



RZECZPOSPOLITA POLSKA
MINISTERSTWO FINANSÓW
Szef Krajowej Administracji Skarbowej

DAS10.9011.14.2021.3.HQCT

Sprawozdanie
z audytu bezpieczeństwa Lokalnego Systemu
Informatycznego LS001 wykorzystywanego
przy wdrażaniu Regionalnego Programu Operacyjnego
Województwa Śląskiego

(NR KODU CCI 2014PL16M2OP012)

Warszawa, listopad 2021 roku

Spis treści

I.	WSTĘP.....	3
I.1.	CEL SPRAWOZDANIA.....	3
I.2.	ORGAN ODPOWIEDZIALNY ZA SPORZĄDZENIE SPRAWOZDANIA	3
I.3.	PODSUMOWANIE USTALEŃ	4
II.	METODYKA I ZAKRES PRAC AUDYTOWYCH.....	5
II.1.	RAMY CZASOWE AUDYTU.....	6
II.2.	ZAKRES WYKONANYCH PRAC	6
III.	WYNIKI OCENY.....	11
III.1.	KRYTERIUM OCENY NR 23 (6.1): KLUCZOWEGO WYMOGU KONTROLNEGO NR 6.....	11
III.2.	KRYTERIUM OCENY NR 24 (6.2): KLUCZOWEGO WYMOGU KONTROLNEGO NR 6.....	11
III.3.	KRYTERIUM OCENY NR 25 (6.3): KLUCZOWEGO WYMOGU KONTROLNEGO NR 6.....	11
1.	POLITYKI BEZPIECZEŃSTWA INFORMACJI	12
2.	BEZPIECZEŃSTWO ZASOBÓW LUDZKICH.....	15
3.	KONTROLA DOSTĘPU.....	17
4.	KRYPTOGRAFIA.....	25
5.	BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE	26
6.	BEZPIECZNA EKSPLOATACJA	32
7.	BEZPIECZEŃSTWO KOMUNIKACJI.....	40
8.	POZYSKIWANIE, ROZWÓJ I UTRZYMANIE SYSTEMÓW	41
9.	RELACJE Z DOSTAWCAMI	42
10.	ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI	44
11.	ASPEKTY BEZPIECZEŃSTWA INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA.....	48
12.	ZGODNOŚĆ.....	51
IV.	AUDYT FOLLOW-UP	52

I. WSTĘP

I.1. CEL SPRAWOZDANIA

Art. 127 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013¹, 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 finansowego²,
- 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 każdego 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 w Ministerstwie Finansów oraz komórek organizacyjnych zlokalizowanych w 16 Izbach Administracji Skarbowej. Jest on również odpowiedzialny za zatwierdzenie przedmiotowego sprawozdania.

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. 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 oraz uchylające rozporządzenie Rady (WE) nr 1083/2006.

² Rozporządzenie 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 uchylające rozporządzenie (UE, Euratom) nr 966/2012.

I.3. PODSUMOWANIE USTALEŃ

Audyt systemu dla Regionalnego Programu Operacyjnego Województwa Śląskiego został przeprowadzony zgodnie ze Strategią audytu Regionalnego Programu Operacyjnego Województwa Śląskiego oraz 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 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 SL2014.

Dla kryterium oceny nr 25 (6.3) wydano 1 rekomendację w kategorii 1. Brak rekomendacji otwartych z lat ubiegłych.

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

W związku z powyższym kluczowy wymóg kontrolny nr 6 został oceniony w kategorii 1 – **System funkcjonuje prawidłowo. Nie są potrzebne żadne lub potrzebne są tylko niewielkie 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 wydanego zalecenia 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 okresie lipiec – październik 2021 r.

II.2. ZAKRES WYKONANYCH PRAC

Prace przeprowadzone zostały w Instytucji Zarządzającej Regionalnym Programem Operacyjnym 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. uzupełniające 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 osiągnięciu 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 27001:2017 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 wspomaganie realizacji Regionalnego Programu Operacyjnego Województwa Śląskiego w perspektywie 2014-2020 (dalej: RPO). 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 departament 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:

Sprawozdanie z audytu bezpieczeństwa Lokalnego Systemu Informatycznego LS001 wykorzystywanego przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Śląskiego.

- pracowników 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,
- pracowników Zintegrowanych Inwestycji Terytorialnych oraz Regionalnych Inwestycji Terytorialnych.
- 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:

- Deklaracji stosowania stanowiącej załącznik 1 do zarządzenia 40/21 z 26.03.2021 r. (wydanie 3),
- Zarządzenia nr 43/21 dotyczącego przyjęcia dokumentacji regulującej funkcjonowanie systemu bezpieczeństwa informatycznego w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego z 26 marca 2021 r.,
- Zarządzenia nr 42/21 dotyczącego przyjęcia Polityki Ochrony Danych Osobowych w Urzędzie Marszałkowskim Województwa Śląskiego z 26 marca 2021 r.,
- Zarządzenia nr 41/21 dotyczącego przyjęcia Księgi Zintegrowanego Systemu w Urzędzie Marszałkowskim Województwa Śląskiego z 26 marca 2021 r.,
- Zarządzenia nr 40/21 dotyczącego przyjęcia dokumentacji zarządzania systemem bezpieczeństwa informacji zgodnie z wymaganiami normy ISO 27001:2017 w Urzędzie Marszałkowskim Województwa Śląskiego z 26 marca 2021 r.,
- Polityki Ochrony Danych Osobowych stanowiącej załącznik do zarządzenia 106/2019 z 19.08.2019 r. (wydanie 2),
- Polityki Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego z 20 marca 2019 r.,
- Pisma znak: RR-RAS.44.10.2021 z dnia 27 października 2021 r., zawierającego stanowisko Instytucji Zarządzającej na wyniki ujęte w sprawozdaniu wstępnym,
- Instrukcji udostępniania profilu: współpracownikowi, firmie konsultingowej,
- Instrukcji Zarządzania Systemem Informatycznym stanowiącej załącznik 1 do zarządzenia 43/21 z 26.03.2021 r. (wydanie 3),

Sprawozdanie z audytu bezpieczeństwa Lokalnego Systemu Informatycznego LS001 wykorzystywanego przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Śląskiego.

- Instrukcji użytkownika Lokalnego Systemu Informatycznego 2014 dla wnioskodawców/beneficjentów RPO WSL 2014-2020,
- Instrukcji odzyskania dostępu do systemu,
- Instrukcji wybierania mocnego hasła i wskazówek jak je chronić,
- Instrukcji użytkownika stanowiącej załącznik 2 do zarządzenia 40/21 z 26.03.2021 r. (wydanie 4),
- Instalacji i konfiguracji systemu LSI WSL 2014-2020,
- Księgi Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego,
- Harmonogramu testowego odtworzenia systemów z kopii bezpieczeństwa,
- Testu SSL wykonanego w 30.07.2021r.,
- Raportu z okresowego przeglądu uprawnień w systemie informatycznym LSI z 23.12.2020 r.,
- Raportu z przeglądów i testów infrastruktury firmy 3S z 06.09.2021r.,
- Rejestru testowego odtworzenia systemów z kopii bezpieczeństwa,
- Odpowiedzi na rekomendację otwarte Urzędu Marszałkowskiego Województwa Śląskiego przekazanych w piśmie, nr. RPW/80902/2021,
- Oświadczeń o odpowiedzialności i poufności dla losowych pracowników,
- Oświadczeń o przejściu szkolenia wstępnego dla losowo wybranych pracowników,
- Oświadczeniu o przyjęciu funkcji administratora merytorycznego,
- Planu Ciągłości Działania i protokołu z uruchomienia planu ciągłości działania z 24.06.2021 r. dla planów odtworzenia systemów kopii zapasowych danych, awarii łączy teleinformatycznych, niedostępności lokalizacji, przeniesienia systemów IT do innej lokalizacji i przywracania systemów IT po incydencie,
- Prezentacji RODO ze szkolenia wewnętrznego dla pracowników,
- Prezentacji z bezpieczeństwa informacji,
- Protokołu z konserwacji systemu gaszenia gazem w serwerowni Urzędu Marszałkowskiego Województwa Śląskiego z 30.06.2021 r.,
- Protokołu z przeglądu klimatyzacji w serwerowni Urzędu Marszałkowskiego Województwa Śląskiego z 28.05.2021 r.,
- Protokołu zdawczo-odbiorczego komisyjnego przekazania do użytku infrastruktury telekomunikacyjnej,
- Protokołu z przeglądu zintegrowanego systemu zarządzania za 2020 r. z 29.03.2021 r.,
- Protokołu zdawczo-odbiorczego zgodnie z umową na „świadczenie usługi kolokowania urzędzeń oraz dostępu do punktu wymiany ruchu sieciowego dla UMWSL” z 1.12.2018 r.,

Sprawozdanie z audytu bezpieczeństwa Lokalnego Systemu Informatycznego LS001 wykorzystywanego przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Śląskiego.

- Procedury zarządzania dostępem i uprawnieniami stanowiącej załącznik 4 do Zarządzenia nr 40/21 z 26.03.2021 r. (wydanie 3),
- Procedury postępowania ze zdarzeniami bezpieczeństwa informacji stanowiącej załącznik 3 do Zarządzenia nr 40/21 z 26.03.2021 r. (wydanie 2),
- Polityki zarządzania ciągłością działania stanowiącej załącznik 4 do zarządzenia 43/21 z 26.03.2021 r. (wydanie 3),
- Uchwały nr 550/28/VI/2019 w sprawie przyjęcia polityki zintegrowanego systemu zarządzania Urzędu Marszałkowskiego Województwa Śląskiego,
- Upoważnienia do przetwarzania danych osobowych dla losowo wybranych pracowników,
- Umowy kolokacyjną pomiędzy firmą 3S, a Urzędem Marszałkowskim Województwa Śląskiego z 17.10.2018r.,
- Umowy nr 3408/CI/2021 zawartej w dniu 19.08.2021 r. z konsorcjum (3S Data Center S.A., 3S S.A.),
- Umowy pomiędzy firmą Sitel, a Urzędem Marszałkowskim z 30.10.2018r. odnośnie dostępu do sieci Internet dla urzędu,
- Załącznika numer 1 do procedury postępowania incydentami: rejestr zdarzeń i słabości z lat 2020 i 2021,
- Zasad zarządzania LSI 2014 w ramach RPO WSL 2014-2020 w wersji 4.0 z czerwca 2020 r.,
- Zakresu obowiązków i odpowiedzialności dla Inspektora Ochrony Danych,
- Zawiadomienia o wyznaczeniu nowego Inspektora Ochrony Danych,
- Zarządzenia nr 109/19 odnośnie wprowadzenia procedury zarządzania ryzykiem w Urzędzie Marszałkowskim Województwa Śląskiego z 19 sierpnia 2019 r.,
- Zrzutu ekranu z blokady strony youtube.pl,
- Zrzutu ekranu z zestawienia systemów urzędu.
- Zrzutu ekranu z narzędzia VDP,
- Zrzutu ekranu z dziennika systemowego,
- Zrzutu ekranu z GitLaba'a,
- Zrzutu ekranu z polityki haseł domeny,
- Zrzutu ekranu z ustawień wygaszacza ekranu Windows,
- Zrzutu ekranu z ustawień i konfiguracji anty-wirusa,
- Zrzutu ekranu z ustawień zegara synchronizacji czasu,
- Zrzutów ekranu z ustawień i harmonogramu wykonywania kopii zapasowych,
- Zrzutów ekranu z programu Zabbix,

Sprawozdanie z audytu bezpieczeństwa Lokalnego Systemu Informatycznego LS001 wykorzystywanego przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Śląskiego.

- Zrzutów ekranu z systemu powiadomień OSSIM informującym o incydencie w systemie,
- Zrzutów ekranu z ustawień i konfiguracji firewall'a,
- Zrzutów ekranu z systemu LSI RPO,
- Wymagań technicznych i konfiguracji przeglądarek internetowych dla użytkowników systemu LSI,
- Wniosku o nadanie zdalnego dostępu dla użytkownika,
- Wniosków o nadanie, zmianę, odebranie uprawnień dla losowo wybranych użytkowników,
- Wykazu nośników zlikwidowanych,
- Wykazu osób wyznaczonych z Urzędu Marszałkowskiego Województwa Śląskiego do kontaktu z zespołem kontrolującym.

Przeprowadzono wywiady z pracownikami:

- Inspektorem Ochrony Danych (IOD),
- Kierownikiem Referatu Analiz Systemu Realizacji RPO WSL w Departamencie Rozwoju Regionalnego,
- Inspektorem, Referatu Analiz Systemu Realizacji RPO WSL w Departamencie Rozwoju Regionalnego,
- Kierownikiem Referatu Zarządzania Infrastrukturą Teleinformatyczną w Departamencie Cyfryzacji i Informatyki,
- Starszym administratorem Referatu Zarządzania Infrastrukturą Teleinformatyczną w Departamencie Cyfryzacji i Informatyki,
- Kierownikiem Referatu Obsługi Technicznej i Serwisu w Departamencie Cyfryzacji i Informatyki,
- Kierownikiem Referatu Projektowania i Rozwoju Systemów Informatycznych w Departamencie Cyfryzacji i Informatyki,
- Pracownikiem firmy 3S.

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,

Sprawozdanie z audytu bezpieczeństwa Lokalnego Systemu Informatycznego LS001 wykorzystywanego przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Śląskiego.

- sprawdzono ustawienia firewall-a,
- sprawdzono wykonywanie backup-u,
- przeprowadzono testy mechanizmów kontrolnych systemu LSI 2014.

Przeprowadzono wizyty w:

- Urzędzie Marszałkowskim Województwa Śląskiego,
- Centrum Danych 3S Data Center S.A. zlokalizowanym przy ul. Gospodarczej 12 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, 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 i zawierania umów o dofinansowanie w zakresie Regionalnego Programu Operacyjnego Województwa Śląskiego. 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 systemu informatycznego SL2014.

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

Obszar audytu Lokalnego Systemu Informatycznego 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,

Sprawozdanie z audytu bezpieczeństwa Lokalnego Systemu Informatycznego LS001 wykorzystywanego przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Śląskiego.

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 przeprowadzonych czynności ... ino:

Zastępca Szefa
Krajowej Administracji Skarbowej

Anna Chatupa
/podpisano kwalifikowanym
podpisem elektronicznym/

