JEDNOLITA ANALIZA KONTROLNA

KRAJOWYCH RAM INTEROPERCYJNOŚCI

PRZY PRZETWARZANIU DANYCH OSOBOWYCH ZGODNIE Z USTAWĄ O INFORMATYZACJI

Administrator Danych:	**Szkoła Podstawowa im .ks. Jana Twardowskiego w Powidzku**
dnia:	**2022-10-11**

zgodnie z:

Art. 24 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).

oraz

Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2017r., poz. 570),

oraz

Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017 poz. 2247),

oraz

§4 pkt 5 Rozporządzenia Ministra Spraw Wewnętrznych I Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U.2004r., nr 100, poz. 1024)

oraz

ustawa z dnia 24 sierpnia 1991 roku o ochronie przeciwpożarowej (Dz. U. 2017, poz. 620)

wprowadza dokument o nazwie:

JEDNOLITA ANALIZA KONTROLNA KRAJOWYCH RAM INTEROPERACYJNOŚCI

PRZY PRZETWARZANIU DANYCH OSOBOWYCH ZGODNIE Z USTAWĄ O INFORMATYZACJI

Zapisy tego dokumentu wchodzą w życie z dniem ogłoszenia.

§1

Sprawnie działający system bezpieczeństwa informacji jest niezwykle istotny z uwagi na sensytywność przetwarzanych danych osobowych oraz sposób ich przetwarzania. Administrator Danych: **Szkoła Podstawowa im .ks. Jana Twardowskiego w Powidzku** ma świadomość, iż jego podstawowym zadaniem jest ochrona przetwarzanych danych osobowych tj. zapewnienie odpowiednich środków organizacyjnych i technicznych, które uniemożliwią dostęp do treści zawierających dane osobą nieuprawnionym. Z uwagi na powyższe, Administrator Danych: **Szkoła Podstawowa im .ks. Jana Twardowskiego w Powidzku** w celu wykonania sprawdzenia na jakim poziomie kształtuje się poziom ryzyka utraty danych osobowych, wdraża dokument o nazwie „Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych zgodnie z ustawą o informatyzacji”.

§2

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga:

1. zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem;

2. ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
3. zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
4. zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
5. zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
6. zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

§ 3

W związku z § 1 niniejszego dokumentu Administrator Danych wprowadza dokument „**Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych zgodnie z ustawą o informatyzacji**” w podmiocie: **Szkoła Podstawowa im .ks. Jana Twardowskiego w Powidzku** w celu badania i obserwowania istniejącego środowiska przetwarzania danych osobowych oraz możliwości stworzenia odpowiednich zabezpieczeń organizacyjnych i technicznych.

§ 4

Ilekroć w „**Jednolitej Analizie Kontrolnej Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych zgodnie z ustawą o informatyzacji**” jest mowa o:

1. **ANALIZIE RYZYKA** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
2. **SZACOWANIU RYZYKA** – proces oceny i analizy ryzyka;
3. **OCENIE RYZYKA** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
4. **POSTĘPOWANIU Z RYZYKIEM** – wdrażanie środków modyfikujących ryzyko;
5. **ZARZĄDZANIU RYZYKIEM** – działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
6. **RYZYKU SZCZĄTKOWYM** – ryzyko pozostające po procesie postępowania z ryzykiem;
7. **AKCEPTOWANIU RYZYKA** – decyzja, aby zaakceptować ryzyko;
8. **BEZPIECZEŃSTWIE INFORMACJI** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
9. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI**

– jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji;

11. **AKTYWACH** – wszystko, co ma wartość dla organizacji;
12. **ZAGROŻENIACH SYSTEMU** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
13. **DOSTĘPNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
14. **INCYDENCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO** — należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
15. **INFORMATYCZNYM NOŚNIKU DANYCH** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
16. **INTEGRALNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
17. **OPROGRAMOWANIU ZŁOŚLIWYM** — należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;
18. **PODATNOŚCI** — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;
19. **POŁĄCZENIU MIĘDZYSYSTEMOWYM** — należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;
20. **POUFNOŚCI** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
21. **PRZEKAZYWANIU INFORMACJI** — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;
22. **TESTACH BEZPIECZEŃSTWA** — należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;
23. **ZABEZPIECZENIU** — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
24. **ZAGROŻENIU** — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
25. **ZASOBACH SYSTEMU TELEINFORMATYCZNEGO** – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

§ 5

Skuteczność zastosowanych środków powinna podlegać cyklicznym badaniom. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany czy modyfikacji wprowadzonych wcześniej przez Administratora Danych systemów ochrony. Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności, określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności odnosi się głównie do środowiska komputerowego, czyli jednego z czterech obszarów przetwarzania danych osobowych, natomiast nie można wykonać całościowej oceny systemu bezpieczeństwa informacji bez uwzględnienia pozostałych zakresów ochrony danych osobowych. Zarządzanie ryzykiem ma na celu zidentyfikowanie i oszacowanie ryzyka związanego z naruszeniem poufności, integralności czy dostępności danych osobowych. Obszary przetwarzania danych osobowych określa **załącznik nr 1**.

§ 6

Możliwe zagrożenia występujące w systemach informatycznych, określa **załącznik nr 2**.

§ 7

Podatność systemu na zagrożenia, określa **załącznik nr 3**.

§ 8

Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności – określenie poziomu ryzyka określona została w **załączniku nr 4**.

§ 9

Wnioski i działania naprawcze, określa **załącznik nr 5**.

§ 10

Plan postępowania z ryzykiem w związku z przeprowadzoną Jednolitą Analizą Kontrolną Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych, określa **załącznik nr 6**.

§ 11

Pytania kontrolne oraz tabela szacowania ryzyka została określona w **załączniku nr 7**.

.....

(Podpis Administratora Danych)