Aesco Group

Sprawozdanie
z audytu
nr 2/2020
w Publicznej Szkole Podstawowej
Kunowie

Jednostka:	Urząd Miasta i Gminy Kunów
Termin audytu:	18.11. – 31.12.2020 r.
Data sprawozdania:	31.12.2020 r.
Audytor:	Tomasz Dygała CIA

Wstęp

Tematem zadania zapewniającego było ogólne funkcjonowanie Publicznej Szkoły Podstawowej w Kunowie w Kunowie, w tym kontrola zarządcza, ochrona danych osobowych i bezpieczeństwo informacji. W związku z pandemią koronawirusa, zadanie zostało przeprowadzone w sposób zdalny.

Zadanie audytowe zostało przeprowadzone w terminie 18.11. – 31.12.2020 r. na podstawie Umowy, zawartej pomiędzy Miastem i Gminą Kunów a Aesco Group Sp. z o.o. Audyt przeprowadził Tomasz Dygała, Certified Internal Auditor no 81126 – audytor spełniający wymogi o których mowa w art. 286 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Audyt wynika z planu pracy na rok 2020.

Zakresem przedmiotowym było:

- Ogólne funkcjonowanie i organizacja Szkoły,
- Ochrona danych osobowych,
- Kontrola zarządcza,
- Bezpieczeństwo informacji w rozumieniu KRI.

W zakresie podmiotowym, audyt dotyczył Dyrektora Szkoły.

Uzgodnione kryteria oceny: zachowanie mechanizmów kontrolnych na każdym etapie akceptacji płatności, zapewnienie ciągłości działania.

Ustalenia z audytu

W ramach tematu ogólna organizacja i kontrola zarządcza, przedstawiono następujące dokumenty:

Ogólna organizacja

- Regulamin organizacyjny z dnia 10 grudnia 2018 r.,

Kontrola zarządcza:

- Instrukcja zarządzania ryzykiem datowana na 19 grudnia 2019 r.,

- Oświadczenie o stanie kontroli zarządczej za 2019 rok, datowane na 10 lutego 2020 r.,
- Samoocena kontroli zarządczej za 2019 rok, datowana na 28 stycznia 2020 r.,
- Plan kontroli zarządczej na rok 2021, datowany na dzień 18 listopada 2020 r.,
- Plan kontroli zarządczej na rok 2020, datowany na dzień 28 stycznia 2020 r.,
- Rejestr ryzyk na rok 2020, datowany na dzień 29 stycznia 2020 r.,
- Wykaz procedur obowiązujących w Szkole, datowany na 5 marca 2020 r.,
- Protokół ze zrealizowanej kontroli zarządczej w roku 2020.

Z punktu widzenia audytora przedstawiona dokumentacja sprawia wrażenie niekompletnej, iż nie przedstawiono planów ciągłości działania, karty zastępstw ani kodeksu etyki, które są elementami systemu kontroli zarządczej.

Ochrona danych osobowych i bezpieczeństwo informacji

W zakresie ochrony danych osobowych i bezpieczeństwa informacji, przedstawiono następujące dokumenty:

- Samoocena w zakresie bezpieczeństwa informacji,
- Informacja z dnia 30 maja 2019 o wyznaczeniu IOD przez usługodawcę zewnętrznego,
- Polityka ochrony danych osobowych z dnia 4 czerwca 2020 r.,
- Zarządzenie Dyrektora Szkoły nr 10/2019 z dnia 1 lipca 2019 r., powołujące Inspektora Ochrony Danych, wraz ze zgłoszeniem do UODO (UPO),
- Wynik wstępnego audytu ze strony IOD z dnia 28 czerwca 2019 r.,
- Protokół kontroli problemowej ze strony IOD w UMiG Kunów w zakresie ochrony danych osobowych z dnia 6 sierpnia 2020 r.,
- Rejestr czynności przetwarzania, datowany na 10 lutego 2020 r.,
- Umowa z dnia 22 maja 2019 o pełnienie funkcji Inspektora Ochrony Danych, wraz z jej kontynuacją,

W ocenie audytora poza przedstawionymi dokumentami Polityki bezpieczeństwa i Rejestru czynności przetwarzania z 2020 roku, brak śladów wypełniania obowiązków Inspektora Ochrony Danych, o których mowa w art. 39 RODO. Brakuje analizy ryzyka w zakresie ochrony danych osobowych.

Zgodnie z art. 39 RODO, obowiązki IOD przedstawiają się następująco:

> *1. Inspektor ochrony danych ma następujące zadania:*
>
> *a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;*
>
> *b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków,* ***działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty****;*

Należy zwrócić uwagę na kwestię udokumentowania działań Inspektora, tak żeby Dyrektor Szkoły mógł wykazać iż działania Inspektora rzeczywiście są prowadzone.

W kwestii powołania Inspektora Ochrony Danych, zgodnie z RODO:

> *Art. 37 1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:*
> *a) przetwarzania dokonują organ lub podmiot publiczny [...]*
>
> *[...]*
>
> *5.* ***Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39****.*

Tym samym Dyrektor Szkoły powinien dysponować informacjami na temat merytorycznego przygotowania IOD, w przeciwnym razie można mówić o braku dołożenia należytej staranności przy powoływaniu Inspektora.

Brak informacji dotyczących ochrony danych osobowych

Na stronach internetowych Szkoły nie ma żadnej informacji na temat Inspektora Ochrony Danych. Doszło tu do złamania przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 poz. 1000):

> ***Art. 10.*** *1. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.*
> *[...]*
> *6. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.*

> ***Art. 11. Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, nie-zwłocznie po jego wyznaczeniu, na swojej stronie internetowej,*** *a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.*

Zgodnie z wytycznymi UODO, podanymi na stronie internetowej Urzędu https://uodo.gov.pl/pl/138/569, *dane Inspektora Ochrony Danych powinny być łatwo dostępne. Wskazane jest, by dane o wyznaczonym IOD znalazły się w ogólnie dostępnym miejscu strony np. w zakładce: „Kontakt", „Inspektor ochrony danych", „RODO" czy „Ochrona danych osobowych". Za niewłaściwie zatem uznać należy publikowanie tych danych w miejscach wymagających długiego przeszukiwania, takich jak „Aktualności" czy „Polityka prywatności".*

Zdziwienie audytora budzi fakt iż powyższe nie zwróciło uwagi Inspektora Ochrony Danych podczas wykonywanych audytów.

Zgodność z Krajowymi Ramami Interoperacyjności

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań wymienionych w § 20 ust. 2 rozporządzenia KRI w zakresie:

> *1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;*
>
> *2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;*
>
> *3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;*
>
> *4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;*
>
> *5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;*
>
> *6) zapewnienia szkolenia 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;*

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Ustalenia szczegółowe

1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia

W myśl przepisu § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji (SZBI) zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Należy regularnie aktualizować System Zarzadzania Bezpieczeństwem Informacji, obejmujący ww. dokumenty a następnie w cyklu 12 miesięcznym dokonywać jego przeglądu i aktualizacji. Należy zwrócić uwagę, żeby system ten obejmował ochronę wszystkich informacji a nie tylko danych osobowych. Przyjęto politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym, z datą 4 czerwca 2020 r., stąd do końca 2021 należy dokonać ich przeglądu a ponadto rozszerzyć całościowo jako SZBI.

Należy także zwrócić uwagę na kwestię ujawniania w Instrukcji Zarządzania Systemem Informatycznym szczegółowych rozwiązań dotyczących np. zabezpieczeń fizycznych i technicznych, nadawania/cofania uprawnień, zabezpieczenia systemu informatycznego, wykonywania przeglądów i konserwacji, postępowania z nośnikami i sprzętem poza urzędem. Szczegółowe informacje w tym zakresie powinny być udostępniane wyłącznie pracownikom odpowiedzialnym za zarządzanie systemami informatycznymi, a nie wszystkim pracownikom, ponieważ stwarza to ryzyko, że informacje w nich zawarte mogą być wykorzystane do przełamania ustanowionych zabezpieczeń.

2) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

Zadeklarowano przeprowadzanie inwentaryzacji, jednak bez wsparcia specjalistycznego oprogramowania do automatycznej inwentaryzacji zasobów. Należy zwrócić uwagę, że inwentaryzacja w sensie księgowym nie spełnia wymogów związanych z KRI.

Istotą tego punktu jest aby w przypadku konieczności odtworzenia zasobów po zniszczeniu (Disaster Recovery Plan), dysponować aktualnymi informacjami pozwalającymi w prosty sposób odtworzyć konfigurację zasobów. Stąd ważne jest aktualizowanie inwentaryzacji oraz przechowywanie kopii zapisu poza siedzibą Urzędu. Audytor pragnie zwrócić uwagę, że dostępne jest zarówno oprogramowanie komercyjne jak i na zasadzie open source.

3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

Aby skutecznie zaprojektować SZBI konieczne 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 jest zależny od istotności informacji podlegających ochronie będących w posiadaniu lub przetwarzaniu urzędu. Rodzaj zastosowanych zabezpieczeń technicznych jak i ich poziom wynika zatem z szacowania ryzyka. Proces zarządzania ryzykiem składa się z następujących etapów: identyfikacja ryzyka, analiza ryzyka, w tym określenie poziomu ryzyka, ocena ryzyka (czy ryzyko jest akceptowalne lub tolerowane, a jeżeli nie, to określenie sposobu postępowania z ryzykiem). Jest to zadanie o charakterze ciągłym. Ujmując kwestię skrótowo – aby bronić się przed ryzykiem, trzeba je najpierw zidentyfikować.

Nie jest prowadzona okresowa analiza ryzyka utraty integralności, poufności, dostępności informacji, co jest niezgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI, bowiem analiza w zakresie ochrony danych osobowych nie wyczerpuje tematu. Dokonywanie cyklicznych analiz ryzyka utraty poufności, integralności i rozliczalności systemów informatycznych pozwala na identyfikację istotnych ryzyk w zakresie bezpieczeństwa informacji występujących w działalności Urzędu i umożliwia ustanowienie odpowiednich zabezpieczeń ograniczających możliwość ich wystąpienia.

4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji i

5) bezzwłoczna zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4

Wszelkie nadawanie czy zmiany w zakresie praw dostępu powinno się odbywać w sposób udokumentowany, na podstawie pisemnego zlecenia. Dla zachowania rozliczalności działań zaleca się aby jakiekolwiek działania związane z nadawaniem, zmianą czy cofanie dostępu do zasobów informatycznych, odbywały się wyłącznie na podstawie pisemnej (mailowej) dyspozycji.

6) zapewnienie szkolenia 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;

Czynnik ludzki jest zawsze najsłabszym ogniwem w systemie zabezpieczeń, stąd niezbędne jest regularne przeprowadzanie szkoleń w zakresie bezpieczeństwa, tak aby stale przypominać pracownikom o ciążących na nich obowiązkach w zakresie bezpieczeństwa a także aby dołożyć należytej staranności ze strony osób odpowiedzialnych za bezpieczeństwo. W ocenie audytora konieczne jest regularne powtarzanie tego rodzaju szkoleń, optymalnie w cyklu kwartalnym.

7) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji

Niepokój audytora budzi dostęp więcej osób niż tylko informatyka do serwerowni, co w konsekwencji może skutkować naruszeniem bezpieczeństwa. Dostępność serwerowni powinna być ograniczona.

8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość i

11) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

Nie dotyczy

9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie

Bez uwag

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

Bez uwag

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania, b) minimalizowaniu ryzyka utraty informacji w wyniku awarii, c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją, d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, e) zapewnieniu bezpieczeństwa plików systemowych, f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

W Szkole nie ma tzw. planów awaryjnych/podtrzymania ciągłości działania, skierowanych do pracowników. Owszem, występują plany wynikające z wymogów obronności i zarządzania kryzysowego, niemniej one są objęte klauzulami ograniczonego dostępu. Każdy pracownik powinien wiedzieć co ma zrobić w sytuacji niedostępności budynku (pożar, klęska żywiołowa, kataklizm etc.) a Dyrektor mieć gotowy algorytm postępowania w takiej sytuacji (miejsca zapasowych lokalizacji, sposób podłączenia się do sieci w tych lokalizacjach, komputery etc.). Konieczne jest sporządzenie takich planów.

Zwrócić uwagę należy na podtrzymywanie rezerwy sprzętowej na wypadek awarii sprzętu komputerowego w Szkole. W ocenie Audytora, dla zapewnienia ciągłości działania, należy zadbać o to aby na stanie stale, znajdował się 1 – 2 komputery na wypadek awaryjny (np. sprawny sprzęt wycofany już ze stanowisk pracy). Audytor zdaje sobie sprawę, że ze względu na skalę działalności, realizacja tego może być utrudniona.

Pamiętać należy o regularnym wykonywaniu kopii zapasowych oraz stosowaniu zasady 3-2-1, opartej na następujących założeniach:

- zawsze miej **trzy** backupy,
- używaj **dwóch** różnych technologii przechowywania danych (chmura, pendrive, zewnętrzny dysk twardy, taśma itp.),
- **jeden** backup przechowuj zawsze poza siedzibą.

Z punktu widzenia audytora, należy zwrócić uwagę na to aby bądź jeden z serwerów z kopiami zapasowymi, bądź kopia na nośniku zewnętrznym była na stałe przechowywana poza siedzibą Urzędu. W przeciwnym razie, w przypadku np. pożaru budynku Szkoły, grozić może także zniszczenie kopii zapasowych i utrata wszelkich danych.

Dla zapewnienia ciągłości działania, konieczne jest także regularne testowanie skuteczności wykonywania kopii zapasowych i sprawdzanie czy Szkoła jest w stanie podjąć działanie wyłącznie na podstawie danych zapisanych w kopiach zapasowych. Przeprowadzane testy należy udokumentować, prowadząc dzienniczek testów.

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

Nie istnieje procedura zgłaszania incydentów i w ciągu ostatniego roku żaden incydent nie został odnotowany. Brak odnotowania jakiegokolwiek incydentu może świadczyć o braku świadomości użytkowników o zagrożeniach lub o zasadach zgłaszania incydentów, co wobec braku szkoleń dla pracowników wydaje się być tezą uzasadnioną. Szkolenia dla pracowników powinny tę kwestię obejmować a procedura zgłaszania incydentów powinna zostać niezwłocznie uzupełniona.

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Bez uwag.

Podsumowanie

Ogólna organizacja i funkcjonowanie kontroli zarządczej nie budzi zastrzeżeń audytora (ewentualne uwagi w treści sprawozdania), natomiast w zakresie ochrony danych osobowych i bezpieczeństwa informacji, należy zwrócić uwagę na dopełnienie kwestii formalnych oraz aspekty związane z bezpieczeństwem, jak np. przechowywanie kopii zapasowych. Całościowo, **ocena pozytywna z nieprawidłowościami.**

W audytowanym obszarze funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza w ograniczonym stopniu

Zalecenia

lp	Treść	Termin	Ryzyko
1.	Niezwłocznie uzupełnić informacje na stronach internetowych, dotyczące Inspektora Ochrony Danych	niezwłocznie	💣💣💣 **wysokie**
2.	Przegląd i ewentualna aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji, obejmującego politykę bezpieczeństwa informacji i instrukcję zarządzania systemem informatycznym a następnie w cyklu 12 miesięcznym dokonywanie jego przeglądu i aktualizacji.	31 grudnia 2021	💣💣💣 **wysokie**
3.	Przeprowadzenie analizy ryzyka utraty integralności, poufności, dostępności informacji wraz z określeniem sposobu reakcji na stwierdzone ryzyka. Następnie okresowe (w cyklu co najmniej rocznym) jej powtarzanie.	31 marca 2021	💣💣💣 **wysokie**
4.	Organizowanie regularnych szkoleń dla pracowników w zakresie bezpieczeństwa systemów informatycznych i ochrony danych osobowych	31 marca 2021	💣💣💣 **wysokie**

5.	Regularne testowanie kopii zapasowych, dokumentowanie testowania.	Od zaraz	💣💣💣 **wysokie**
6.	Nadawanie, zmienianie praw dostępu do zasobów informatycznych, wyłącznie na podstawie pisemnej dyspozycji	Od zaraz	💣💣💣 **wysokie**
7.	Sporządzenie planów awaryjnych BCP/DRP	31 grudnia 2021	💣💣 **średnie**
	Skala ryzyka: 💣 niskie, 💣💣 średnie, 💣💣💣 wysokie, ☠ krytyczne		

Tomasz Dygała
Certified Internal Auditor no 81126

Zapoznałem się ze sprawozdaniem:
Burmistrz Kunowa (data i podpis)

Pouczenie:

W terminie 14 dni od dostarczenia niniejszego sprawozdania, Audytowanemu przysługuje prawo do wniesienia w drodze pisemnej, uwag, zastrzeżeń, w tym do terminu realizacji zaleceń.

Aesco Group
Finanse | Audyty | Oszczędności

Audyt Bezpieczeństwa Informacji, zgodnie z KRI, SAMOOCENA

1	Czy opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji?	tak
2	Czy SZBI jest zgodny z ISO 27001?	tak
3	Czy istnieje polityka bezpieczeństwa informacji?	tak
4	Czy polityka jest aktualna?	tak
5	Czy przyjęto Instrukcję zarządzania systemem informatycznym?	tak
6	Czy instrukcja jest aktualna?	tak
7	Czy istnieje system monitorowania, poddawania przeglądom i udoskonalania polityk i instrukcji?	tak
8	Czy polityka określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych?	tak
9	Czy instrukcja ZSI zawiera procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazuje sosby odpowiedzialne za te czynności?	tak
10	Czy instrukcja ZSI zawiera stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem?	tak
11	Czy instrukcja ZSI zawiera procedury rozpoczęcia, zawieszania i zakończenia pracy przeznaczone dla użytkowników systemu?	tak
12	Czy instrukcja ZSI zawiera procedury tworzenia kopii zapasowych zbiorów danych oraz programówi narzędzi programowych służących do ich przetwarzania?	tak
13	Czy instrukcja ZSI zawiera informacje o sposobie, miejscu i okresie przechowywania elektronicznych nośników informacji zawierających dane osobowe, oraz kopii zapasowych?	tak
14	Czy instrukcja ZSI zawiera sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego?	tak
15	Czy część instrukcji zawierająca informacje techniczne dot. bezpieczeństwa, posiada ograniczoną dostępność?	tak
16	Czy zidentyfikowano zbiory danych podlegających przetwarzaniu i zabezpieczeniu?	tak
17	Czy dokonano inwentaryzacji sprzętu IT?	tak

18	Czy inwentaryzacja jest aktualna?	tak
19	Czy inwentaryzacja przeprowadzana jest w sposób automatyczny	nie
20	Czy inwentaryzacja zawiera informacje o jego rodzaju i konfiguracji?	nie
21	Czy zapisana aktualna wersja inwentaryzacji znajduje się także w bezpiecznej lokalizacji?	tak
22	Czy inwentaryzacja obejmuje oprogramowanie?	tak
23	Czy przeprowadzono audyt licencji?	tak
24	Czy inwentaryzacja obejmuje także inny sprzęt niż komputery (routery, drukarki etc.)?	tak
25	Czy przeprowadzana jest okresowa analiza ryzyka w zakresie IT i bezpieczeństwa informacji?	tak
26	Czy istnieje procedura dot. przeprowadzania analizy ryzyka?	w trakcie przygot.
27	Czy analizy są okresowo powtarzane?	Nie
28	Czy ostatnią analizę przeprowadzono w ciągu ostatnich 12 miesięcy?	Nie
29	Czy podjęto działania wynikające z przeprowadzonej analizy?	nie
30	Czy istnieje dokumentacja z przeprowadzonej analizy ryzyka?	nie
31	Czy istnieje rejestr ryzyk?	nie
32	Czy powstał plan postępowania z ryzykiem?	nie
33	Czy ryzyko jest monitorowane?	nie
34	Czy nadane uprawnienia są adekwatne do wykonywanych zadań?	tak
35	Czy pracownicy mają zablokowaną możliwość instalacji dowolnego oprogramowania?	tak
36	Czy opracowano i wdrożono procedury zarządzania użytkownikami?	nie
37	Czy zarządzanie użytkownikami (nadawanie dostępów) odbywa się w sposób udokumentowany?	nie
38	Czy wszyscy pracownicy posiadają aktualne upoważnienia do dostępu do zasobów?	nie
39	Czy uprawnienia dostępowe do zasobów IT posiadają tylko aktualnie zatrudnieni pracownicy?	tak
40	Czy osobom które zakończyły zatrudnienie odebrano dostępy do zasobów IT?	tak
41	Czy uprawnienia administratora posiada wyłącznie osoba do tego upowazniona?	tak
42	Czy osobom które zakończyły zatrudnienie odbierane są dostępy do zasobów IT?	tak
43	Czy IT dostaje na czas informacje o ustaniu zatrudnienia?	tak
44	Czy istnieje plan szkoleń w zakresie bezpieczeństwa informacji?	tak
45	Czy w ciągu ostatnich 12 miesięcy przeprowadzono takie szkolenie?	tak
46	Czy w ciagu ostatnich 6 miesięcy przeprowadzono takie szkolenie?	tak

47	Czy szkolenia są udokumentowane?	tak
48	Czy szkolenie obejmowało tematykę zagrożenia bezpieczeństwa informacji?	tak
49	Czy szkolenie obejmowało tematykę skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawną?	tak
50	Czy szkolenie obejmowało tematykę stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich	tak
51	Czy informatyk uczestniczy w szkoleniach, w wymiarze min 40 godzin szkoleniowych w roku?	nie
52	Czy dostęp do serwerowni jest należycie chroniony?	tak
53	Czy drzwi do serwerowni są ognioodporne i przeciwwłamaniowe?	tak
54	Czy w serwerowni znajduje się gaśnica?	tak
55	Czy serwerownia jest zabezpieczona czujnikami antywłamaniowymi?	tak
56	Czy serwerownia jest zabezpieczona czujnikami p.poż?	tak
57	Czy w serwerowni znajduje się klimatyzacja?	nie
58	Czy w serwerowni nie znajdują się rury wodne i kanalizacyjne?	tak
59	Czy zapewnione jest podtrzymanie napięcia?	tak
60	Czy w razie awarii prądu dostęp do serwerowni pozostaje chroniony?	tak
61	Czy dostęp do serwerowni posiada wyłącznie informatyk?	nie
62	Czy wprowadzono system zastępstw zapewniających ciągłość działania?	tak
63	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez monitorowanie dostępu do informacji?	tak
64	Czy prowadzona jest archiwizacja logów do systemu?	nie
65	Czy prowadzony jest regularny monitoring logów?	nie
66	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji	ttak
67	Czy prowadzony jest monitoring logów pod kątem nieudanych logowań czy innych prób naruszenia bezpieczeństwa logicznego systemu IT?	nie
68	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji	tak
69	Czy pracownicy korzystają z urządzeń mobilnych?	nie

70	Czy pracownicy korzystają z możliwości pracy na odległość?	nie
71	Czy opracowano zasady korzystania z urządzeń mobilnych poza siedzibą urzędu?	nie
72	Czy utworzono zasady posługiwania się laptopami?	tak
73	Czy istnieją zasady dotyczące posługiwania się pamięciami USB?	tak
74	Czy zasady te zostały przyjęte w sposób formalny?	tak
75	Czy osoby pracujące mobilnie i na odległość potwierdziły pisemnie zapoznanie się z ww. zasadami?	nie
76	Czy zapewniono zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie?	nie
77	Czy serwis sprzętu/oprogramowania odbywa się na podstawie zawartych umów serwisowych?	tak
78	Czy ww. umowy zawierają zapis zapewniający odpowiedni poziom bezpieczeństwa informacji (zobowiązanie serwisu do poufności)?	tak
79	Czy stosowane są zabezpieczenia antywirusowe i antyspamowe?	tak
80	Czy stosowane są zapory sieciowe typu firewall?	tak
81	Czy sprzęt do niszczenia podlega demontażowi i jest przkazywany tylko specjalistycznym firmom?	tak
82	Czy pracownicy posiadają indywidualne loginy i hasła?	tak
83	Czy w ramach zastępstw każdy posiada indywidualny login i hasło na stanowisku osoby zastępowanej?	tak
84	Czy pomieszczenia biurowe są fizycznie zabezpieczone?	tak
85	Czy szafy z dokumentami zamykane są na klucz?	tak
86	Czy istnieją procedury przechowywania kluczy?	tak
87	Czy klucze przechowywane są w bezpiecznym miejscu?	tak
88	Czy kserokopiarki znajdują się w strefach bezpieczeństwa?	tak
89	Czy na parterze budynku zabezpieczone są okna?	tak
90	Czy w budynku jest alarm i czy jest on regulrnie testowany?	tak
91	Czy sprzęt jest chroniony przed zalaniem, pożarem?	tak
92	Czy okablowanie rozmieszczone jest w bezpieczny sposób?	tak
93	Czy sprzęt jest ubezpieczony?	tak
94	Czy w urzędzie wszystkie pomieszczenia w których przechowywane są informacje posiadają zabezpieczenia fizyczne?	tak
95	Czy pomieszczenia urzędu wyposażone są w niszczarki?	tak
96	Czy zapewniono dbałość o aktualizację oprogramowania?	tak

97	Czy oprogramowanie aktualizuje się automatycznie?	tak
98	Czy ustanowiono plany awaryjne BCP/DRP?	nie
99	Czy plany te znają kluczowe osoby w Urzędzie?	nie
100	Czy plany awaryjne są regularnie, okresowo testowane?	nie
101	Czy zapasowe hasła administracyjne są zabezpieczone i zdeponowane w bezpiecznej lokalizacji?	tak
102	Czy określono zasady korzystania z haseł zapasowych?	tak
103	Czy wykonywane są kopie zapasowe?	tak
104	Czy wykonywane są kopie zapasowe wszystkich baz danych?	tak
105	Czy kopie zapasowe są testowane?	tak
106	Czy testowanie kopii zapasowych ma swoje odzwierciedlenie w dzienniku testów?	nie
107	Czy testy kopii zapasowych przeprowadzono w ciągu ostatniego roku?	tak
108	Czy trwałość kopii zapasowych gwarantuje możliwość odtworzenia danych przez okres co najmniej 5 lat?	nie
109	Czy określono okres przechowywania kopii zapasowych?	tak
110	Czy częstostliwość i sposób wykonywania kopii gwarantuje możliwość odtworzenia danych sprzed awarii (utrata danych nie większa niż 1 dzień roboczy)?	tak
111	Czy serwer kopii zapasowych znajduje się w innej lokalizacji niż serwerownia?	tak
112	Czy istnieje kopia zapasowa poza siedzibą Urzędu?	tak
113	Czy serwery kopii zapasowych znajdują się w bezpiecznej lokalizacji?	tak
114	Czy dostęp do serwerów kopii zapasowych podlega monitorowaniu?	tak
115	Czy utrzymywany jest sprzęt zapasowy na wypadek awarii?	tak
116	Czy zapewniono ochronę przed błędami, utratą, nieuprawnioną modyfikacją?	tak
117	Czy zapewniono stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa?	nie
118	Czy zapewniono bezpieczeństwo plików systemowych?	tak
119	Czy zapewniono redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych?	tak
120	Czy zapewniono niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa?	tak
121	Czy zapewniono kontrolę zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa	tak
122	Czy istnieje procedura dot. zgłaszania incydentów?	tak

123	Czy incydenty są bezzwłocznie zgłaszane zgodnie z tą procedurą?	tak
124	Czy pracownicy potwierdzili zapoznanie się z tą procedurą?	tak
125	Czy w ostatnim roku zgłoszone zostały jakieś incydenty?	nie
126	Czy w poprzednim roku zgłoszone zostały jakieś incydenty?	nie
127	Czy w reakcji na zgłoszenia podjęto działania korygujące?	nie
128	Czy przeprowadzono audyt bezpieczeństwa informacji w roku 2014?	nie
129	Czy przeprowadzono audyt bezpieczeństwa informacji w roku 2015?	tak
130	Czy przeprowadzono audyt bezpieczeństwa informacji w roku 2016?	nie
131	Czy przeprowadzono audyt bezpieczeństwa informacji w roku 2017?	nie
132	Czy przeprowadzono audyt bezpieczeństwa informacji w roku 2018?	nie
133	Czy przeprowadzono audyt bezpieczeństwa informacji w roku 2019?	nie
134	Czy wdrożono zalecenia wynikające z tych audytów?	tak