadczenie usług stałego dostępu do sieci INTERNET, umowa zawarta na czas określony od 01.01.2019 r. do 30.09.2021. r.,
- *Umowę nr 4794/OR/2018* z dnia 17.10.2018 r. zawartą z Konsorcjum (3S Data Center S.A., 3S S.A. SITEL Spółka z o.o. na świadczenie usługi kolokowania urządzeń oraz dostępu do punktu wymiany ruchu sieciowego dla Urzędu Marszałkowskiego Województwa Śląskiego, umowa zawarta na czas określony od 01.12.2018 r. do 30.09.2021. r.,
- *Umowę nr 3475/OR/2017* z dnia 03.11.2017 zawartą z 3S Spółka Akcyjna w zakresie dzierżawy łączy światłowodowych, umowa zawarta na czas określony od 01.01.2018 r. do 31.12.2020 r.,
- *Umowę nr 3424/OR/2018* z dnia 10.08.2018 r. zawartą z Intaris Sp. z o.o. 3S Spółka Akcyjna na jednorazową dostawę sprzętu komputerowego z gwarancją 60 miesięcy licząc od dnia podpisania bez zastrzeżeń protokołu odbioru przedmiotu umowy.

W wyniku analizy treści ww. umów potwierdzono, iż w umowach znajdują się zapisy regulujące zasady współpracy, które obowiązują strony, zdefiniowano warunki realizacji umowy oraz sposób realizacji zgłoszenia, w przypadku

wystąpienia awarii. Podstawą wypłaty wynagrodzenia jest przekazanie przez wykonawcę protokołu odbiorczego lub protokołu zdawczo-odbiorczego.

12. Zgodność

12.1. Zgodność z wymaganiami prawnymi i umownymi

12.1.1. 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. IOD, 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.

Z uzyskanych informacji od IOD oraz na podstawie analizy zapisów *Regulaminu organizacyjnego* wprowadzonego w UMWSL uchwałą nr 1514/53/VI/2019 z 3 lipca 2019 r. w urzędzie ma funkcjonować pion Inspektora ochrony danych. Do zakresu działania pionu będą należały sprawy związane z bezpieczeństwem i ochroną danych osobowych, w tym w szczególności:

- wypełnianie obowiązków określonych w rozporządzeniu o ochronie danych – RODO,
- monitorowanie przestrzegania rozporządzenia o ochronie danych – RODO,
- współpraca z komórkami organizacyjnymi urzędu w zakresie związanym z bezpieczeństwem, danych osobowych oraz w zakresie doskonalenia ochrony danych osobowych.

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* stanowiąca załącznik do *Zarządzenia nr 00084/2018 Marszałka Województwa Śląskiego* z dnia 19.09.2018 r.). Proces zarządzania ryzykiem został opisany również w pkt 10.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami.