RZECZPOSPOLITA POLSKA

MINISTERSTWO FINANSÓW

Szef Krajowej Administracji Skarbowej

DAS10.9011.22.2023

Sprawozdanie z audytu bezpieczeństwa Lokalnego Systemu Informatycznego (LS001) wykorzystywanego przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Śląskiego 2014-2020

CCI 2014PL16M2OP006

Warszawa, listopad 2023 r.

Spis treści

I. WSTĘP

I.1. CEL SPRAWOZDANIA

Art. 127 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/20131 nakłada na Instytucję Audytową (IA) 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 finansowego[2],

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

Dokumenty, o których mowa powyżej przekazywane są Komisji do dnia 15 lutego każdego roku obrachunkowego.

System zarządzania i kontroli Regionalnego Programu Operacyjnego Województwa Śląskiego 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 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 uchylającego rozporządzenie Rady (WE) nr 1083/2006.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE, EURATOM) 2018/1046 z dnia 18 lipca 2018 roku w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające 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 bezpieczeństwa Centralnego Systemu Teleinformatycznego (CST) 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 podczas audytu bezpieczeństwa CST.

Dla kryterium oceny nr 25 (6.3) wydano 4 rekomendacje w kategorii 1. Wszystkie rekomendacje z lat ubiegłych zostały wdrożone. Nie zidentyfikowano rekomendacji niewdrożonych 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.	Bezpieczeństwo Zasobów Ludzkich	-	-	-	-	1
2.	Kontrola dostępu	1	-	-	-	1
3.	Bezpieczeństwo fizyczne i środowiskowe	1	-	-	-	1
4.	Bezpieczna eksploatacja	1	-	-	-	1
5.	Bezpieczeństwo komunikacji	1	-	-	-	1
6.	Pozyskiwanie, rozwój i utrzymanie systemów	-	-	-	-	1
7.	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	-	-	-	-	1
8.	Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	-	-	-	-	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 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 okresie lipiec – listopad 2023 r.

II.2. ZAKRES WYKONANYCH PRAC

Prace przeprowadzone zostały w Instytucji Zarządzającej Regionalnym Programem Operacyjnym Województwa Śląskiego – Urzędzie Marszałkowskim Województwa Śląskiego w Katowicach (dalej: IZ, urząd lub UMWSL).

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 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 27001:2017 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 (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 LSI odpowiada Departament Cyfryzacji i Informatyki Urzędu Marszałkowskiego Województwa Śląskiego. System utrzymywany jest na infrastrukturze własnej urzędu zlokalizowanej w Centrum Przetwarzania Danych (CPD) firmy 3S Data Center S.A. (serwerownia główna LSI2014). System zapewnia obsługę konkursów dofinansowanych ze środków EFRR i EFS. Dostępny jest dla:

- pracowników Urzędu Marszałkowskiego Województwa Śląskiego,

- 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:

- Zarządzenia nr 5/23 Marszałka Województwa Śląskiego z 05.01.2023 r. w sprawie przyjęcia dokumentacji zarządzania systemem bezpieczeństwa informacji zgodnie z wymaganiami normy ISO 27001:2017 w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,
- Zarządzenia nr 73/23 Marszałka Województwa Śląskiego z 05.01.2023 r. w sprawie zmiany zarządzenia nr 5/23 przyjęcia dokumentacji zarządzania systemem bezpieczeństwa informacji zgodnie z wymaganiami normy ISO 27001:2017 w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,
- Zarządzenia nr 4/23 Marszałka Województwa Śląskiego z 05.01.2023 r. w sprawie przyjęcia Księgi Zintegrowanego Systemu Zarządzania oraz Procedury auditu wewnętrznego w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,
- Zarządzenia nr 6/23 Marszałka Województwa Śląskiego z 05.01.2023 r. w sprawie przyjęcia Polityki Ochrony Danych Osobowych w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,
- Zarządzenia nr 41/21 Marszałka Województwa Śląskiego z 26.03.2023 r. w sprawie przyjęcia Księgi Zintegrowanego Systemu Zarządzania oraz procedur podstawowych w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,
- Zarządzenia nr 40/21 Marszałka Województwa Śląskiego z 26.03.2021 r. w sprawie przyjęcia dokumentacji zarządzania systemem bezpieczeństwa informacji zgodnie z wymaganiami normy ISO 27001:2017 w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,
- Zarządzenia nr 42/21 Marszałka Województwa Śląskiego z 26.03.2021 r. w sprawie przyjęcia Polityki Ochrony Danych Osobowych w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,

- Uchwały nr 550/28/VI/2019 Zarządu Województwa Śląskiego z 20.03.2019 r. w sprawie przyjęcia Polityki Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego,
- Deklaracji stosowania (wydanie 3) stanowiącej załącznik nr 1 do zarządzenia nr 5/23 Marszałka Województwa Śląskiego z 05.01.2023 r.,
- Procedury Zarządzania Dostępem i Uprawnieniami (wydanie 4, dalej: PZDiU), stanowiącej załącznik nr 4 do zarządzenia nr 5/23 Marszałka Województwa Śląskiego z 05.01.2023 r.,
- Instrukcji Zarządzania Kartami Identyfikacyjnymi (wydanie 1) stanowiącej załącznik nr 5 do zarządzenia nr 5/23 Marszałka Województwa Śląskiego z 05.01.2023 r.,
- Procedury Postępowania ze Zdarzeniami Bezpieczeństwa Informacji (wydanie 4, dalej: PPZBI) stanowiącej załącznik nr 3 do zarządzenia nr 5/23 Marszałka Województwa Śląskiego z 05.01.2023 r.,
- Polityki Ochrony Danych Osobowych (wydanie 2) wprowadzonej Zarządzeniem Marszałka Województwa Śląskiego nr 42/21 z 26.03.2021 r.,
- Polityki Ochrony Danych Osobowych (wydanie 3, dalej PODO) wprowadzonej Zarządzeniem Marszałka Województwa Śląskiego nr 6/23 z 05.01.2023 r.,
- Instrukcji Użytkownika (wydanie 6, dalej: IU) stanowiącej załącznik nr 2 do zarządzenia nr 73/23 Marszałka Województwa Śląskiego z 21.04.2023 r.,
- Księgi Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego (wydanie 3, dalej: KZSZ) stanowiącej załącznik nr 1 do zarządzenia nr 4/23 Marszałka Województwa Śląskiego z 05.01.2023 r.,
- Księgi Zintegrowanego Systemu Zarządzania Urzędu Marszałkowskiego Województwa Śląskiego (wydanie 2, dalej: KZSZ) stanowiącej załącznik nr 1 do zarządzenia nr 41/21 Marszałka Województwa Śląskiego z 26.03.2021 r.,
- Procedury auditu wewnętrznego (wydanie 3) stanowiącej załącznik nr 2 do zarządzenia nr 4/23 Marszałka Województwa Śląskiego z 05.01.2023 r.,
- Procedury działań korygujących (wydanie 2) stanowiącej załącznik nr 2 do zarządzenia nr 41/21 Marszałka Województwa Śląskiego z 26.03.2021 r.,
- Procedury auditu wewnętrznego (wydanie 2) stanowiącej załącznik nr 3 do zarządzenia nr 41/21 Marszałka Województwa Śląskiego z 26.03.2021 r.,
- Raportu z okresowego przeglądu uprawnień w systemie informatycznym wykonanego 26.06.2023 r.,
- Zasad zarządzania LSI 2014 w ramach RPO WSL 2014-2020 (wersja 4.0) stanowiącej załącznik nr 1 do uchwały Zarządu Województwa Śląskiego nr 1470/144/VI/2020z z 30.06.2020 r.,
- Załącznika do zarządzenia wewnętrznego nr 01/CI/2023 Dyrektora Departamentu Cyfryzacji i Informatyki z 07.03.2023 r.,
- Instrukcji użytkownika Lokalnego Systemu Informatycznego 2014 dla Wnioskodawców/Beneficjentów RPO WSL 2014-2020 (wersja 3.0 z 2020 r.),

- Instrukcji dla administratora systemu informatycznego LSI WSL 2014-2020 dotyczącej instalacji i konfiguracji systemu,
- Materiałów instruktażowych dotyczących Lokalnego Systemu Informatycznego dla użytkowników zamieszczonych na stronie lsi.slaskie.pl,
- Protokołu z przeglądu zintegrowanego systemu zarządzania za 2022 r., zatwierdzonego 29.03.2023 r. przez Marszałka Województwa Śląskiego,
- Raportu z przeglądu Zintegrowanego Systemu Zarządzania za 2022 r., zatwierdzonego 29.03.2023 r. przez Marszałka Województwa Śląskiego,
- Instrukcji Zarządzania Systemem Informatycznym (wydanie 4, dalej: IZSI) stanowiącej załącznik nr 1 do Zarządzenia nr 30/22 Marszałka Województwa Śląskiego z 18.03.2022 r.,
- Polityki Zarządzania Ciągłością Działania (wydanie 3, dalej: PZCD) wraz z załącznikami stanowiącej załącznik nr 4 do Zarządzenia nr 30/22 Marszałka Województwa Śląskiego z 18.03.2022 r.,
- Procedury Kopii Zapasowych (wydanie 3, dalej: PKZ) wraz z załącznikami stanowiącej załącznik nr 2 do Zarządzenia nr 30/22 Marszałka Województwa Śląskiego z 18.03.2022 r.,
- Zasad zarządzania zmianami i wydaniami IT stanowiącej załącznik nr 3 do Zarządzenia nr 30/22 Marszałka Województwa Śląskiego z 18.03.2022 r.,
- Umowy nr 2978/OR/2017 zawartej 09.09.2017 r., pomiędzy Województwem Śląskim, a Centrum Informatyki „Zeto" S.A. dotyczącej rozbudowy Lokalnego Systemu Informatycznego dla Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020 wraz z asystą techniczną i aktualizacją środowiska Systemu,
- Umowy nr 260/OR/2018 zawartej 05.02.2018 r. pomiędzy Województwem Śląskim, a Centrum Informatyki „Zeto" S.A. dotyczącej rozbudowy Lokalnego Systemu Informatycznego dla Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020 poprzez utworzenie modułu instrumenty finansowe,
- Umowy nr 3106/AI/2016 zawartej 03.12.2016 r. pomiędzy Województwem Śląskim, a Art4Net s.c. dotyczącej usługi standaryzacji oprogramowania Lokalnego Systemu Informatycznego dla Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020,
- Umowy nr 2064/RR/2016 zawartej 04.05.2016 r. pomiędzy Województwem Śląskim, a Alterout IT Sp. z o.o. dotyczącej asysty technicznej i utrzymania Systemu Informatycznego Wdrażania i Zarządzania Regionalnego Programu Operacyjnego Województwa Śląskiego,
- Umowy nr 4143/OR/2018 zawartej 11.09.2018 r. pomiędzy Województwem Śląskim, a Centrum Informatyki „Zeto" S.A. dotyczącej rozbudowy Lokalnego Systemu Informatycznego dla Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020,

- Umowy nr 2387/OR/2017 zawartej 09.06.2017 r. pomiędzy Województwem Śląskim, a Art4Net s.c. dotyczącej asysty technicznej Lokalnego Systemu Informatycznego dla Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020,
- Umowy nr 2475/RR/2014 zawartej 31.07.2014 r. pomiędzy Województwem Śląskim, a Art4Net s.c. dotyczącej wytworzenia, uruchomienia, asysty technicznej i utrzymania Lokalnego Systemu Informatycznego dla Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020,
- Wyników testu SSL weryfikującego stosowane protokoły dla strony Lokalnego Systemu Informatycznego, dostępnej pod adresem lsi.slaskie.pl wykonanego przez IA 23.08.2023 r. oraz 29.08.2023 r.,
- Upoważnień do przetwarzania danych osobowych dla pracowników Urzędu Marszałkowskiego Województwa Śląskiego (próba 25 pracowników),
- Zrzutów ekranu z systemu eOrg prezentujących datę oraz tematykę szkolenia dla pracowników Urzędu Marszałkowskiego Województwa Śląskiego (25 zrzutów ekranu),
- Zrzutów ekranu z systemu eOrg prezentujących posiadane uprawnienia systemowe użytkowników Urzędu Marszałkowskiego Województwa Śląskiego (25 zrzutów ekranu),
- Wniosków o nadanie uprawnień do systemu informatycznego dla pracowników Urzędu Marszałkowskiego Województwa Śląskiego (25 wniosków),
- Oświadczeń o odbyciu szkoleń wstępnych dla pracowników Urzędu Marszałkowskiego Województwa Śląskiego (25 oświadczeń),
- Oświadczeń o odpowiedzialności i poufności dla pracowników Urzędu Marszałkowskiego Województwa Śląskiego (25 oświadczeń),
- Zrzutu ekranu z systemu helpdesk dotyczącego zgłoszenia incydentu bezpieczeństwa z 04.08.2023 r.,
- Korespondencji pomiędzy Inspektorem Ochrony Danych, a firmą związaną z incydentem bezpieczeństwa z 04.08.2023 r.,
- Korespondencji pomiędzy pracownikiem odpowiedzialnym za obsługę incydentu z referatu ds. zarządzania systemem bezpieczeństwa informacji a Inspektorem Ochrony Danych związaną z incydentem bezpieczeństwa z 04.08.2023 r.,
- Oceny zdarzenia z 08.08.2023 r. dotyczącej zgłoszonego incydentu bezpieczeństwa z 04.08.2023 r.,
- Oceny naruszenia ochrony danych osobowych stanowiącej załącznik nr 3 do PPZBI dotyczącej zgłoszonego incydentu bezpieczeństwa z 04.08.2023 r.,
- Certyfikatu ISO 9001:2015 (ważnego do 02.04.2025 r.) wystawionego dla Centrum Przetwarzania Danych 3S Data Center S.A. przez IAF (International Accreditation Forum) oraz UKAS (United Kingdom Accreditation Servic),
- Certyfikatu ISO 27001:2013 (ważnego do 31.10.2025 r.) wystawionego dla Centrum Przetwarzania Danych 3S Data Center S.A. przez IAF (International Accreditation

Forum), UKAS(United Kingdom Accreditation Servic) oraz SGS(Societe Generale de Surveillance),

- Certyfikatu ISO 27015:2015 (ważnego do 26.05.2026 r.) wystawionego dla Centrum Przetwarzania Danych 3S Data Center S.A. przez SGS (Societe Generale de Surveillance),
- Certyfikatu ISO 27018:2019 (ważnego do 26.05.2026 r.) wystawionego dla Centrum Przetwarzania Danych 3S Data Center S.A. przez SGS (Societe Generale de Surveillance),
- Zrzutów ekranu z firewall'a firmy PaloAlto prezentujących:
  - Kategoryzację stron i aplikacji w Urzędzie Marszałkowskim Województwa Śląskiego,
  - Odblokowane porty,
  - Uruchomione usługi w tym IPS(Intrusion Prevention System), IDS (Intrusion Detection System) oraz antyspam,
  - Logi przedstawiające próby ataków,
  - Logi przedstawiające ruch sieciowy pracowników urzędu.
- Zrzutów ekranu ze strony wewnętrznej urzędu (intranet) prezentujących:
  - Harmonogram szkoleń na rok 2023,
  - Prezentację ze szkoleń wewnętrznych,
  - Miejsce w intranecie gdzie zamieszczone są informacje o szkoleniach.
- Zrzutu ekranu ze strony dedykowanej dla Inspektora Ochrony Danych zamieszczonej na Sharepoincie,
- Zrzutu ekranu prezentującego ustawienia haseł dla kont domenowych z Active Directory,
- Zrzutu ekranu prezentującego ustawienia wygaszacza ekranu dla komputerów pracowników urzędu,
- Raportu zbiorczego z usługi WSUS-a (Windows Server Update Services) o stanie aktualizacji komputerów urzędu z grupy Windows 10,
- Zrzutów ekranu z konsol prezentujących wersję bazy danych systemu LSI oraz wersję oprogramowania systemu LSI,
- Zrzutu ekranu z oprogramowania Nessus, służącego do wyszukiwania podatności,
- Notatki z posiedzenia nr 1/2023 Komitetu Bezpieczeństwa Urzędu z 15.05.2023 r.,
- Listy uczestników szkolenia z bezpieczeństwa informacji i ochrony danych osobowych z 13.06.2023 r.,
- Certyfikatu do umowy ubezpieczenia mienia, sprzętu elektronicznego oraz odpowiedzialności cywilnej zawartej 15.12.2022 r., pomiędzy Województwem Śląskim, a TUIR „WARTA" S.A na okres od 17.12.2022 r. do 16.12.2023 r.,

- Umowy nr 4196/CI/2021 zawartej 19.11.2021 r., pomiędzy Województwem Śląskim, a konsorcjum 3S Data Center S.A. dotyczącej świadczenia usługi Data Center – kolokacja serwerów wraz z transmisją danych,
- Umowy nr 3465/CI/2021 zawartej 27.08.2021 r., pomiędzy Województwem Śląskim, a SITEL Sp. z o.o. dotyczącej świadczenia usługi stałego szerokopasmowego dostępu do sieci Internet dla urzędu,
- Umowy nr 3099/CI/2022 zawartej 28.07.2022 r., pomiędzy Województwem Śląskim, a SALUTARIS Sp. z o.o. dotyczącej dostawy systemu przetwarzania danych – serwerów wraz z instalacją i gwarancją,
- Wniosku o dostęp zdalny poprzez tunel VPN dla pracownika Departamentu Cyfryzacji i Informatyki z 15.10.2020 r.,
- Zarządzenia nr 30/22 Marszałka Województwa Śląskiego z 18.03.2022 r. w sprawie przyjęcia dokumentacji regulującej funkcjonowanie systemu bezpieczeństwa informatycznego w ramach zintegrowanego systemu zarządzania w Urzędzie Marszałkowskim Województwa Śląskiego,
- Wiadomości elektronicznej UWMSL z 12.09.2023 r., informującej o przechowywaniu logów zdarzeń LSI1240 dłużej niż 2 lata,
- Wiadomości elektronicznej UMWSL z 12.09.2023 r., informującej o szkoleniach pracowników UMWSL po przeprowadzonej kampanii phishingowej.
- Wiadomości elektronicznej UMWSL z 29.09.2023 r., informującej m.in. o wersji systemu operacyjnego, pod kontrolą którego działa LSI, zawierającej raport z odtwarzania LSI z kopi bezpieczeństwa z 29.09.2023 r. oraz skan wniosku o dostęp zdalny do sieci UMWSL z 19.09.2023 r.,
- Wiadomości elektronicznej z 03.11.2023 przekazującej pismo z 24.10.2023 r. znak: RT-RNR.1710.6.2023 RT-RNR.KW-00041/23, stanowiące odpowiedź IZ na wyniki audytu ujęte w sprawozdaniu wstępnym.

Przeprowadzono wywiady z pracownikami:

- Kierownikiem Referatu Projektowania i Rozwoju Systemów Informatycznych w Departamencie Cyfryzacji i Informatyki,
- Kierownikiem Referatu Zarządzania Infrastrukturą Teleinformatyczną w Departamencie Cyfryzacji i Informatyki,
- Informatykiem Zespołu Sieci i Systemów Serwerowych w Referacie Zarządzania Infrastrukturą Teleinformatyczną w Departamencie Cyfryzacji i Informatyki,
- Inspektorem Ochrony Danych,
- Kierownikiem Referatu ds. Zarządzania Systemem Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu.

Przeprowadzono m. in. następujące testy:

- dokonano weryfikacji funkcjonowania procedur wymienionych w pkt. II.2,
- dokonano weryfikacji umów wymienionych w pkt. II.2,
- przeprowadzono testy protokołów sieciowych dla domeny wykorzystywanej w ramach LSI,
- dokonano testów mechanizmów kontrolnych zaimplementowanych w LSI,
- sprawdzono ustawienia infrastruktury IT w zakresie LSI,
- sprawdzono ustawienia domenowe w zakresie polityki kont i haseł,
- sprawdzono ustawienia firewall-a,
- sprawdzono wyposażenie i zabezpieczenia pomieszczeń serwerowni.

Przeprowadzono wizyty w:

- Lokalizacjach Urzędu Marszałkowskiego Województwa Śląskiego, 40-037 Katowice przy ulicach:
  - Juliusza Ligonia 46,
  - Dąbrowskiego 23,
  - Powstańców 34.
- Centrum Przetwarzania 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 CST.

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 CST.

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, został określony na podstawie przeprowadzonej analizy ryzyka, w której uwzględniono:

- arkusz ustaleń (audyt follow-up) zatwierdzony w sierpniu 2022 r.,
- arkusz oceny zmian, wypełniony przez UMWSL, zawierający zmiany w poszczególnych obszarach/domenach normy ISO/IEC27002, które nastąpiły po 15 lutego 2022 roku.
- wizytę na miejscu w serwerowni Urzędu Marszałkowskiego Województwa Śląskiego, w której znajduje się środowisko produkcyjne,
- przegląd wstępny dokumentacji bezpieczeństwa, przeprowadzony przez audytorów IA.

IA w celu potwierdzenia prawidłowości wyznaczenia zakresu badania dokonała analizy dokumentów źródłowych i przekazanego przez instytucję arkusza zmian w obszarach normy ISO/IEC 27002. W wyniku analizy IA potwierdziła, że zaktualizowane zostały m. in. dokumenty: Polityka Ochrony Danych Osobowych, Księga Zintegrowanego Systemu Zarządzania, Procedury Audytu Wewnętrznego, Procedury Zarządzania Dostępem i Uprawnieniami, Procedury Postępowania ze Zdarzeniami Bezpieczeństwa Informacji, Instrukcja Użytkownika, Instrukcja Zarządzania Systemami Informatycznymi, Procedura Kopii Zapasowych, Polityka Zarządzania Ciągłością Działania oraz Zasady Zarządzania Zmianami IT.

Wprowadzone zmiany w wyżej wymienionych dokumentach dotyczyły zmian technicznych i organizacyjnych w następujących obszarach normy ISO/IEC 27002: Uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji, Procedury bezpiecznego logowania, System zarządzania hasłami, Fizyczna granica obszaru bezpiecznego, Fizyczne zabezpieczenie wejść, Lokalizacja i ochrona sprzętu, Zapasowe kopie informacji, Rejestrowanie zdarzeń, Synchronizacja zegarów, Zarządzanie podatnościami technicznymi, Zabezpieczenia sieci, Analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji, Odpowiedzialność i procedury, Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji, Zgłaszanie słabości związanych z bezpieczeństwem informacji, Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji, Reagowanie na incydenty związane z bezpieczeństwem informacji, Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji, Planowanie ciągłości bezpieczeństwa informacji, Wdrożenie ciągłości bezpieczeństwa informacji. Uwzględniając powyższe, zakres audytu bezpieczeństwa Lokalnego Systemu Informatycznego, stanowią następujące obszary:

1. Bezpieczeństwo zasobów ludzkich,
2. Kontrola dostępu,
3. Bezpieczeństwo fizyczne i środowiskowe,
4. Bezpieczna Eksploatacja,
5. Bezpieczeństwo komunikacji,
6. Pozyskiwanie, rozwój i utrzymanie systemów,
7. Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
8. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania.

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.

Z upoważnienia
Szefa Krajowej Administracji Skarbowej

Anna Chałupa
Zastępca Szefa Krajowej Administracji Skarbowej