Muzeum Podkarpackie w Krośnie
Raport z audytu

Przeprowadzony w dniu 12.03.2025

przez

CBI24 sp. z o. o. z siedzibą w Lublinie

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

Spis treści

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

Przebieg i cel audytu

W dniu 12 marca 2025 r. został przeprowadzony w Muzeum Podkarpackim w Krośnie audyt bezpieczeństwa informacji przez firmę: CBI24 sp. z o. o. z siedzibą w Lublinie (dalej „CBI24 sp. z o. o.). Celem audytu jest przedstawienie zaobserwowanego przez audytorów stanu bezpieczeństwa informacji w jednostce oraz wskazanie ewentualnych podatności mających wpływ na przetwarzane dane. Audyt został przeprowadzony pod kątem zgodności z obowiązującymi przepisami prawa w zakresie przetwarzania informacji oraz dobrych praktyk i standardów bezpieczeństwa. Audyt został zrealizowany na podstawie udostępnionej dokumentacji (procedur), sprzętu oraz w oparciu o następujące przepisy prawne:

1. Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz. U. z 2024 r. poz. 307);
2. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz. U. z 2024 r. poz. 773);
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - Dz. U. UE. L. z 2016 r., nr 119, str. 1 ze zm.);
4. Normy ISO: 27001:2017, 27005:2017.

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

I. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1. Świadczenie przez instytucję usług drogą elektroniczną.

Stan faktyczny:	Instytucja świadczy usługi drogą elektroniczną.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu. Jednym z podstawowych celów działania jednostki jest realizacja określonych usług wobec obywateli i innych podmiotów w sposób szybki, sprawny oraz maksymalnie przyjazny dla obywatela/podmiotu. Realizację praktyczną powyższych celów można uzyskać poprzez udostępnienie i promowanie usług elektronicznych dostępnych przez sieć Internet.
Podstawa prawna/dobre praktyki:	Art. 16 ustawy o informatyzacji Art. 19d ustawy o informatyzacji § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI

2. Promowanie e-usług elektronicznych przez jednostkę.

Stan faktyczny:	Instytucja nie promuje korzystania z e-usług.
Rekomendacje:	Jednym z podstawowych celów działania jednostki jest realizacja określonych usług wobec obywateli i innych podmiotów w sposób szybki, sprawny oraz maksymalnie przyjazny dla obywatela/podmiotu. Realizację praktyczną powyższych celów można uzyskać poprzez udostępnienie usług elektronicznych.
Podstawa prawna/dobre praktyki:	Art. 16 ustawy o informatyzacji Art. 19d ustawy o informatyzacji § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI

3. Strona BIP powinna zawierać opisy usług świadczonych przez Instytucję drogą elektroniczną.

Stan faktyczny:	Strona BIP nie zawiera opisów usług świadczonych przez Instytucję drogą elektroniczną.
Rekomendacje:	Opisy usług powinny być publikowane w BIP i zawierać wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw.
Podstawa prawna/dobre praktyki:	Art. 16 ustawy o informatyzacji Art. 19d ustawy o informatyzacji § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

4. **Wykorzystywanie wzorów dokumentów zatwierdzonych i/lub opracowanych przez CRWDE.**

Stan faktyczny:	Instytucja wykorzystuje wzory dokumentów zatwierdzonych i opracowanych przez Centralne Repozytorium Wzorów Dokumentów Elektronicznych (CRWDE).
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu, ponieważ w przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot np. właściwego ministra, lecz służy do świadczenia usług przez inne podmioty). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.
Podstawa prawna/dobre praktyki:	Art. 16a i 16 b ustawy o informatyzacji Art. 19b ust. od 3 do 5 ustawy o informatyzacji

5. **Wdrożenie i wykorzystywanie w Instytucji sytemu do elektronicznego zarządzania dokumentacją (EZD).**

Stan faktyczny:	Instytucja nie wykorzystuje systemów informatycznych do elektronicznego zarządzania dokumentacją (EZD).
Rekomendacje:	Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu jest sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego celu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.
Podstawa prawna/dobre praktyki:	Art. 14 ustawy o informatyzacji Art. 15 ustawy o informatyzacji § 5 ust. 3 pkt 3 rozporządzenia KRI § 11 rozporządzenia KRI § 13 rozporządzenia KRI § 16 rozporządzenia KRI Informacja o dostępności opisów standardów w zakresie protokołów komunikacyjnych i szyfrujących, zamieszczana przez Ministra Cyfryzacji w BIP zgodnie z § 16 ust. 3 rozporządzenia KRI.

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

6. **Weryfikacja, czy systemy teleinformatyczne komunikują się między sobą (np. czy EZD jest bezpośrednio „zasilane" z Elektronicznej Skrzynki Podawczej).**

Stan faktyczny:	Nie dotyczy – w jednostce brak EZD.
Rekomendacje:	Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu jest sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego celu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.
Podstawa prawna/dobre praktyki:	Art. 14 ustawy o informatyzacji Art. 15 ustawy o informatyzacji § 5 ust. 3 pkt 3 rozporządzenia KRI § 11 rozporządzenia KRI § 13 rozporządzenia KRI § 16 rozporządzenia KRI Informacja o dostępności opisów standardów w zakresie protokołów komunikacyjnych i szyfrujących, zamieszczana przez Ministra Cyfryzacji w BIP zgodnie z § 16 ust. 3 rozporządzenia KRI.

7. **Wykorzystywanie poczty elektronicznej w dedykowanej płatnej domenie, do realizacji zadań służbowych.**

Stan faktyczny:	Poczta elektroniczna służąca do realizacji zadań służbowych jest oparta o dedykowaną domenę indywidualną.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu, gdyż ewentualne wykorzystanie darmowych skrzynek pocztowych niepowiązanych z oficjalną domeną jednostki uniemożliwia weryfikację wiarygodności odbiorcy/nadawcy wiadomości oraz zwiększa ryzyko zawirusowania komputera ze względu na słabsze filtry antyspamowe i reklamy.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz. U. z 2024 r. poz. 773)

8. **Stosowanie bezpiecznego dostępu do służbowej poczty elektronicznej (np. klient pocztowy, dedykowany adres IP WAN).**

Stan faktyczny:	Klient pocztowy lub przeglądarka WWW z dowolnego adresu IP.
Rekomendacje:	Zaleca się ograniczenie dostępu do poczty elektronicznej. Dostęp do poczty możliwy wyłącznie z poziomu dedykowanego programu pocztowego. Dostęp wyłącznie z określonych adresów IP lub z wykorzystaniem VPN. Aktywacja/wdrożenie mechanizmu weryfikacji dwuetapowej lub przeniesienie usług na serwer posiadający taką funkcjonalność.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz. U. z 2024 r. poz. 773)

II. System zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych.

9. **Spełnienie obowiązku posiadania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).**

Stan faktyczny:	Instytucja nie posiada SZBI.
Rekomendacje:	Podmiot publiczny realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Ważne jest, by wszyscy pracownicy instytucji zapoznali się z SZBI i zobowiązali się do jego przestrzegania.
Podstawa prawna/dobre praktyki:	§ 19 ust. 1 rozporządzenia KRI § 19 ust. 2 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

10. **Weryfikacja czy dokumentacja SZBI została opracowana i zatwierdzona przez kierownictwo.**

Stan faktyczny:	Nie dotyczy – Instytucja nie posiada SZBI.
Rekomendacje:	Podmiot publiczny realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Ważne jest, by wszyscy pracownicy instytucji zapoznali się z SZBI i zobowiązali się do jego przestrzegania.
Podstawa prawna/dobre praktyki:	§ 19 ust. 1 rozporządzenia KRI § 19 ust. 2 rozporządzenia KRI

11. **Weryfikacja czy dokumentacja SZBI jest aktualizowana w sposób bieżący.**

Stan faktyczny:	Nie dotyczy – Instytucja nie posiada SZBI.
Rekomendacje:	Podmiot publiczny realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Ważne jest, by wszyscy pracownicy instytucji zapoznali się z SZBI i zobowiązali się do jego przestrzegania.
Podstawa prawna/dobre praktyki:	§ 19 ust. 1 rozporządzenia KRI § 19 ust. 2 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

12. Potwierdzenie czy pracownicy Instytucji zostali zapoznani z dokumentacją SZBI.

Stan faktyczny:	Nie dotyczy – Instytucja nie posiada SZBI.
Rekomendacje:	Podmiot publiczny realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI, w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym do skutecznego zarządzania bezpieczeństwem informacji w podmiocie. Ważne jest, by wszyscy pracownicy instytucji zapoznali się z SZBI i zobowiązali się do jego przestrzegania.
Podstawa prawna/dobre praktyki:	§ 19 ust. 1 rozporządzenia KRI § 19 ust. 2 rozporządzenia KRI

13. Potwierdzenie realizacji przeprowadzenia analizy ryzyka.

Stan faktyczny:	W Instytucji nie została przeprowadzona analiza ryzyka.
Rekomendacje:	Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i zależny od wielu czynników. Oznacza to, że nie ma jednego uniwersalnego i bezwzględnego kryterium oceny rodzaju i poziomu zabezpieczeń. Rodzaj i poziom zabezpieczeń jest zawsze pochodną szacowania ryzyka przeprowadzonego (w danym momencie) w realiach danego podmiotu.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 3 rozporządzenia KRI.

14. Podejmowanie działań minimalizujących wystąpienie ryzyka, stosownie do wyników przeprowadzonych analiz.

Stan faktyczny:	Nie dotyczy – brak analizy ryzyka.
Rekomendacje:	Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i zależny od wielu czynników. Oznacza to, że nie ma jednego uniwersalnego i bezwzględnego kryterium oceny rodzaju i poziomu zabezpieczeń. Rodzaj i poziom zabezpieczeń jest zawsze pochodną szacowania ryzyka przeprowadzonego (w danym momencie) w realiach danego podmiotu.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 3 rozporządzenia KRI.

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

15. **Posiadanie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.**

Stan faktyczny:	W instytucji została przeprowadzona inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji obejmująca ich rodzaj i konfigurację.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu. Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W praktyce oznacza to bieżące prowadzenie rejestru zasobów teleinformatycznych, zawierającego informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. Rejestr zasobów teleinformatycznych umożliwia m.in. odtworzenie infrastruktury teleinformatycznej po katastrofie lub innym zdarzeniu losowym.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 2 rozporządzenia KRI

16. **Potwierdzenie, że inwentaryzacja jest aktualizowana na bieżąco.**

Stan faktyczny:	Inwentaryzacja nie jest aktualizowana na bieżąco.
Rekomendacje:	Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W praktyce oznacza to bieżące prowadzenie rejestru zasobów teleinformatycznych, zawierającego informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. Rejestr zasobów teleinformatycznych umożliwia m.in. odtworzenie infrastruktury teleinformatycznej po katastrofie lub innym zdarzeniu losowym.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 2 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

17. Wykonywanie okresowych audytów legalności oprogramowania.

Stan faktyczny:	Nie przeprowadzono audytu legalności oprogramowania.
Rekomendacje:	Zarządzanie infrastrukturą informatyczną wymaga utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W praktyce oznacza to bieżące prowadzenie rejestru zasobów teleinformatycznych, zawierającego informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. Rejestr zasobów teleinformatycznych umożliwia m.in. odtworzenie infrastruktury teleinformatycznej po katastrofie lub innym zdarzeniu losowym.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 2 rozporządzenia KRI

18. Przeprowadzanie okresowych przeglądów infrastruktury IT (stacje robocze, serwery, urządzenia sieciowe).

Stan faktyczny:	Wyłącznie bieżąca obsługa bez tworzenia dokumentacji.
Rekomendacje:	Należy przeprowadzać okresowe kontrole infrastruktury teleinformatycznej, co pozwala na pozyskanie faktycznego stanu technicznego oraz zabezpieczeń komponentów sieciowych, serwerów, czy poszczególnych stacji roboczych. Kontrole takie powinny być wykonane na przykład na podstawie zarządzenia osoby kierującej jednostką oraz powinny zawierać raport. Okresowe i systematyczne kontrole minimalizują również ryzyko niezachowania ciągłości działania przez jednostkę.
Podstawa prawna/dobre praktyki:	EN ISO/IEC 27001:2017 A.11.2.4 Dobre praktyki IT.

19. Tworzenie dokumentacji z przeglądów okresowych infrastruktury IT (np. protokoły, dzienniki informatyczne).

Stan faktyczny:	Z przeglądów nie jest wykonywana dokumentacja.
Rekomendacje:	Należy przeprowadzać okresowe kontrole infrastruktury teleinformatycznej, co pozwala na pozyskanie faktycznego stanu technicznego oraz zabezpieczeń komponentów sieciowych, serwerów, czy poszczególnych stacji roboczych. Kontrole takie powinny być wykonane na przykład na podstawie zarządzenia osoby kierującej jednostką oraz powinny zawierać raport. Okresowe i systematyczne kontrole minimalizują również ryzyko niezachowania ciągłości działania przez jednostkę.
Podstawa prawna/dobre praktyki:	EN ISO/IEC 27001:2017 A.11.2.4 Dobre praktyki IT.

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

20. Zarządzanie uprawnieniami, potwierdzenie przyjęcia wewnętrznych procedur.

Stan faktyczny:	W instytucji nie zostały przyjęte procedury wewnętrzne zarządzania uprawnieniami.
Rekomendacje:	Zaleca się opracowanie, wdrożenie i stosowanie procedur, które szczegółowo regulują wewnętrzne zasady zarządzania (nadawania/zmian/odbierana) uprawnieniami pracy w systemach informatycznych. Procedury dotyczące zarządzania uprawnieniami powinny nakładać na instytucję również obowiązek prowadzenia rejestru upoważnień.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 4 rozporządzenia KRI § 19 ust. 2 pkt 5 rozporządzenia KRI

21. Weryfikacja czy osoby zaangażowane w proces przetwarzania informacji uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

Stan faktyczny:	W jednostce nie prowadzi się rejestru wydanych uprawnień.
Rekomendacje:	Rekomenduje się nadawanie uprawnień dla danego użytkownika, w stopniu adekwatnym do wykonywanych obowiązków czy zadań.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 4 rozporządzenia KRI § 19 ust. 2 pkt 5 rozporządzenia KRI

22. Weryfikacja uprawnień wszystkich użytkowników na stacjach roboczych, spełniających warunek zachowania minimalizacji do wymaganego poziomu (praca na kontach ograniczonych).

Stan faktyczny:	Wszyscy użytkownicy korzystają z kont posiadających uprawnienia ograniczone.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, ponieważ zaleca się, by wszyscy użytkownicy systemów informatycznych pracowali na ograniczonych kontach użytkowników. Jedynie w przypadku wykonania koniecznych działań, zaleca się by osoby do tego uprawnione logowały się na kontach administracyjnych.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 4 rozporządzenia KRI § 19 ust. 2 pkt 5 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

23. Bieżące wykonywanie przeglądu uprawnień nadanych do pracy w systemach informatycznych.

Stan faktyczny:	Przegląd uprawnień nadanych do pracy w systemach informatycznych jest wykonywany na bieżąco.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, ponieważ rekomenduje się okresowe, zgodne z przyjętymi w instytucji procedurami, przeglądy uprawnień nadanych do pracy w systemach informatycznych. Zaleca się, aby zakres uprawnień osób zaangażowanych w przetwarzanie danych był każdorazowo, bezzwłocznie zmieniany w przypadku zmiany zadań tych osób.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 4 rozporządzenia KRI § 19 ust. 2 pkt 5 rozporządzenia KRI

24. Potwierdzenie faktu przeprowadzania w instytucji szkoleń z bezpieczeństwa informacji.

Stan faktyczny:	W instytucji były prowadzone szkolenia z zakresu bezpieczeństwa informacji.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, ponieważ zaleca się szkolenie osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji; b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna; c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 4 rozporządzenia KRI § 19 ust. 2 pkt 5 rozporządzenia KRI

25. Posiadanie stosownych dokumentów potwierdzających fakt odbycia szkoleń z bezpieczeństwa informacji.

Stan faktyczny:	Instytucja posiada stosowne dokumenty potwierdzające fakt odbycia szkoleń z bezpieczeństwa informacji.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, gdyż zalecane jest prowadzenie dokumentacji z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, sposób potwierdzenia odbycia szkolenia; uczestnicy, data, zakres/temat, prowadzący/organizator itp.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 6 rozporządzenia KRI

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

26. Posiadanie wdrożonych regulacji wewnętrznych dotyczących pracy na odległość.

Stan faktyczny:	Instytucja przyjęła regulacje wewnętrzne dotyczące pracy na odległość.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, gdyż zaleca się, by w instytucji opracowano i przyjęto szczegółowe regulacje wewnętrzne dotyczące pracy na odległość.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 8 rozporządzenia KRI

27. Stosowanie przez instytucję bezpiecznego sposobu łączenia się podczas pracy zdalnej (np. VPN).

Stan faktyczny:	Instytucja stosuje odpowiednio zabezpieczony sposób łączenia się podczas pracy zdalnej.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, aby dostęp zdalny do systemu informatycznego w jednostce był możliwy wyłącznie poprzez wykorzystanie uwierzytelnionego połączenia VPN. Możliwe jest wykorzystanie oprogramowania typu TeamViewer, AnyDesk tylko i wyłącznie pod nadzorem osoby upoważnionej.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 8 rozporządzenia KRI

28. Spełnienie warunku zabezpieczenia poprzez szyfrowanie przestrzeni do przechowywania danych dla wszystkich urządzeń mobilnych stosowanych w jednostce.

Stan faktyczny:	Urządzenia mobilne nie są szyfrowane.
Rekomendacje:	Zaleca się by wszystkie urządzenia mobilne dostępne w instytucji posiadały odpowiednie zabezpieczenia kryptograficzne.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 8 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

29. **Nośniki uszkodzone lub niezdolne do ponownego użycia (przechowywanie w bezpiecznym miejscu, np. serwerownia).**

Stan faktyczny:	Nośniki uszkodzone lub niezdolne do ponownego użycia przechowywane są w bezpiecznym miejscu.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, gdyż takie nośniki powinny być przechowywane z takimi zabezpieczeniami jak dane produkcyjne.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

30. **Weryfikacja, czy wszystkie uszkodzone nośniki są niszczone w sposób bezpieczny oraz proces czy proces niszczenia komisyjnego jest potwierdzony stosownym protokołem.**

Stan faktyczny:	Nie dotyczy ze względu na brak niszczenia nośników. Wycofane nośniki gromadzone na terenie jednostki.
Rekomendacje:	Nie dotyczy.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

31. **Weryfikacja podpisanych umów serwisowych pod kątem posiadania zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.**

Stan faktyczny:	Umowy serwisowe podpisywane ze stronami trzecimi posiadają zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, gdyż zalecane jest zabezpieczenie umów serwisowych podpisywanych ze stronami trzecimi odpowiednimi zapisami gwarantującymi właściwy poziom bezpieczeństwa informacji.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 10 rozporządzenia KRI

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

32. Posiadanie regulacji wewnętrznych postępowania z incydentami.

Stan faktyczny:	Instytucja nie posiada regulacji wewnętrznych postępowania z incydentami naruszenia bezpieczeństwa informacji.
Rekomendacje:	Instytucja powinna posiadać procedury postępowania na wypadek zdarzeń związanych z naruszeniem bezpieczeństwa. Ma to na celu zwiększenie bezpieczeństwa danych przechowywanych w systemie. Zaleca się, aby wszyscy pracownicy byli poinformowani o istnieniu procedury dotyczącej zarzadzania incydentami związanymi z bezpieczeństwem informacji i przeszkoleni w zakresie zgłaszania zdarzeń, mogących świadczyć o naruszeniu bezpieczeństwa danych, a także potencjalnych słabości systemu informatycznego.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 13 rozporządzenia KRI

33. Potwierdzenie posiadania rejestru naruszeń.

Stan faktyczny:	Rejestr naruszeń nie jest prowadzony.
Rekomendacje:	Instytucja powinna posiadać procedury postępowania na wypadek zdarzeń związanych z naruszeniem bezpieczeństwa. Ma to na celu zwiększenie bezpieczeństwa danych, przechowywanych w systemie. Zaleca się, aby wszyscy pracownicy byli poinformowani o istnieniu procedury dotyczącej zarzadzania incydentami związanymi z bezpieczeństwem informacji i przeszkoleni w zakresie zgłaszania zdarzeń mogących świadczyć o naruszeniu bezpieczeństwa danych, a także potencjalnych słabości systemu informatycznego.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 13 rozporządzenia KRI

34. Podejmowanie działań korygujących przez Instytucję w przypadku wystąpienia naruszeń.

Stan faktyczny:	Nie dotyczy ze względu na fakt, iż do czasu audytu w jednostce nie wykryto naruszeń.
Rekomendacje:	Nie dotyczy.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 13 rozporządzenia KRI

35. Wykonywanie corocznych audytów bezpieczeństwa zgodnych z Krajowymi Ramami Interoperacyjności.

Stan faktyczny:	W instytucji nie był przeprowadzony audyt bezpieczeństwa zgodnie z zapisami zawartymi w KRI.
Rekomendacje:	Główną metodą kontroli bezpieczeństwa systemu informatycznego w instytucji jest prowadzenie audytów bezpieczeństwa. Audyty mogą być prowadzone przez osobę albo komórkę wewnętrzną instytucji lub przez wyspecjalizowany podmiot zewnętrzny. Coroczny audyt bezpieczeństwa prowadzi do ciągłego podnoszenia bezpieczeństwa przechowywanych danych, dlatego niezmiernie istotne jest, by instytucja wdrażała zalecenia poaudytowe.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 14 rozporządzenia KRI.

36. Podejmowanie działań korygujących na podstawie informacji zebranych podczas corocznych audytów bezpieczeństwa zgodnych z Krajowymi Ramami Interoperacyjności.

Stan faktyczny:	Nie dotyczy ze względu na brak audytu w jednostce.
Rekomendacje:	Nie dotyczy.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 14 rozporządzenia KRI.

37. Opracowanie przez jednostkę zasad / procedur tworzenia kopii zapasowych.

Stan faktyczny:	W jednostce zostały określone zasady tworzenia kopii zapasowych.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, gdyż zaleca się, aby wszystkie newralgiczne dane umożliwiające odtworzenie systemu po awarii były poddawane procesowi tworzenia kopii bezpieczeństwa. Dodatkowo zaleca się wykonywać kopie zapasowe plików konfiguracyjnych, logów systemowych oraz dzienników zdarzeń.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 lit. b rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

38. Tworzenie kopii zapasowych baz danych wszystkich systemów krytycznych.

Stan faktyczny:	Jednostka wykonuje kopie wszystkich baz danych systemów krytycznych.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, gdyż zaleca się, aby wszystkie newralgiczne dane umożliwiające odtworzenie systemu po awarii były poddawane procesowi tworzenia kopii bezpieczeństwa. Dodatkowo zaleca się wykonywać kopie zapasowe plików konfiguracyjnych, logów systemowych oraz dzienników zdarzeń.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 lit. b rozporządzenia KRI

39. Tworzenie kopii zapasowych logów systemowych.

Stan faktyczny:	Kopia logów systemowych wykonywana jedynie wraz z obrazem serwera.
Rekomendacje:	Zaleca się, aby wszystkie newralgiczne dane umożliwiające odtworzenie systemu po awarii były poddawane procesowi tworzenia kopii bezpieczeństwa. Dodatkowo zaleca się wykonywać kopie zapasowe plików konfiguracyjnych, logów systemowych oraz dzienników zdarzeń.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 lit. b rozporządzenia KRI

40. Tworzenie kopii zapasowych urządzeń sieciowych.

Stan faktyczny:	Są wykonywane kopie konfiguracji urządzeń sieciowych.
Rekomendacje:	Rekomendujemy utrzymanie bieżącego stanu, gdyż zaleca się, aby wszystkie newralgiczne dane umożliwiające odtworzenie systemu po awarii były poddawane procesowi tworzenia kopii bezpieczeństwa. Dodatkowo zaleca się wykonywać kopie zapasowe plików konfiguracyjnych, logów systemowych oraz dzienników zdarzeń.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

41. Tworzenie kopii zapasowych pozostałych danych mających wpływ na zachowanie ciągłości jednostki.

Stan faktyczny:	Są kopie plików wybranych folderów i stacji roboczych
Rekomendacje:	Zaleca się, aby wszystkie newralgiczne dane umożliwiające odtworzenie systemu po awarii były poddawane procesowi tworzenia kopii bezpieczeństwa. Dodatkowo zaleca się wykonywać kopie zapasowe plików konfiguracyjnych, logów systemowych oraz dzienników zdarzeń.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 lit. b rozporządzenia KRI

42. Wykonywanie okresowej weryfikacji poprawności wykonywanych kopii zapasowych.

Stan faktyczny:	W jednostce nie określono i nie przyjęto wytycznych dotyczących testowania kopii zapasowych.
Rekomendacje:	Kopie zapasowe powinny być regularnie testowane. Zaleca się wykonywanie okresowych testów odtwarzania systemu i aplikacji z backupu. Każdorazowo po przeprowadzeniu testów kopii zapasowych konieczne jest udokumentowanie tegoż procesu.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

43. Relokowanie kopii bezpieczeństwa poza obszar przetwarzania danych produkcyjnych.

Stan faktyczny:	Instytucja nie posiada alternatywnej lokalizacji do przechowywania kopii zapasowych.
Rekomendacje:	Ze względów bezpieczeństwa zaleca się przechowywanie kopii zapasowych w różnych miejscach, jedna z kopii powinna być przechowywana w lokalizacji innej niż podstawowa w celu ochrony przed zalaniem lub pożarem.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 lit. b rozporządzenia KRI

44. Zabezpieczenie kopii bezpieczeństwa fizyczne lub/i za pomocą mechanizmów kryptograficznych.

Stan faktyczny:	Wyłącznie zabezpieczenie fizyczne przed dostępem do nośnika kopi zapasowych.
Rekomendacje:	Należy wdrożyć odpowiednie środki techniczne i organizacyjne celem zabezpieczenia danych, np. poprzez opracowanie i wdrożenie polityki stosowania zabezpieczeń kryptograficznych kopii zapasowych lub/i utrzymać zabezpieczenie fizycznie przed dostępem osób nieuprawnionych.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 lit. b rozporządzenia KRI

45. Wykorzystywanie wyłącznie systemów teleinformatycznych zaprojektowanych i wdrożonych zgodnie ze odpowiednimi metodykami.

Stan faktyczny:	Systemy teleinformatyczne nie zostały zaprojektowane i wdrożone zgodnie z odpowiednimi metodykami. Zidentyfikowano pojedynczy system z ograniczonym wsparciem lub całkowitym jego brakiem.
Rekomendacje:	Projektowanie i wdrożenie systemów teleinformatycznych zgodnie z odpowiednia metodyką zapewnić może poprawność działania systemu, jego niezawodność, funkcjonalność, rozliczalność i bezpieczeństwo gromadzonych danych, a także zapewnia interoperacyjność, tj. zdolność do wymiany informacji z innymi systemami w oczekiwanej zgodności.
Podstawa prawna/dobre praktyki:	§ 15 ust. 1 rozporządzenia KRI

46. Zarządzanie bezpieczeństwem haseł (systemy centralnego zarządzania / Active Directory lub wdrożone polityki GPO) dla całego systemu teleinformatycznego jednostki.

Stan faktyczny:	Jednostka posiada system zarządzania bezpieczeństwem haseł dla całego systemu teleinformatycznego jednostki. Zidentyfikowano jednak stacje robocze nie podłączone do domeny Active Directory
Rekomendacje:	Zaleca się wdrożenie scentralizowanego systemu zarządzającego bezpieczeństwem haseł (Active Directory, Terminale) lub wdrożenie lokalnych polityk haseł (GPO) na wszystkich stacjach roboczych jednostki.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). EN ISO/IEC 27001:2017 A.9.4.2

47. Zgodność polityki haseł z wymogami zawartymi w dokumentacji opisowej (SZBI).

Stan faktyczny:	Polityka haseł na wszystkich komputerach nie jest zgodna z PB.
Rekomendacje:	Zaleca się zawsze, aby hasła były zgodne z dokumentacją opisową wdrożoną w jednostce.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

48. Realizacja obowiązku spisania i bezpiecznego zdeponowania haseł najwyższego poziomu z dostępem dla AD (bezpieczna koperta/szyfrowany plik).

Stan faktyczny:	Hasła najwyższego poziomu są spisane i zdeponowane w sposób bezpieczny z dostępem w każdej chwili do tych haseł przez AD.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu. Zawsze należy prowadzić pełną ewidencję haseł administracyjnych, zarówno do urządzeń jak i systemów. Ewidencja ta powinna być aktualna i dostępna dla kierownika jednostki w każdym momencie.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

49. Realizacja obowiązku bieżącej aktualizacji rejestru haseł najwyższego poziomu.

Stan faktyczny:	Hasła najwyższego poziomu są aktualizowane na bieżąco.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu. Zawsze należy prowadzić pełną ewidencję haseł administracyjnych, zarówno do urządzeń jak i systemów. Ewidencja ta powinna być aktualna i dostępna dla kierownika jednostki w każdym momencie.
Podstawa prawna/dobre praktyki:	Art. 24 i 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). EN ISO/IEC 27001:2017 A.9.4.2

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

50. Możliwość wystartowania komputera z innego nośnika niż dysk twardy.

Stan faktyczny:	Brak możliwości wystartowania komputera z innego nośnika niż dysk twardy.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu, tj. uniemożliwienie wystartowania stacji roboczej z innego nośnika niż dysk twardy. W przypadku braku możliwości blokady wystartowania stacji roboczej z innego nośnika niż dysk twardy, rekomenduje się zaszyfrowanie przestrzeni dyskowej.
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

51. Zastosowanie elementów ochrony fizycznej biur pomieszczeń i urządzeń, zapewniających bezpieczeństwo przetwarzanych informacji.

Stan faktyczny:	Zastosowane elementy ochrony fizycznej biur, pomieszczeń i urządzeń w instytucji zapewniają bezpieczeństwo przetwarzanych informacji.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu, ponieważ Instytucja zobligowana jest do zapewnienia właściwego poziomu ochrony przetwarzanych informacji. Poziom zabezpieczeń fizycznych powinien być dostosowany do potencjalnych zagrożeń, zidentyfikowanych na etapie szacowania ryzyka.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

52. Posiadanie wydzielonej serwerowni (bezpiecznego pomieszczenia technicznego) przez instytucję.

Stan faktyczny:	Instytucja posiada wydzieloną serwerownię lub bezpieczne wydzielone pomieszczenie techniczne.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

53. Dostęp do serwerowni wyłącznie dla osób upoważnionych.

Stan faktyczny:	Do serwerowni mają dostęp tylko osoby upoważnione.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu, gdyż dostęp do obszaru bezpiecznego powinien być zapewniony wyłącznie dla osób upoważnionych przez kierownika jednostki. W przypadku, gdy do serwerowni chce uzyskać dostęp osoba nieuprawniona, taki dostęp powinien być udzielony wyłącznie w obecności osoby upoważnionej. Wizyta wyżej wymienionej osoby musi być odnotowana w rejestrze wejść i wyjść.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

54. Prowadzenie rejestru osób upoważnionych do przebywania w serwerowni.

Stan faktyczny:	W instytucji nie jest prowadzony rejestr osób upoważnionych do przebywania w serwerowni.
Rekomendacje:	Dostęp do obszaru bezpiecznego powinien być zapewniony wyłącznie dla osób upoważnionych przez kierownika jednostki. Kierownik jednostki powinien posiadać stosowny rejestr osób upoważnionych do przebywania w bezpiecznym obszarze jakim jest w szczególności pomieszczenie serwerowni.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

55. Prowadzenie rejestru wejść i wyjść do serwerowni.

Stan faktyczny:	W instytucji jest prowadzony rejestr wejść i wyjść do/z serwerowni, zawierający wszelkie niezbędne informacje, w tym: datę i godzinę wejścia-wyjścia, cel wizyty oraz czytelny podpis.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu, gdyż dostęp do obszaru bezpiecznego powinien być zapewniony wyłącznie dla osób upoważnionych przez kierownika jednostki. W przypadku, gdy do serwerowni chce uzyskać dostęp osoba nieuprawniona, taki dostęp powinien być udzielony wyłącznie w obecności osoby upoważnionej. Wizyta wyżej wymienionej osoby musi być odnotowana w rejestrze wejść i wyjść.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

56. Drzwi do pomieszczenia technicznego/serwerowni wzmocnione/antywłamaniowe uniemożliwiające dostęp osobom nieupoważnionym.

Stan faktyczny:	Pomieszczenie serwerowni nie jest wyposażone w certyfikowane drzwi antywłamaniowe, uniemożliwiające dostęp osobom nieuprawnionym.
Rekomendacje:	Obszar bezpiecznego przetwarzania danych powinien posiadać zabezpieczenia fizyczne uniemożliwiające w sposób skuteczny dostęp do tego pomieszczenia osobom nieuprawnionym, np. drzwi spełniające określone wymogi bezpieczeństwa, certyfikowane zamki, strefy, śluzy bezpieczeństwa, ochronę.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

57. Pomieszczenie serwerowni wyposażone jest w klimatyzację.

Stan faktyczny:	Pomieszczenie serwerowni wyposażone jest w klimatyzację.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu, ponieważ urządzenie klimatyzacji minimalizuje ryzyko uszkodzenia lub przegrzania sprzętu (wysoka temperatura/wilgoć), a tym samym ryzyko uszkodzenia danych. Odpowiednie chłodzenie takiego pomieszczenia pomaga zachować również wyższą sprawność zasilania awaryjnego UPS sprzętu serwerowego.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

58. Pomieszczenie serwerowni wyposażone jest w system monitorowania klimatu z powiadomieniem administratora.

Stan faktyczny:	Pomieszczenie serwerowni nie jest wyposażone w system monitorowania klimatu z powiadomieniem administratora.
Rekomendacje:	Zaleca się monitorowanie klimatu serwerowni za pomocą czujników wraz z powiadomieniem osoby upoważnionej o wystąpieniu czynnika niekorzystnego (np. wzrost temperatury, zalanie, dym, itp.)
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

59. Pomieszczenie serwerowni wyposażone jest w system gaśniczy lub czujnik dymu wraz z ważną gaśnicą do gaszenia elektroniki.

Stan faktyczny:	Pomieszczenie serwerowni posiada instalację przeciwpożarową oraz gaśnicę przystosowaną do gaszenia elektroniki.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu. Zarówno system gaśniczy, jak i posiadanie rozwiązania uproszczonego, tj. czujnik wykrywania dymu wraz z gaśnicą do elektroniki, zmniejszają ewentualne skutki wystąpienia pożaru w pomieszczeniu serwerowni, a tym samym mogą zapobiec zniszczeniu przetwarzanych tam danych.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

60. Stosowanie w instytucji zabezpieczeń kryptologicznych na stacjach roboczych.

Stan faktyczny:	Brak dodatkowych zabezpieczeń - wyłącznie login i hasło do konta.
Rekomendacje:	Zaleca się stosowanie mechanizmów kryptologicznych chroniących przed nieautoryzowanym dostępem do stacji roboczych. Należy wprowadzić zabezpieczenia uniemożliwiające dostęp do aplikacji lub danych bez wcześniejszego uwierzytelnienia.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

61. Stosowanie w instytucji systemów antywirusowych i antyspamowych.

Stan faktyczny:	W instytucji stosowane są systemy antywirusowe i antyspamowe.
Rekomendacje:	Dla zapewnienia bezpieczeństwa systemów oraz przetwarzanych danych należy utrzymać ochronę przed kodem złośliwym, zarówno na poziomie stacji roboczych, urządzeń mobilnych, jak i na poziomie serwerów.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

62. Stosowanie w instytucji zapór sieciowych Firewall.

Stan faktyczny:	W instytucji stosowane są zapory sieciowe typu firewall.
Rekomendacje:	Dla zapewnienia bezpieczeństwa systemów oraz przetwarzanych danych należy utrzymać ochronę przed kodem złośliwym, zarówno na poziomie stacji roboczych, urządzeń mobilnych, jak i na poziomie serwerów.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 rozporządzenia KRI

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

63. **Czy jednostka posiada urządzenie brzegowe zapewniające zabezpieczenie sieci firewallem sprzętowym (np. klasy UTM) posiadającym między innymi takie funkcjonalności jak: Firewall, IPS/IDS, itp.**

Stan faktyczny:	Jednostka posiada urządzenie brzegowe zapewniające zabezpieczenie sieci firewallem sprzętowym (np. klasy UTM), posiadającym między innymi takie funkcjonalności jak: Firewall, IPS/IDS, itp.
Rekomendacje:	Bieżąca kontrola i utrzymanie obecnego stanu.
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

64. **Czy wdrożono blokadę stron internetowych niezwiązanych z pracą na stanowiskach.**

Stan faktyczny:	Jednostka stosuje filtrowanie stron WWW nie mnie jednak audytor uzyskał dostęp do witryn niepożądanych co oznacza konieczność weryfikacji zabezpieczeń wprowadzonych w jednostce.
Rekomendacje:	Weryfikacja mechanizmu blokowania stron internetowych niezwiązanych z pracą na stanowiskach.
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

65. **Czy jednostka stosuje ograniczenia ruchu sieciowego tylko do wymaganych usług/aplikacji.**

Stan faktyczny:	Polityka wprowadzona w urządzeniu brzegowym spełnia minimalne wymagania co do bezpieczeństwa.
Rekomendacje:	Bieżąca kontrola i utrzymanie obecnego stanu.
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

66. **Czy jednostka udostępnia infrastrukturę sieciową innym podmiotom.**

Stan faktyczny:	Jednostka nie udostępnia infrastruktury sieciowej innym podmiotom.
Rekomendacje:	Każdy z Administratorów Danych powinien posiadać oddzielną sieć logiczną lub fizyczną, celem minimalizacji ryzyk, takich jak: niezachowania poufności danych, integralności, a także rozliczalności działań w obrębie sieci administratora danych. Udostępnianie infrastruktury sieciowej jednostki innym podmiotom powinno być nadzorowane np. przez urządzenie typu UTM.
Podstawa prawna/dobre praktyki:	§ 19 ust. 7c rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

67. Czy sieć jednostki posiada podział fizyczny lub logiczny (np. VLAN).

Stan faktyczny:	Jednostka posiada podział fizyczny lub logiczny (np. VLAN).
Rekomendacje:	Utrzymanie bieżącego stanu, gdyż każda jednostka/organizacja powinna posiadać fizycznie bądź logicznie wydzieloną sieć informatyczną, natomiast w obrębie własnej sieci zaleca się wdrożenie dodatkowej segmentacji, celem minimalizacji ryzyk rozprzestrzeniania się np. złośliwego oprogramowania. W przypadku ataku na dany segment sieci istnieje duże prawdopodobieństwo, iż pozostałe segmenty sieci zachowają swoją integralność.
Podstawa prawna/dobre praktyki:	§ 19 ust. 7c rozporządzenia KRI

68. Identyfikacja czy poziom uprawnień poszczególnych logicznych segmentów sieci został zaimplementowany w sposób prawidłowy.

Stan faktyczny:	Sieć produkcyjna jest odseparowana od innych sieci/podsieci.
Rekomendacje:	Utrzymanie bieżącego stanu, dlatego że zawsze zaleca się ograniczenie ruchu pomiędzy segmentami sieci jedynie do wymaganego oraz dokonanie jej podziału za pomocą VLAN. Najczęściej zaleca się wdrożenie segmentacji sieci na serwery, urządzenia drukujące i stacje robocze, gdzie ruch sieciowy na styku tych segmentów będzie filtrowany oraz ograniczony wyłącznie do wymaganego.
Podstawa prawna/dobre praktyki:	§ 19 ust. 7c rozporządzenia KRI

69. Występowania w sieci informatycznej jednostki niezabezpieczonych przed dostępem udziałów ogólnodostępnych.

Stan faktyczny:	W sieci informatycznej jednostki występują niezabezpieczone udziały ogólnodostępne.
Rekomendacje:	Rekomenduje się wyłączenie udostępniania niezabezpieczonych zasobów lub zabezpieczenie ich przed dostępem osób nieupoważnionych, czy też zabezpieczenie przed złośliwym oprogramowaniem, gdyż skanowanie sieci wewnętrznej jednostki pozwoliło na znalezienie ogólnodostępnych udziałów sieciowych, do których dostęp może posiadać każdy użytkownik sieci bez posiadania stosownych dodatkowych uprawnień.
Podstawa prawna/dobre praktyki:	§ 19 ust. 7c rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

70. Czy jednostka podejmuje działania związane z aktualizacją oprogramowania software/firmware.

Stan faktyczny:	Zidentyfikowano systemy bez wsparcia - Windows 8.1 czy Windows Serwer 2012 R2
Rekomendacje:	Weryfikacja wersji firmware i w razie potrzeby zaktualizowanie oprogramowania na urządzeniach sieciowych jednostki do najnowszych stabilnych wersji. Należy prowadzić aktualizacje systemów operacyjnych i oprogramowania dodatkowego do najnowszych stabilnych wersji, w przypadku systemów niewspieranych zaleca się ich wymianę na nowsze, posiadające aktualne wsparcie producenckie.
Podstawa prawna/dobre praktyki:	§ 19 ust. 12a rozporządzenia KRI

71. Czy jednostka podejmuje działania związane z minimalizowaniem ryzyka utraty informacji poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych.

Stan faktyczny:	Jednostka nie podejmuje działań związanych z minimalizowaniem ryzyka utraty informacji poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych.
Rekomendacje:	Podjęcie działań związanych z minimalizowaniem ryzyka utraty informacji.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI

72. Czy jednostka podejmuje działania związane z zastosowaniem mechanizmów kryptograficznych dla transmisji danych dla poczty elektronicznej.

Stan faktyczny:	Jednostka podejmuje działania związane z zastosowaniem mechanizmów transmisji danych dla poczty elektronicznej, podpisów (kwalifikowanych/profil zaufany do autoryzacji dokumentów).
Rekomendacje:	Zalecamy utrzymanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

73. Podejmowanie działań mających na celu eliminowanie zidentyfikowanych podatności systemów teleinformatycznych (audyt podatności).

Stan faktyczny:	Jednostka nie podejmuje działań w związku z dostrzeżeniem nieujawnionych podatności systemów teleinformatycznych.
Rekomendacje:	Aby zapewnić bezpieczeństwo informacji przetwarzanych przez systemy teleinformatyczne niezbędna jest aktualizacja oprogramowania systemowego, dziedzinowego, antywirusowego i antyspamowego, aktualizacja firmware, stosowanie szeregu zabezpieczeń techniczno-organizacyjnych oraz zabezpieczeń kryptograficznych poczty elektronicznej, dotyczących środowiska teleinformatycznego pracy danego systemu. Rodzaj i poziom zastosowanych zabezpieczeń powinien wynikać z planu postępowania z ryzykiem i powinien być adekwatny do poziomu ryzyka wynikającego z analizy ryzyka BI.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI

74. Potwierdzenie faktu generowania i gromadzenia logów zarówno systemowych, jak i logów wszystkich użytkowników.

Stan faktyczny:	W instytucji nie są zbierane logi.
Rekomendacje:	Mając na uwadze zachowanie rozliczalności pracy w systemach teleinformatycznych instytucja zobligowana jest do gromadzenia wszystkich logów. Sposób zapisu oraz przechowywania logów powinien gwarantować integralność i niezaprzeczalność danych oraz ich bezpieczeństwo. Należy zapewnić kontrolę dostępu do logów, a także zadbać o zabezpieczenie przed ich nieuprawnionym usunięciem, modyfikacją, zniszczeniem. W celu analizy logów rekomenduje się korzystanie przez instytucję ze specjalistycznego oprogramowania. Zgodnie z zapisami § 20 ust. 4 KRI instytucja zobowiązana jest do przechowywania logów przez okres dwóch lat.
Podstawa prawna/dobre praktyki:	§ 20 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

75. Potwierdzenie prowadzenia dzienników logów.

Stan faktyczny:	W instytucji nie są prowadzone dzienniki logów.
Rekomendacje:	Mając na uwadze zachowanie rozliczalności pracy użytkowników i administratorów w systemach teleinformatycznych instytucja zobligowana jest do gromadzenia logów. Sposób zapisu oraz przechowywania logów powinien gwarantować integralność i niezaprzeczalność danych oraz ich bezpieczeństwo. Należy zapewnić kontrolę dostępu do logów, a także zadbać o zabezpieczenie przed ich nieuprawnionym usunięciem, modyfikacją, zniszczeniem. W celu analizy logów rekomenduje się korzystanie przez instytucję ze specjalistycznego oprogramowania. Zgodnie z zapisami § 20 ust. 4 KRI instytucja zobowiązana jest do przechowywania logów przez okres dwóch lat.
Podstawa prawna/dobre praktyki:	§ 20 rozporządzenia KRI

76. Weryfikacja czy instytucja posiada możliwość automatycznej analizy logów za pomocą dedykowanego oprogramowania.

Stan faktyczny:	Instytucja nie posiada oprogramowania do automatycznej analizy logów.
Rekomendacje:	Mając na uwadze zachowanie rozliczalności pracy użytkowników i administratorów w systemach teleinformatycznych instytucja zobligowana jest do gromadzenia logów. Sposób zapisu oraz przechowywania logów powinien gwarantować integralność i niezaprzeczalność danych oraz ich bezpieczeństwo. Należy zapewnić kontrolę dostępu do logów, a także zadbać o zabezpieczenie przed ich nieuprawnionym usunięciem, modyfikacją, zniszczeniem. W celu analizy logów rekomenduje się korzystanie przez instytucję ze specjalistycznego oprogramowania. Zgodnie z zapisami § 20 ust. 4 KRI instytucja zobowiązana jest do przechowywania logów przez okres dwóch lat.
Podstawa prawna/dobre praktyki:	§ 20 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

77. Potwierdzenie spełnienia warunku, iż instytucja gromadzi wszystkie logi i przechowuje je przez okres co najmniej dwóch lat.

Stan faktyczny:	W instytucji logi nie są przechowywane przez okres 2 lat.
Rekomendacje:	Mając na uwadze zachowanie rozliczalności pracy użytkowników i administratorów w systemach teleinformatycznych instytucja zobligowana jest do gromadzenia logów. Sposób zapisu oraz przechowywania logów powinien gwarantować integralność i niezaprzeczalność danych oraz ich bezpieczeństwo. Należy zapewnić kontrolę dostępu do logów, a także zadbać o zabezpieczenie przed ich nieuprawnionym usunięciem, modyfikacją, zniszczeniem. W celu analizy logów rekomenduje się korzystanie przez instytucję ze specjalistycznego oprogramowania. Zgodnie z zapisami § 20 ust. 4 KRI instytucja zobowiązana jest do przechowywania logów przez okres dwóch lat.
Podstawa prawna/dobre praktyki:	§ 20 rozporządzenia KRI

78. Jednostka wprowadziła zasady zabezpieczenia logów systemowych przed nieautoryzowaną modyfikacją.

Stan faktyczny:	Nie wprowadzono zasad zabezpieczenia logów systemowych przed nieautoryzowaną zmianą.
Rekomendacje:	Mając na uwadze zachowanie rozliczalności pracy użytkowników i administratorów w systemach teleinformatycznych instytucja zobligowana jest do gromadzenia logów. Sposób zapisu oraz przechowywania logów powinien gwarantować integralność i niezaprzeczalność danych oraz ich bezpieczeństwo. Należy zapewnić kontrolę dostępu do logów, a także zadbać o zabezpieczenie przed ich nieuprawnionym usunięciem, modyfikacją, zniszczeniem. W celu analizy logów rekomenduje się korzystanie przez instytucję ze specjalistycznego oprogramowania. Zgodnie z zapisami § 20 ust. 4 KRI instytucja zobowiązana jest do przechowywania logów przez okres dwóch lat.
Podstawa prawna/dobre praktyki:	§ 20 rozporządzenia KRI

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

79. Posiadanie przez wszystkich użytkowników systemów informatycznych indywidualnych kont (warunek dotyczy zarówno użytkowników, jak i administratorów).

Stan faktyczny:	Wszyscy użytkownicy i administratorzy systemów informatycznych posiadają indywidualne konta.
Rekomendacje:	Zalecamy utrzymanie bieżącego stanu faktycznego, dlatego że mając na uwadze zachowanie zasady rozliczalności pracy użytkowników w systemach teleinformatycznych instytucji konieczne jest, by wszyscy użytkownicy i administratorzy systemów teleinformatycznych posiadali indywidualne konta. Ważne jest również, by w procedurach wewnętrznych instytucja zawarła zapisy o zakazie przekazywania haseł dostępu do kont innych użytkowników.
Podstawa prawna/dobre praktyki:	§ 20 rozporządzenia KRI

80. Czy jednostka korzysta z rozwiązań służących zabezpieczeniu przed wyciekami informacji z organizacji typu DLP (ang. Data Leak /Loss Prevention).

Stan faktyczny:	Jednostka nie stosuje mechanizmów typu DLP.
Rekomendacje:	Zalecamy wdrożenie mechanizmów DLP, celem zabezpieczenia informacji podlegających ochronie przez wyciekiem czy kradzieżą, takimi kanałami jak np. urządzenia przenośne USB, poczta elektroniczna, wydruki, itp.
Podstawa prawna/dobre praktyki:	§ 19 ust. 2 pkt 7 rozporządzenia KRI

81. Posiadanie przez jednostkę aktywnych sieci bezprzewodowych.

Stan faktyczny:	Jednostka posiada aktywne sieci bezprzewodowe WIFI.
Rekomendacje:	O ile istnieją możliwości techniczne rekomendujemy stosowanie sieci przewodowych ze względu na większe bezpieczeństwo i stabilność połączenia.

82. Stosowanie szyfrowania dla sieci bezprzewodowej (protokół co najmniej WPA/WPA2) z dodatkowym mechanizmem uwierzytelniania, np. serwer Radius – WPA-Enterprise.

Stan faktyczny:	Sieci WiFi jednostki są szyfrowane.
Rekomendacje:	Utrzymanie i kontrola stanu faktycznego. Nie mniej jednak w przypadku konieczności wykorzystywania sieci bezprzewodowej jako sieci produkcyjnej, zaleca się wdrożenie dodatkowego mechanizmu uwierzytelniania użytkowników do sieci bezprzewodowej (np. serwer Radius – WPA-Enterprise).
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

ISO 27001 | ISO 22301
CERTYFIKAT

CBI24 sp. z o. o. z/s w Lublinie
ul. Puławska 4D/10
20-046 Lublin

NIP: 712 347 91 56
REGON: 529271070
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 570 33 03
e-mail: biuro@cbi24.pl
www.cbi24.pl

83. Dostęp użytkowników sieci Wi-Fi do sieci produkcyjnej jednostki.

Stan faktyczny:	Sieć dla higrometrów jest odseparowana ale sieć w sekretariacie znajduje się w sieci produkcyjnej.
Rekomendacje:	Sieć bezprzewodowa powinna być oddzielona od sieci produkcyjnej. Jeśli jednak użytkownicy muszą mieć dostęp do sieci lokalnej, należy wprowadzić dodatkowe uwierzytelnianie użytkownika za pomocą np. serwera RADIUS.
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

84. Dostęp do sieci bezprzewodowej posiadają.

Stan faktyczny:	Sieć Wifi w sekretariacie na potrzeby jednego laptopa.

85. Weryfikacja czy złożoność hasła szyfrującego do sieci Wi-Fi zapewnia odpowiedni poziom bezpieczeństwa, tj. nie jest zbudowane w standardowych maskach dla oprogramowania deszyfrującego.

Stan faktyczny:	Hasło nie spełnia wymagań co do złożoności, długości oraz okresu zmian.
Rekomendacje:	Rekomendujemy, aby stosować hasła spełniające określone wymagania bezpieczeństwa, tj. przynajmniej 4 grup znaków, minimum 12 znaków długości i niebędące hasłem słownikowym. Należy również pamiętać o okresowej zmianie (co 30 dni) tych haseł i prowadzeniu rejestru wydanych poświadczeń.
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

III. Redukcja ryzyk wynikających z wykorzystania opublikowanych podatności systemów teleinformatycznych.

86. Wykonywanie testów penetracyjnych/testów podatności dla systemu teleinformatycznego jednostki.

Stan faktyczny:	Jednostka nie przeprowadzała testów penetracyjnych/testów podatności dla systemów teleinformatycznych.
Rekomendacje:	Rekomendujemy co najmniej raz do roku przeprowadzanie testów podatności w celu dokonania praktycznej oceny poziomu bezpieczeństwa zasobów informatycznych systemu w zdefiniowanej części pod kątem szczelności i odporności na nieupoważnione ingerencje w działanie systemu z obszaru sieci wewnętrznej i od strony sieci Internet.
Podstawa prawna/dobre praktyki:	Dobre praktyki IT.

IV. Obserwacje audytora.

Pełna treść materiału z uwagi na ochronę danych osobowych i zasobów informatycznych muzeum (certyfikaty) zostanie udostępniona na pisemny wniosek Zainteresowanego.